MAIRIE DE PARIS

INSPECTION GENERALE

Exemplaire n°

RAPPORT DEFINITIF

AUDIT DES FICHIERS INFORMATIQUES DE LA VILLE ET DU DEPARTEMENT DE PARIS

n° 09-23

- juin 2010 -

Rapporteurs :

…, Inspecteur Général
…, Chargé de mission

Le Maire de Paris

09.23

15 2009

NOTE

à l'attention de Madame

Directrice Générale de l'Inspection Générale

Objet : Audit des fichiers informatiques de la Ville et du Département de Paris.

Le respect du droit à la protection des données personnelles est une exigence démocratique forte qui s'impose à toute administration. Je souhaite que l'administration parisienne soit à cet égard exemplaire.

La désignation, en 2006, d'un correspondant de la Commission Nationale Informatique et Libertés va dans ce sens.

Je souhaite que nous allions plus loin et vous demande de procéder à un audit complet des pratiques des directions tant à travers les outils informatiques qu'elles développent que la façon dont elles garantissent la confidentialité des données qu'elles détiennent et l'anonymisation de leurs archives.

Cette mission est aussi indispensable compte tenu de l'ancienneté de certaines applications informatiques et du caractère transversal des nouvelles applications.

Je souhaite donc que vous me proposiez des recommandations afin de sécuriser nos outils dans le respect des textes qui organisent la protection des données personnelles.

Le Secrétariat Général facilitera votre mission à laquelle sera associé le correspondant informatique et libertés.

Votre rapport sera rendu au plus tard à la fin du 1er trimestre 2010.

Très cordialement

Bertrand DELANOË

INSPECTION GENERALE
(rapport n°09-23)

NOTE DE SYNTHESE
DU
RAPPORT DÉFINITIF
juin 2010

La désignation en 2006 d'un correspondant informatique et libertés (CIL) au sein de la Ville a marqué la volonté de celle-ci de se placer au meilleur niveau pour le respect des obligations légales en matière de protection des données personnelles. L'incident survenu en 2008 (l'affaire GESPER) a montré cependant la nécessité d'une vigilance accrue. Les activités très diverses des services municipaux, l'avènement de la micro informatique de masse, le vieillissement de certaines applications développées à une époque où le souci de respect des normes était moindre, sont cependant autant de facteurs de risque. La commission nationale de l'informatique et des libertés (CNIL) a dans la période récente fort légitimement multiplié les contrôles. Il était donc nécessaire de procéder à un état des lieux, de réaliser un bilan et de proposer un ensemble de mesures pour sécuriser au mieux les données personnelles objets de fichiers et de traitements sous la responsabilité de la Ville.

Les rapporteurs ont pris un double parti :

- l'utilisation d'un questionnaire, diffusé auprès de l'ensemble des services, destiné à recueillir l'information. L'envoi de ce document a du reste favorisé dans un certain nombre de services une véritable prise de conscience des enjeux.

Les rapporteurs ont ensuite rencontré, en fonction des réponses, un certain nombre de directions parmi les plus exposées.

- l'examen d'exemples d'entités certes différentes de la Ville, mais comparables par la taille et les préoccupations. Les échanges ont été complétés par un rendez-vous, indispensable, avec la CNIL.

Le bilan réalisé n'a pas révélé de faille majeure ni de secteur particulièrement « à risque ». Mais il invite à poursuivre l'effort engagé en 2006, notamment par un renforcement des moyens administratifs de suivi, un effort soutenu de formation et d'information, et des contrôles périodiques destinés à sensibiliser toujours plus les services à ce sujet éminemment sensible.

Rapporteurs :

…, Inspecteur Général
…, Chargé de mission

SOMMAIRE

Introduction

Les rapporteurs ont démarré leurs travaux en rencontrant M. …… , correspondant informatique et libertés (CIL) depuis 2006, et l'état major de la DSTI.

Le premier constat a été **l'impossibilité de procéder à un recensement exhaustif et fiable de l'ensemble des traitements et fichiers contenant ou susceptibles de contenir des informations nominatives**. Ce point méritait d'être précisé d'emblée : il est aujourd'hui impossible dans une entité comme la Ville de prétendre sérieusement réaliser une telle opération, alors même qu'il est possible à tout un chacun à partir de son micro-ordinateur de créer et exploiter un fichier contenant ce type de données – il y a plus de 20 000 micro-ordinateurs dans les services !

Ce constat n'interdit pas d'exercer un contrôle attentif sur l'ensemble des applications et traitements qui dépendent directement de la DSTI et de celles qui sont connues et gérées par les directions, soit à partir de la DSTI, soit localement.

La démarche d'audit a été conduite en quatre phases :

- une enquête par questionnaire auprès de l'ensemble des services de la Ville (hors CASVP),
- des entretiens auprès de quelques directions plus particulièrement exposées dans cette catégorie de risques (DRH, DASES, DFPE, DAC, DASCO, DJS, DICOM, DPE),
- une comparaison avec trois structures similaires en termes de taille et de niveau de sensibilité à ces types de risque (EDF, AG2R, Banque de France),
- et in fine, un entretien avec la CNIL.

Le point d'entrée pour réaliser l'analyse de la situation a été recherché auprès des « correspondants informatique et télécommunication » (les CIT), présents dans la quasi-totalité des directions ; le moyen retenu pour les mobiliser a été celui du **questionnaire**, construit pour tenter d'identifier avec les services les zones à risque et évaluer les différents aspects des situations rencontrées. L'opération a été lancée au cours d'une réunion des CIT qui a permis de les informer et d'évaluer leurs premières réactions.

Le recours à cette méthode du questionnaire a suscité des interrogations, des demandes et des réactions qui permettent d'envisager une mobilisation large et durable sur le sujet après la remise du présent rapport. Le dépouillement des réponses aux questions a été corroboré ensuite par des entretiens approfondis auprès de huit directions (cf. supra) : les réunions mobilisaient toujours le CIT de la direction et un ou deux responsables hiérarchiques (directeur adjoint, sous-directeur, chef de bureau) plus spécifiquement en charge de ces questions.

Les rapporteurs se sont ensuite attachés à procéder, en compagnie de notre CIL, à un certain nombre d'entretiens avec des CIL de grandes entités aux problématiques comparables à celles de la Ville. Il a ainsi été possible de recouper les conclusions de l'enquête, et les indications ainsi recueillies ont permis d'enrichir et de renforcer les recommandations sur les mesures à mettre en œuvre, à la fois pour pérenniser les acquis et pour améliorer à travers une forte action d'information et de formation la sécurité générale des données personnelles recueillies et traitées, qu'il s'agisse de celles des Parisiens ou de celles des agents de la Ville.

Enfin, les rapporteurs et le CIL se sont rapprochés du responsable des CIL au sein de la CNIL pour recueillir ses recommandations sur les différents points soulevés tout au long des différents entretiens.

1. LES ENJEUX ET LES LIMITES DU SUJET

1.1. Les enjeux : la Ville face à un problème important de libertés publiques : l'affaire GESPER

A la suite de l'alerte et de la diffusion d'informations par une organisation syndicale, la Commission nationale de l'informatique et les libertés (CNIL) a diligenté le 21 novembre 2008 une mission d'inspection à la direction des espaces verts et de l'environnement (DEVE).

Cette mission avait pour objet « d'apprécier les conditions dans lesquelles cette direction mettait en œuvre des traitements de données à caractère personnel » au regard des dispositions de la loi n° 78-17 du 6 janvier 1978, modifiée le 6 août 2004, notamment quant à l'application de gestion des plannings des agents de surveillance, dénommée « GESPER ».

Cette application GESPER gère les plannings de roulement des agents de surveillance des parcs et jardins ainsi que leurs tâches quotidiennes. Fonctionnant à l'origine en monoposte, elle a ensuite été centralisée et mise en réseau. Elle comprend un ensemble d'informations détaillées sur les agents et leur activité :

- une fiche « identité »
- une fiche de « paramètres » : l'affectation de base, le cycle du travail, le mode de calcul des congés acquis, le mode de calcul des éléments de paie, les absences
- une fiche sur le contrat de travail
- une fiche sur les stages de formations suivis
- une fiche relative à l'assermentation
- une fiche relative à un bilan annuel des heures pour le calcul des éléments variables
- une fiche pour le suivi des demandes de congé et des fonctions de planning : le planning standard, distribué à la hiérarchie, et celui des tâches distribuées à l'agent.

La version d'origine, contrôlée par la CNIL en 1999, comprenait un certain nombre d'autres fiches : les enfants à charge, le nombre et le suivi des repas, les éventuelles reprises d'ancienneté, les éventuels congés bonifiés accordés à l'agent, les contraventions dressées par celui-ci… et une fiche « **divers** ».

L'application comportait en outre de **nombreuses zones de commentaires libres**, susceptibles d'être renseignées par la hiérarchie et de contenir des appréciations sur les agents et leur manière de servir.

Les principales observations de la CNIL, assez sévères, et contenues dans un courrier du 17 avril 2009, sont reproduites ci-après :

« En premier lieu, je note que l'outil informatique GESPER+ permet de recueillir un nombre important d'informations relatives aux agents municipaux relevant de cette direction. Or, certaines données traitées apparaissent sans lien évident avec la finalité du traitement.

En effet, les données relatives à la nationalité de l'agent, à son lieu de naissance, à sa qualité d'électeur, à la cause de fin de son contrat, aux noms et prénoms de ses enfants ou encore à l'historique des types de repas ne semblent pas indispensables à la planification des tâches. En outre, cette application comporte de nombreuses zones de commentaire libre dont certaines ne se justifient pas.

Or, je vous rappelle que l'article 6-3 de la loi précitée[1] prévoit que les données traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées.

Ensuite, j'observe que, si lors de la déclaration de ce traitement il était question de ne conserver les données relatives à un agent que 5 ans après son départ, la pratique est différente.

Il ressort ainsi de l'exploitation de la copie de la base de données remise à la délégation le jour du contrôle que nombre de données relatives à des agents dont le contrat a pris fin il y a plus de 5 ans sont conservées en base active. Cette situation est contraire à l'article 6-5 de la loi précitée qui interdit la conservation des données au-delà du temps nécessaire à la poursuite de la finalité du traitement.

En second lieu, la délégation de la commission a relevé un manque de rigueur dans le contrôle des mesures de sécurité des données mises en œuvre. En effet, il a été constaté que l'accès à l'application GESPER+ est possible à partir d'un simple nom d'utilisateur et sans que la saisie d'un mot de passe ne s'avère nécessaire.

Plus généralement, il est apparu qu'il n'existe pas au sein de la direction des espaces verts et de l'environnement de politique précise et contraignante en matière de sécurité des données (règles d'attribution, de robustesse et de renouvellement des mots de passe, verrouillage automatique des postes informatiques en cas d'inactivité prolongée, sensibilisation du personnel aux enjeux de confidentialité et de sécurité des données). Une telle situation n'est pas conforme à l'article 34 de la loi précitée qui fait obligation au responsable du traitement de mettre en œuvre toute mesure utile à la préservation de la sécurité des données ».

Le jour même du contrôle, le service était en mesure de remettre aux représentants de la commission **un document contenant un certain nombre de propositions de modifications**, confirmées quelques jours plus tard par courrier (dès le 28 novembre 2008).

Le 17 avril 2009, **la commission en donnait acte à la Ville** en écrivant que « … globalement, les modifications proposées [me] semblent appropriées pour éviter dorénavant que des informations ou commentaires excessifs ne figurent dans cette application ». Le courrier contient aussi l'annonce « de nouvelles missions de vérification auprès d'autres directions de la commune dans les prochains mois ».

[1] il s'agit bien entendu de la loi 78-17 modifiée par la loi du 6 août 2004

Son exécution nécessitant la passation d'un nouveau marché, la remise aux normes de GESPER n'a pu démarrer immédiatement et s'est déroulée durant l'année 2009. Elle a notamment comporté la suppression des fiches incriminées déjà citées, l'affichage systématique dans les zones de commentaire d'un message rappelant à l'utilisateur que les mentions y figurant devaient être directement liées à l'exécution du service. Les données relatives aux agents ayant quitté le service depuis plus de 5 ans sont désormais archivées, avec suppression des informations à caractère personnel. Une application indépendante (tableau EXCEL) a été mise en place pour le suivi des contraventions. Enfin l'accès à l'application nécessite désormais obligatoirement la saisie d'un mot de passe, et la formation des agents sur la sécurité des données a été renforcée.

La bonne mise en œuvre de ces modifications a été vérifiée par les rapporteurs.

Si les répercussions médiatiques de cette affaire ont été heureusement limitées, elle a fait apparaître **la nécessité d'un audit de fond sur les traitements et fichiers informatiques**, au-delà du travail accompli quotidiennement par le correspondant CNIL depuis 2006.

1.2. Les limites du sujet : fichiers manuels et archives

Le travail effectué et retracé dans le présent rapport comporte par construction des limites qu'il est important de définir.

1.2.1. Fichiers et documents manuels

La législation et la réglementation que la CNIL a pour vocation de faire respecter essentiellement les données personnelles informatisées et les traitements dont celles-ci font l'objet. Mais le droit à la protection de ces données englobe également les fichiers et dossiers « papier » que ceux-ci soient le résultat d'un traitement informatisé ou non. S'ils n'étaient pas inclus dans la loi de 1978 ils l'ont été dans celle de 2004, et depuis 2007 les traitements manuels doivent être conformes aux obligations suivantes :

- régularité de la collecte (article 6 de la loi 78-17)
- consentement obligatoire (article 7 de la loi 78-17)
- certaines informations sont interdites (origine raciale ou ethnique, opinions politiques philosophiques ou religieuses, appartenance syndicale, données afférentes à la santé, aux orientations sexuelles…)

Il faut noter aussi que si les fichiers manuels sont dispensés de déclaration (à ce titre ils n'intéressent donc pas notre correspondant CNIL) ils sont depuis 2004 inclus dans le périmètre de la loi et soumis à un régime d'autorisation s'ils présentent un risque pour les libertés fondamentales, s'ils utilisent des données sensibles, s'ils sont relatifs à des poursuites ou des condamnations, s'ils utilisent les numéros du répertoire national d'identification des personnes physiques (le numéro « SS »).

Les rapporteurs n'ont pas étudié de tels fichiers, pour la raison simple que ceux-ci ont a priori disparu en tant qu'outils de travail depuis plusieurs années ; ils n'en ont par ailleurs pas rencontré lors de leurs échanges avec les services, de la DRH notamment, où ceux-ci étaient très utilisés autrefois et ont survécu assez longtemps en parallèle à l'informatisation des traitements. Mais il ne peut être absolument exclu que subsistent ici où là de tels documents dont leurs détenteurs peuvent en toute bonne foi supposer qu'ils échappent à toute contrainte légale.

1.2.2. La question des archives

L'activité de l'administration aboutit à une production de documents qui pour une part sont dépourvus d'intérêt scientifique, statistique ou historique et doivent être détruits (code du patrimoine, article L 212-4) et pour les autres ont vocation à être déposés dans les services d'archives.

Pour les services de la Ville et du Département, ce sont les Archives de Paris qui donnent le « feu vert » à la destruction des documents rentrant dans la première catégorie, et sont dépositaires de ceux rentrant dans la seconde. Des correspondants, dans les différents services, sont en charge des modalités pratiques de ces dépôts, qui ont été organisés depuis l'origine pour recevoir des documents « papier ».

Le sujet général de l'archivage a été récemment (26 mars 2010) abordé lors d'une réunion du comité de direction des services, où a été entériné un plan d'action pour la gestion des archives.

Le thème particulier de l'archivage numérique y a été évoqué à travers le concept de l'archivage dématérialisé ; en réalité, il faut distinguer deux notions différentes :

- **la numérisation des archives sur support papier**, comme instrument de conservation ; cette perspective est a priori exclue du présent rapport,
- **le devenir des informations numérisées** – qui peut aboutir à un archivage au moins partiel des fichiers et documents issus d'applications comportant des données nominatives ; la question posée est celle des modalités du suivi, d'anonymisation et de conservation – ou non – au-delà de la durée d'utilisation.

On verra qu'il s'agit d'un domaine dans lequel de gros progrès restent encore à faire.

2. LES REGLES EN VIGUEUR

2.1. Le droit applicable à la Ville et au Département : cadre légal, principes généraux et textes particuliers

2.1.1. Le cadre légal d'ensemble et la CNIL

Celui-ci est composé de plusieurs textes : tout d'abord et principalement la loi 78-17 du 6 janvier 1978, modifiée par la loi du 6 août 2004, qui a établi les bases de l'ensemble, la loi 2004-575 du 21 juin 2004 sur la confiance dans l'économie numérique, plusieurs directives communautaires, et même des conventions internationales. De nombreux textes contiennent par ailleurs des dispositions ponctuelles relatives au sujet. Enfin il faut savoir que la commission nationale informatique et libertés (CNIL) a été créée par la loi de 1978.

Cette loi pose le fondement de la protection des données à caractère personnel dans les traitements informatiques mis en œuvre sur le territoire français. Les modifications intervenues dans le cadre de la loi du 6 août 2004 concernaient notamment les obligations des détenteurs de fichiers, qui ont été allégées et précisées, tandis que les pouvoirs de la CNIL en ce qui concerne les investigations sur place et les sanctions étaient renforcés. Cet organisme a vu son rôle et ses moyens se renforcer au fil du temps, **il emploie aujourd'hui plus de 120 agents (contre 57 en 1995) et devrait réaliser plus de 300 contrôles de terrain en 2010**. Autorité administrative indépendante, la CNIL est composée d'un collège pluraliste de commissaires majoritairement élus par l'Assemblée nationale, le Sénat, le Conseil d'Etat et la Cour de cassation, la Cour des comptes et le Conseil économique et social. Elle met en œuvre une politique d'information auprès des professionnels et des citoyens, de contrôle des dossiers de déclaration, de visites sur place, généralement suite à des plaintes, et de répression ; celle-ci va de la mise en demeure jusqu'à la dénonciation au parquet, en passant par l'avertissement et la sanction financière. La Ville s'est dotée depuis 2006 d'un correspondant CNIL, sur le rôle et les attributions duquel on reviendra.

2.1.2. Les principes généraux du droit applicable

Les principes sont brièvement développés ci-après :

- **le principe de finalité** : il définit le lien entre les données et les traitements ; les données à caractère personnel ne peuvent être recueillies et traitées que « pour des finalités déterminées, explicites et légitimes » et leur utilisation ultérieure doit toujours être compatible avec ces finalités.
- **les données ne peuvent pas être conservées dans un fichier de façon illimitée** : la loi précise que « les données à caractère personnel sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ». L'indication de la durée de conservation doit figurer aussi bien dans les déclarations simplifiées, que dans les dispenses de déclaration et les autorisations uniques.

Il en résulte par exemple qu'en matière de gestion des ressources humaines des durées réglementaires très variables existent : « le temps nécessaire à l'établissement des bulletins de paye » pour le motif des absences ; cinq ans pour les évaluations et la notation ; pour les droits à pension, il n'y a aucune limite.

La conservation des données et documents présentant un intérêt historique qui les fait basculer dans la catégorie des archives pose par ailleurs le problème de la conservation de celles-ci, déjà évoqué supra.

- **les données personnelles ne peuvent être divulguées** : l'informatique ne doit pas porter atteinte à la vie privée.

- **les fichiers doivent être exploités en toute sécurité** : les responsables des traitements ont une obligation générale de sécurité, portant sur la confidentialité (cf. aussi le point précédent) et sur l'intégrité tant physique que de contenu, des données. La sécurité doit s'organiser à partir de la fiabilité des matériels et des logiciels ainsi que d'un ensemble de procédures permettant d'éviter les accidents matériels aussi bien que les atteintes volontaires (détournement, malveillance).

- **la nécessaire information des usagers sur leurs droits :**
  Il s'agit tout d'abord du **consentement** : les personnes intéressées doivent, tacitement ou non, consentir à l'utilisation de traitement les concernant (il existe cependant des exceptions, encadrées, à partir du moment où s'y opposent des « intérêts légitimes » généralement définis sur le plan légal).

- **le droit d'accès et de rectification** : il s'agit d'un des principes les plus importants.

  En effet, toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :

  - la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;
  - des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou catégories de destinataires auxquels les données sont communiquées ;
  - le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la CE ;
  - la communication sous forme accessible des données à caractère personnel qui la concernent ainsi que toute information disponible quant à l'origine de celle-ci ;
  - les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé.

Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Les demandes manifestement excessives peuvent être rejetées.

Corollaire de ce droit d'accès, toute personne peut exiger du responsable d'un traitement que le cas échéant les données qui la concernent soient rectifiées, complétées ou mises à jour ; **il est aussi possible de faire valoir un « droit d'opposition »** au recueil ou à la conservation et au traitement des données (sauf lorsque ceux-ci sont prévus par la loi) ; ce dernier droit trouve notamment à s'appliquer pour les fichiers d'organismes à vocation politique ou religieuse.

2.2. Les normes applicables à la Ville et au Département

2.2.1. Le principe de la déclaration

Sauf exceptions définies par la loi, tout fichier ou traitement nominatif doit faire l'objet d'une déclaration.

Parmi la liste des exceptions légales, celles qui sont susceptibles de concerner la Ville et le Département sont assez marginales : les archives à long terme, les registres d'information du public établis en application de dispositions législatives ou réglementaires, destinés exclusivement à l'information du public, et ouverts au public pour la consultation.

Enfin et surtout **la déclaration n'a pas à être faite, sauf pour certaines exceptions lorsque l'organisme s'est doté d'un correspondant**, comme c'est le cas de la Ville : ce point sera évoqué dans le développement consacré infra à ce correspondant.

2.2.2. Les normes s'appliquant à la Ville de Paris

La CNIL a élaboré un certain nombre de normes, dans divers domaines, qui permettent de simplifier les formalités de déclaration. Ces normes s'appliquent à des domaines déterminés ; sont définis les périmètres, les contenus (les données), les traitements, les destinataires et les droits des personnes concernées, et bien sûr les obligations de sécurité. Ces normes sont adoptées par délibération de l'organisme, elles ont bien entendu force obligatoire pour les acteurs concernés.

Les principales sont à ce jour les suivantes :

- la norme concernant **l'état civil** (délibération du 24 janvier 2004) concerne les données contenues dans les actes, leur traitement, les destinataires, la durée de conservation. On notera que le téléservice de demande d'actes a fait l'objet d'un texte particulier distinct en 2006.
- la gestion des demandes de validation des **attestations d'accueil des étrangers** : données relatives aux hébergements, aux personnes hébergées, définition des destinataires, prohibition des interconnexions, durée de conservation, sécurité … (délibération 2005-052 du 30 mars 2005).
- **les fichiers électoraux** : norme simplifiée n° 24 et n° 38 sur la base de délibérations au 15 septembre 1981 et du 26 avril 1994. Elles définissent notamment strictement les destinataires, pour éviter toute dérive à caractère politique.
- les tiers autorisés à bénéficier **d'informations sur les administrés** : la liste limitative a été dressée par la CNIL (Trésor public, justice, autres administrations et organismes sociaux…).
- **le cadastre** (norme simplifiée n° 44) : cette norme vise le contenu et la consultation du cadastre ainsi que les destinataires.
- **la fiscalité directe locale** (norme simplifiée n° 45). La norme vise l'utilisation des traitements mis en œuvre à partir du rôle des impôts directs locaux : nature des informations, finalités, destinataires, conservation, sécurité.
- **des taxes diverses** : droits de voirie, droits de place de taxis… (délibération 80-18 du 6 mai 1980).

- la dématérialisation du **contrôle de légalité** (délibération 2006-056 du 2 mars 2006) : il s'agit d'une dispense de déclaration à partir du moment où sont respectées un certain nombre d'obligations (sécurité, destinataires, conservation…).

- **la gestion des élèves**, de la maternelle aux établissements du second degré, fait l'objet de plusieurs normes :
  - n° 33 pour les écoles maternelles et élémentaires : données, finalité des traitements, établissement de statistiques, destinataires… ; la norme n° 27 vise de manière parallèle les services offerts : restauration scolaire, activités périscolaires. La norme n° 29 vise de son côté l'enseignement secondaire.

Il existe aussi une norme (délibération du 22 avril 1999) pour les bibliothèques qui précise les données, les traitements et les destinataires, ainsi qu'une durée de conservation particulièrement courte (un an à compter de la fin de chaque prêt, quatre mois pour l'objet lui-même).

L'ensemble de ces normes, qui a vocation à s'enrichir dans l'avenir, constitue d'ores et déjà un « corpus » réglementaire non négligeable qui s'impose à la Ville et doit notamment être pris en considération lorsque de nouvelles applications, ou des refontes d'applications anciennes, interviennent dans ces domaines.

On notera enfin que la CNIL peut être compétente pour les installations de vidéosurveillance, à partir du moment où les images recueillies permettent de constituer des fichiers nominatifs (sur un plan général, l'installation à Paris d'un système de vidéosurveillance relève d'un régime d'autorisation du préfet de Police).

2.3. L'organisation Ville : le correspondant informatique et libertés (CIL)

Depuis 2006, la Ville s'est dotée d'un correspondant informatique et libertés (CIL), comme environ 1 800 entreprises ou administrations.

Le premier effet de la désignation d'un CIL est d'éviter la transmission à la CNIL de la plupart des demandes d'autorisation du traitement.

Toutefois, la CNIL garde le contrôle sur certaines données et applications (article 25 de la loi 1978-17) ; il faut citer :

- les traitements réalisés par l'INSEE
- ceux nécessaires à la recherche en matière de santé
- ceux justifiés par l'intérêt public (données dites « sensibles »)
- les données génétiques
- les traitements contenant des informations susceptibles d'exclure des personnes du bénéfice d'un droit
- les traitements réalisant des interconnexions entre fichiers aux finalités différentes, utilisant le numéro SS
- les fichiers comprenant des appréciations sur les difficultés sociales des personnes
- et enfin les données biométriques.

Si pour la Ville le premier avantage est d'éviter un ensemble de formalités administratives pesantes, il faut bien voir que le correspondant CNIL est en charge de faire respecter la législation et la réglementation ; son rôle est officiel et a été acté par une notification auprès de la CNIL ; il était chargé lors de sa nomination d'auditer la situation existante et de mettre en place les dispositifs de procédures permettant d'exercer sa mission.

La réglementation (décret 5005-1309 du 20 octobre 2005) prévoit notamment que le CIL « exerce sa mission directement **auprès du responsable des traitements**[2] » et que celui-ci doit lui fournir tous les éléments permettant d'établir et d'actualiser la liste des traitements automatisés mis en œuvre. Le CIL actualise et entretient cette liste, veille sur un plan général au respect des obligations légales, est consulté préalablement à la mise en œuvre de tout nouveau traitement.

C'est le CIL qui reçoit les réclamations relatives aux traitements figurant sur la liste ; en cas d'irrégularité, il en informe le responsable et peut saisir la CNIL. Enfin il doit établir un bilan annuel, qui est présenté au responsable des traitements (notre CIL estime que la valeur ajoutée d'un tel document est faible et n'en réalise pas, mais communique un rapport mensuel au Secrétariat Général).

La CNIL, enfin, ne dispose pas d'un véritable droit d'agrément (et donc d'une possibilité de refus de désignation) sur les correspondants. Elle demande toutefois, en prenant acte de la désignation, que celui-ci justifie, par son curriculum vitae, **d'une compétence établie en matière juridique et informatique**. Elle est aussi attentive au positionnement du correspondant dans l'organigramme, celui-ci devant à la fois justifier d'une autonomie totale dans l'exercice de ses fonctions, et ne pas être le responsable des traitements (directement ou par délégation) ; par contre, le CIL « exerce sa mission directement auprès du responsable des traitements ».

Ces conditions sont réunies dans le cas de la Ville dans la mesure où notre correspondant, même s'il est rattaché administrativement à la DSTI et apparaît dans son organigramme, est clairement identifié comme tel et assume de manière indépendante sa mission, en détenant la signature dans l'ensemble du domaine en cause. Il faut noter qu'à la création de la fonction en 2006 qui avait fait l'objet d'une information officielle auprès du Comité technique paritaire central, il était rattaché au Secrétariat Général.

Sa mise en place avait fait l'objet d'une présentation officielle à l'ensemble des directeurs de la Ville ; celle-ci avait été suivie de réunions avec des sous-directeurs et des CIT. L'ensemble de la documentation relative au sujet avait été mise en ligne sur le site du Secrétariat Général.

Depuis lors, elle en a été retirée et il faut désormais se reporter sur celui de la DSTI. Malgré ses demandes, le CIL ne dispose pas d'un espace individualisé sur l'Intranet municipal, non plus que sur le site « Paris.fr ». Ces points devraient être corrigés (cf. les propositions des rapporteurs…).

[2] la désignation officielle « responsable des traitements » ne doit pas être confondue avec la fonction opérationnelle « responsable des traitements informatiques » : **il s'agit d'une appellation juridique qui désigne dans les faits le Maire de Paris**

2.4. Réalisations et activités du CIL depuis 2006

Actuellement la première activité du correspondant demeure bien entendu de recevoir les déclarations de fichiers contenant des données personnelles. Deux cas de figure se présentent : soit l'application n'a pas encore fait l'objet de déclaration et ses gestionnaires peuvent utiliser un formulaire disponible en ligne ; soit il s'agit d'une modification et il faut simplement envisager des compléments.

Lors de sa nomination, le CIL a récupéré le fichier de la CNIL. Celui-ci était en « mode texte » et a dû être intégralement repris en saisie manuelle pour constituer une véritable base de données, avec le concours de la DSTI.

Ce travail effectué pour chaque application recensée a fait l'objet d'une fiche reprenant tous les éléments détenus par la CNIL.

Ces fiches ont été adressées aux CIT des directions pour vérification et mise à jour ; l'opération s'est bien passée et a permis de nouer les premiers contacts, complétés ensuite par des interventions dans des réunions avec les CIT, et lors des séances du comité opérationnel des utilisateurs du système d'information (COSI).

Les documents nécessaires sont maintenant disponibles sur le site de la DSTI.

En pratique, le correspondant recommande de rentrer en contact avec lui pour examiner les dossiers au cas par cas, et cet échange est quasi systématique pour toutes les premières déclarations.

Chaque année une soixantaine de déclarations nouvelles ou modifications significatives sont ainsi traitées.

Lorsque le fichier ou l'application considérée ne rentrent pas dans le champ de compétence de notre correspondant, celui-ci instruit le dossier et assure la transmission à la CNIL. Depuis sa mise en place en 2006, trois dossiers ont fait l'objet d'une telle procédure : à la DVD pour l'utilisation du NIR (n° de SS…), un pour Vélib à la DPE, et à la DASCO pour l'application « Facil Famille ».

Le correspondant gère, pour chaque direction, la liste des fichiers et traitements.

Le tableau ci-après récapitule l'état du fichier en mars 2010 :

Directions	Nombre de fichiers	Travaux en cours
DAC	37	
DAJ	3	
DALIAT	16	mise à jour en cours
DASCO	51	
DASES	92	dossier « SALSA » en instruction
DDATC	42	
DDEE	4	
DF	13	
DFDE	10	
DICOM	20	
DJS	19	
DLH	21	
DPA	8	
DPE	38	
IG	0	application temporaire supprimée
DPJEV	16	
DPP	9	
DRH	39	
DSTI	23	
DU	23	
DVD	30	
CASVP	73	

On notera que notre CIL a également dans ses fichiers les applications concernées du CASVP. **Cette situation devrait être réglée sur le plan administratif (aucune décision n'a été prise officiellement lui confiant la responsabilité de CIL pour cet organisme).**

Notre correspondant s'efforce d'intervenir **le plus en amont possible** lors de la mise en place d'applications nouvelles dont certains aspects vont impacter des données personnelles. Il est en effet évidemment plus facile sur le plan technique d'anticiper la prise en compte des exigences légales sur la protection et le traitement des données que d'apporter après coup des corrections et des sécurités non mises en place au départ. Son intervention **s'inscrit donc dès la phase de préparation des nouveaux projets** lors de la rédaction des clauses techniques qui imposent le moment venu aux prestataires de prendre en compte la protection des données personnelles.

Toujours en interne, le correspondant est évidemment amené à intervenir en appui auprès des services qui rencontrent des difficultés avec des agents de la Ville ou avec des usagers. Les cas, rares, lui sont systématiquement transmis ; il a par exemple été signalé le cas d'une personne ayant quitté la capitale et qui se plaignait de continuer à recevoir le journal « A Paris ».

Enfin, à l'extérieur, notre correspondant entretient des liens étroits avec la CNIL dont il consulte les services en cas de doute et des contacts réguliers avec un certain nombre de ses homologues, notamment à travers l'Association Française des Correspondants pour la Protection des Données Personnelles (AFCDP). Les rapporteurs ont ainsi pu bénéficier d'entretiens très intéressants (cf. chapitre 5).

En conclusion, un gros effort a été réalisé depuis 2006 de mise en place du dispositif du correspondant, et la Ville est dotée aujourd'hui d'une structure fonctionnelle de bon niveau. On verra toutefois en étudiant les réponses au questionnaire que les attentes des services sont encore très importantes, en terme de documentation et de formation notamment, et justifient un effort nouveau de développement.

* *
*

3. LA SITUATION VUE PAR LA DSTI

3.1. L'activité de la direction pour son compte propre

Il existe en pratique très peu de fichiers traitant de données personnelles propres à la DSTI ; ces fichiers sont recensés et ont fait l'objet d'une déclaration CNIL (ou CIL) si nécessaire. Dans la majeure partie des cas, ils bénéficient d'une déclaration simplifiée dans la mesure où ils correspondent à des situations de gestion « standard ».

Par exemple, les coordonnées personnelles enregistrées à travers l'application « ZenWorks » sont destinées à permettre la télédistribution automatisée des mises à jour systèmes sur l'ensemble des postes de travail de la Ville.

Il faut noter que la DSTI ne possède pas de « correspondant informatique et télécom » (CIT) au même titre que l'ensemble des directions. D'autre part, **il existe bien un responsable général de la sécurité**, mais il n'est pas le référent dûment mandaté pour prendre en charge l'ensemble des questions spécifiquement liées à la protection des données personnelles.

Il réside vraisemblablement et collectivement dans les esprits une confusion avec le rôle du CIL qui est rattaché administrativement au DSTI. Or le CIL de par son statut ne doit en aucun cas assumer ce genre de responsabilités.

La vigilance sur ces questions de protection des données personnelles est donc complètement éclatée au niveau des différents pôles techniques de la DSTI.

Dans ce contexte, la création d'un référent CIL distinct du CIL lui-même et spécifique à la DSTI apparaît une nécessité ; cette fonction pourrait être parfaitement remplie par le responsable sécurité de la DSTI, dans la mesure des moyens et de la disponibilité dont il dispose.

3.2. L'exploitation pour compte de tiers

Cette partie est beaucoup plus complexe à appréhender, dans la mesure où elle est directement impactée par le principe d'organisation adopté par la Ville en 2002 qui stipule une séparation forte des responsabilités entre la maîtrise d'œuvre (MOE) et la maîtrise d'ouvrage (MOA) : chacune des deux parties peut avoir la tentation d'imaginer que c'est l'autre qui prend en charge certaines tâches liées à la protection des données personnelles (fichiers, logiciels, gestion des comptes, pistes d'audit, etc.).

Dans la pratique cela se traduit par le fait que si **les risques sont en général bien identifiés lors de la phase projet**, il n'existe pas toujours en face un plan d'action adéquat pour garantir la même sécurité en phase d'exploitation et de maintenance (problème du turn over des agents et de la sous-traitance). A titre d'exemple, **la DSTI reçoit très rarement une copie de l'enregistrement de la déclaration CNIL avant la mise en exploitation d'une application traitant des données personnelles**.

Néanmoins les risques s'amplifient continuellement sous la poussée conjuguée du progrès technologique (ex. : utilisation de logiciels libres, ouverture grandissante des réseaux informatiques à travers les terminaux portables de toute nature, arrivée d'une population jeune complètement familiarisée avec l'informatique) et de l'extension des télé-services à l'usager, avec notamment le paiement « en ligne » par quelque moyen que ce soit (carte de crédit, téléphone portable, pass, etc.).

Le cas des télé-services (pour la mise en œuvre desquels l'avis préalable de la CNIL est obligatoire) va être réexaminé suite à la publication du dernier décret (2 fév. 2010) qui indique clairement l'entière responsabilité de la MOA dans ce domaine, avec la description des règles du référentiel général de sécurité.

Face à cette situation, la DSTI a entrepris plusieurs actions :

Les développements figurant ci-dessous ont été occultés conformément aux dispositions de la loi du 17 juillet 1978 relative à l'accès aux documents administratifs.

……
……
……
……
……
……
……
……..

Il ne faut cependant pas, par ailleurs, imaginer une surveillance prochaine des services de fichiers mis à disposition des directions.

La DSTI a bien testé une solution logicielle pour essayer de détecter les fichiers qui pourraient contenir des données personnelles : les résultats ont été décevants, dans la mesure où l'outil ressortait trop de cas « faux-positifs ». Dans l'immédiat, aucune solution de rechange n'est envisagée. D'une manière générale un véritable contrôle interne au sein de la DSTI en tant qu'opérateur pour compte de tiers n'existe pas : les contrôles sont assurés de façon très déconcentrée au cas par cas, sans documentation précise à ce sujet, par une population de techniciens au demeurant bien informés de la problématique.

Enfin, s'agissant **de la purge des historiques et de l'archivage des données personnelles**, cet aspect n'est pratiquement pas traité : beaucoup de cahiers des charges ne mentionnent même pas cette partie du projet lors de leur lancement, chacun s'accordant à considérer qu'elle sera traitée ultérieurement lorsque l'exploitation aura atteint son régime de croisière.

4. LES RESULTATS DU QUESTIONNAIRE

Le questionnaire est reproduit intégralement en annexe 1 accompagné du dépouillement d'ensemble des résultats.

Le document était organisé en trois parties :

- une première consacrée à l'organisation générale de la direction pour le contrôle de la bonne application des règles relatives au respect du droit à la protection des données personnelles,
- une seconde intitulée « le recensement des fichiers et des traitements – l'analyse des risques »,
- la troisième relative à l'archivage et à la destruction des fichiers.

Un document synthétique d'une page, extrait des dossiers disponibles dans les documents consacrés au sujet sur les pages du site de la DSTI consacrées au CIL, rappelait le cadre général défini par la loi.

Les résultats qui suivent et les commentaires intègrent bien évidemment les différents entretiens menés avec les directions qui ont semblé aux rapporteurs les plus exposées compte tenu de leur activité : DRH (données personnelles des agents de la Ville), DFPE, DASES, DASCO, DJS, DICOM (données personnelles des usagers et des Parisiens) et bien entendu DSTI.

4.1. L'organisation générale dans la direction

4.1.1. L'organisation administrative

Une première batterie de questions portait sur les points suivants :

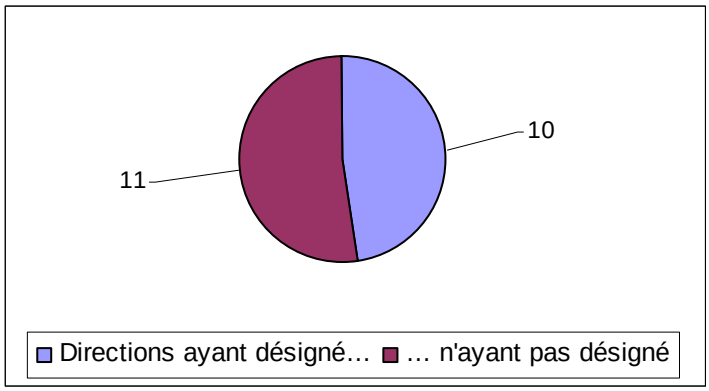
- **un agent de la direction a-t-il été officiellement désigné** en tant que responsable des questions liées à la protection des données personnelles ?

- dans l'affirmative, appartient il à la catégorie A, B ou C ? Sa formation est-elle plutôt administrative, plutôt à dominante informatique, ou autre ? Quel est son rattachement hiérarchique (direction générale, ou sous-direction, un bureau…) ; depuis quand exerce-t-il cette fonction : avant 2006, depuis 2006, plus récemment (depuis 2009) ?

- les items suivants sont relatifs à son **niveau d'information** : a-t-il été informé de la nomination d'un correspondant informatique et liberté à la Ville, d'une présentation de ses missions et responsabilités, dispose t-il d'une documentation « claire, suffisante et accessible » (et dans la négative, quelles sont ses attentes), et enfin a-t-il bénéficié d'une formation spécifique dispensée par un partenaire extérieur ?

* *

*



Dix directions ont désigné « officiellement » un responsable, onze non ; **la situation est donc très partagée**. Il faut noter qu'il n'a pas été trouvé trace de décision à caractère administratif confiant cette responsabilité à une personne désignée (par exemple dans le cadre d'une délégation de signature). Il faut donc interpréter les réponses positives comme la simple reconnaissance de la vocation des intéressés à traiter le sujet ; les réponses négatives ne signifient pas que personne ne s'en occupe, mais qu'aucune formalisation n'est jamais intervenue.

Les rapporteurs estiment qu'il est indispensable de désigner, dans chaque direction, une personne « correspondant officiel » de notre CIL (il faut d'ailleurs signaler que l'envoi du questionnaire aux directions a dans plusieurs cas entraîné une désignation rapide du référent pour s'occuper du sujet ; c'est par exemple le cas de la DFPE : « non, mais le CIT va assurer ce rôle »).

Si dans certaines directions l'absence de responsable officiel n'empêche pas une centralisation de fait des dossiers auprès d'une personne non officiellement désignée, dans d'autres la situation est apparue plus préoccupante, chaque responsable d'application ou de fichier étant réputé déclarer de son côté, sans aucune coordination au niveau de la direction.

L'ancienneté dans la fonction est moyenne (très peu d'agents l'exerçaient avant 2006).

A deux exceptions près (un B, un C) **le responsable désigné est de catégorie A**, et d'une formation à dominante informatique, ou mixte (informatique et administrative) ; seule la DPE a choisi de désigner le chef du bureau des affaires juridiques, en collège avec le CIT. A la DICOM, c'est la directrice adjointe qui assure cette responsabilité. Le choix, dans ce cas, s'explique autant par la sensibilité des sujets traités que par le fait que le CIT de la direction n'a pas forcément connaissance de l'ensemble des fichiers ou traitements de la direction susceptibles de contenir des données personnelles.

D'une manière générale, les CIT sont impliqués et en première ligne face à la problématique et la protection des données personnelles. En effet, même si une autre personne est désignée pour en être responsable, ce sont eux qui maîtrisent les aspects techniques du sujet et ont a priori la meilleure connaissance des applications et fichiers de leur direction.

Le « maillage » qu'ils constituent s'étend naturellement aux responsables des projets et aux agents gérant au quotidien les informations contenues dans les fichiers.

Nombreux sont toutefois les CIT qui ont fait part aux rapporteurs de leur **hésitation à assumer une fonction dont ils maîtrisent bien les données techniques mais pas les aspects juridiques[3].**

La réponse à apporter est triple :

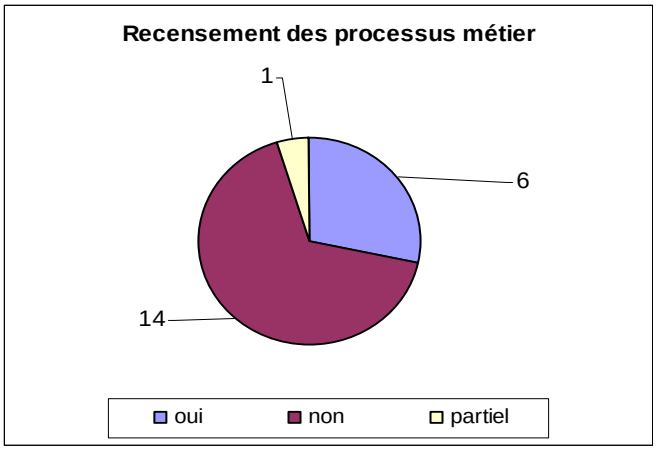
- **inciter comme à la DPE les CIT à se rapprocher de leurs collègues juristes** de leur direction ; toutefois toutes les directions ne disposent pas en interne de telles compétences, **même si la mise en place d'un véritable binôme représente la meilleure organisation possible,**
- **les inviter à prendre l'attache aussi souvent que nécessaire du CIL** qui peut leur apporter tous les conseils nécessaires et les aider à instruire les cas complexes,
- **leur offrir une formation juridique minimale** sur le sujet, régulièrement actualisée, en s'appuyant sur le CIL et éventuellement des prestataires extérieurs.

Le niveau d'information des responsables est variable. **Le CIL est connu de tous. Mais seule une minorité** (5 réponses) **estime bénéficier d'une documentation suffisante**, deux directions (DPE et DDATC) ont bénéficié d'une formation spécifique. Cinq personnes seulement signalent avoir bénéficié d'une présentation des missions du CIL : ce faible chiffre s'explique aussi par le « turn over » des responsables. Le CIL devrait réunir ses correspondants au moins une fois par an.

4.1.2. Les risques liés aux métiers de la direction, le contrôle interne et les relations avec le correspondant informatique et liberté

La première question portait sur le recensement des « processus métier » : « Existe-t-il un recensement des principaux processus métier dans lesquels la création et l'utilisation de fichiers contenant des données personnelles intervient ?».

[3] ce qu'exprime bien l'un d'entre eux :
« La proposition de désigner le CIT d'une direction comme référent CIL doit être assortie de précautions, faute de quoi un rejet des intéressés n'est pas à écarter.
Le « CIT-référent CIL » au sein d'une direction ne doit pas subir une sorte de « déconcentration » des tâches et responsabilités primitivement dévolues au CIL : il n'a pas la disponibilité suffisante, ni les compétences, et ce rôle n'entrerait pas véritablement dans son cœur de métier.
Par contre, il a vocation à connaître le système d'information propre à sa direction : il peut donc relayer utilement les actions impulsées par le CIL (formation, bilan annuel, déclarations) au sein de la structure et guider les utilisateurs dans leur démarche dans ce domaine particulier.
Le principe de l'inclure dans une structure de coresponsabilité avec une cellule juridique, si cette dernière existe, est très bien ressenti ».
Le CIL pour sa part estime (à juste titre) dans sa réponse provisoire que « le CIT… ne peut se substituer au CIL, ne serait ce que par sa dépendance hiérarchique. Il ne peut être q'un point d'accès vers le CIL ou pour le CIL ».



Six directions seulement se sont livrées à cet exercice, et une « partiellement ». Parmi celles qui ont procédé à cette analyse, on trouve la DRH, évidemment très concernée par le sujet, ainsi que la DSTI, pour des raisons fonctionnelles.

Les réponses possibles renvoient d'ailleurs en général à l'appropriation et au suivi de la liste que tient à jour, pour chaque direction, le CIL. Aucune véritable évaluation des risques n'a jamais été entreprise, à l'exception de la DFPE. L'explication réside dans le fait que les services raisonnent par famille d'application, **en fonction de données techniques, mais sans accorder une place privilégiée aux caractéristiques des contenus.**

A la question suivante **« l'encadrement de la direction a-t-il connaissance des règles de base à appliquer en matière de protection des données personnelles », les trois quarts des directions répondent par l'affirmative**.

Toutefois, la question suivante révèle les limites de la culture des services sur le sujet : à la question « l'encadrement de la direction a-t-il connaissance des responsabilités et des sanctions pénales, financières et administratives encourues en cas d'infraction ? », un quart seulement répondent par l'affirmative.

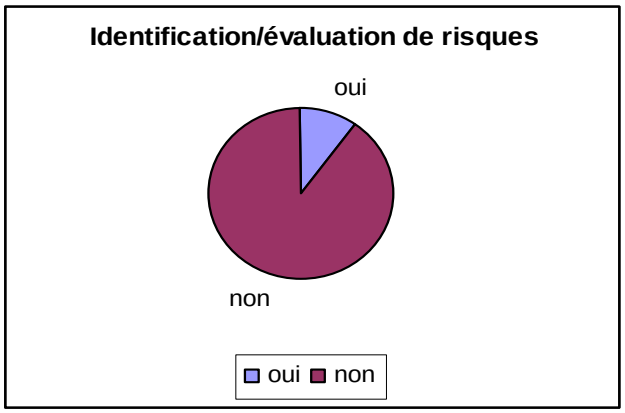
DRH et DSTI se distinguent aux côtés de la DFPE par leur connaissance du sujet, mais d'une manière générale les directions n'ont qu'une idée assez vague du régime de sanctions applicable en la matière.

L'évaluation des risques propres aux directions

Les rapporteurs ont cherché à cerner les risques spécifiques aux différentes directions, en les interrogeant d'abord sur l'existence d'une évaluation de ceux-ci, dans chaque service[4].

Pour l'ensemble des processus métiers faisant appel au traitement de données personnelles, existe-t-il une **identification et une évaluation des risques liés** ?

[4] Le CIL signale pour sa part que « l'évaluation des risques est d'autant plus faible que [les directions] comportent des unités décentralisées ».



Seules deux directions, la DRH et la DFPE, ont effectué une telle démarche.

Le tableau suivant du questionnaire incitait les services à s'interroger sur les risques particuliers que leur activité leur faisait encourir.

rang	risques
	dénonciation par un agent de la présence de données personnelles non autorisées dans les fichiers de la Ville
	dénonciation par un usager des téléservices sur www.paris.fr de la présence de données personnelles non autorisées dans les fichiers de la Ville
	copie de fichiers à des fins frauduleuses par un tiers extérieur
	perte de fichiers durant les phases de transport
②	**accès non-autorisé à des données personnelles et sensibles sur un agent**
②	**accès non-autorisé à des données personnelles et sensibles sur un usager**
①	**plainte en justice d'un agent pour exploitation non-autorisée de données personnelles**
	plainte en justice d'un usager pour exploitation non-autorisée de données personnelles
	autres :

Certaines directions n'ont pas procédé à une hiérarchisation (rang 1, 2, etc), d'autres ont fait des réponses incomplètes, et d'autres enfin ont répondu par la mention « fort » ou « faible » ce qui rend les réponses difficilement exploitables. **D'une manière générale ce sont les accès non autorisés qui sont les plus fréquemment cités en premier rang ainsi que les plaintes en justice et les dénonciations.**

La copie ou la perte de fichiers est moins redoutée à l'exception du cas particulier de la DICOM qui fait sous traiter des fichiers à l'extérieur.

L'activité de contrôle interne dans les directions

Les rapporteurs souhaitaient savoir si des procédures de contrôle interne pour assurer la maîtrise des risques liés à la protection des données personnelles avaient été mises en place, et dans l'affirmative si elles étaient documentées, validées avec le CIL, connues des personnes concernées, et si elles faisaient l'objet d'un bilan annuel.

Deux directions seulement ont répondu par l'affirmative : la DRH et la DSTI.

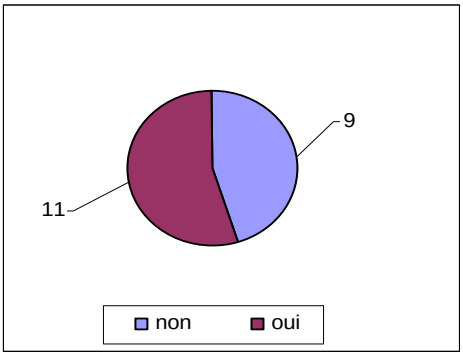
Pour la DSTI, ces procédures s'inscrivent dans les consignes générales de sécurité qui sont accessibles sur l'intranet de la direction.

Celles-ci contiennent aussi bien un rappel de la législation sur les données personnelles (distinct de l'onglet réservé au CIL) que des thèmes divers liés à la sécurité (par exemple sur la gestion sécurisée des mots de passe) enrichis régulièrement par l'actualité technique. On trouve également un document de base, la « charte du bon usage des ressources informatiques et des systèmes d'information de la Ville et du Département de Paris », qui contient des consignes et des références sur la protection des données personnelles. Ces documents indispensables ne relèvent toutefois pas d'une procédure de contrôle interne au sens strict et sont plutôt des guides pratiques à l'usage des utilisateurs, au demeurant bien adaptés à leur objet.

A la DRH, les procédures de contrôle interne portent sur l'habilitation et le suivi des personnes habilitées à faire des extractions et établir des requêtes portant sur des données nominatives. Ces procédures s'inscrivent dans une longue tradition de protection des données relatives aux agents. Il faut aussi observer que la DRH dispose d'un petit journal « RH infos » par lequel elle informe le réseau des gestionnaires et professionnels de ressources humaines de la Ville. Ce journal pourrait être utilisé pour diffuser des recommandations et des informations sur le sujet de la protection des données personnelles, en tant que de besoin.

Les relations avec le correspondant « informatique et libertés »

« L'agent en charge de la protection des données personnelles a-t-il déjà eu l'occasion de traiter des dossiers avec le CIL ? ».



Un peu plus de la moitié des directions déclarent avoir déjà traité un dossier avec le CIL. Des entretiens avec les services, il résulte que ce chiffre est en fait sous estimé. Certains services considèrent que la simple déclaration d'un fichier au CIL n'est pas un « traitement de dossier ». D'autres comme la DJS ayant répondu ne pas avoir de correspondant chargé du dossier de la protection des données personnelles ont répondu par la négative à cette question, alors que l'entretien a révélé des contacts suivis et fructueux avec le CIL.

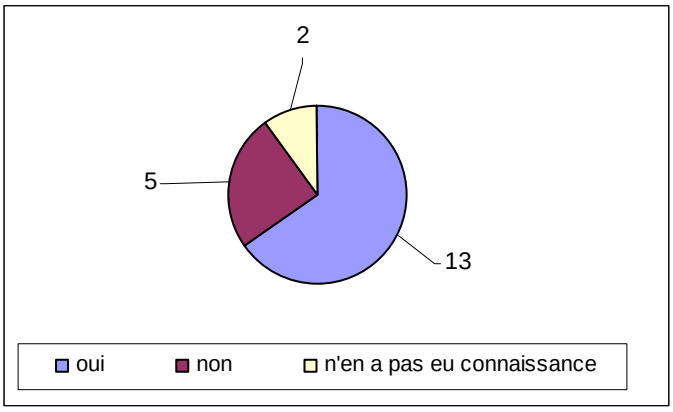
Pour un autre au moins (la DICOM) la réponse négative s'explique par le fait que les contacts avec le CIL n'étaient pas, au moins jusqu'à une date récente, centralisés par une seule personne, mais à l'initiative des services.

La plupart des directions entretiennent en réalité des relations avec le correspondant, ce que du reste confirme formellement ce dernier.

Il était ensuite demandé si « le principe de simple déclaration par courriel auprès du CIL satisfaisait [les directions] ».

La quasi-totalité des directions ont répondu par l'affirmative, à l'exception d'une direction qui « n'y a pas eu recours mais trouve la formule intéressante dans son principe » (la DPVI).

A la question **« les supports pédagogiques diffusés par le CIL sont-ils adaptés à vos attentes ? »,** les réponses sont plus contrastées.



Si en effet **une majorité s'en déclare satisfaite**, une minorité non négligeable les conteste, deux directions la DAC et la DJS signalent « n'en avoir pas eu connaissance ». Le CIL a signalé aux rapporteurs que le responsable informatique de la DAC venait d'être nommé, et qu'il y avait toujours eu des contacts avec la DJS (cf. sa réponse au rapport provisoire).

Ces supports pédagogiques sont constitués, comme il a déjà été signalé, par une série de fiches disponibles sur l'intranet de la DSTI. Il faut pour les trouver ouvrir l'onglet « documentation » et cliquer sur la rubrique « CNIL CADA » pour accéder à une fiche qui renvoie à une série de documents (cf. annexe 2).

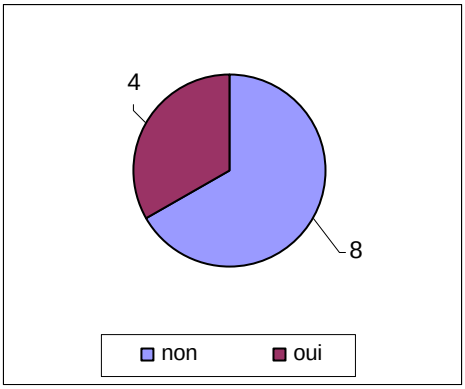
Plusieurs directions regrettent de n'avoir « rien reçu » (donc en fait ignoraient l'existence de cette rubrique). La DASES pour sa part a émis un ensemble de suggestions qui sont reproduites ci-après :

« Ces supports sont sans doute ceux que l'on peut trouver sur l'intranet de la DSTI. 25 % d'entre eux traitent de la CADA. Le reste est composé de 4 schémas méthodologiques sans commentaire, d'une fiche de synthèse relative aux obligations et de 2 fiches méthodologiques. Ces documents sont les premiers éléments d'une boîte à outils. Cependant ils ne peuvent pas constituer un support pédagogique puisqu'ils ne sont pas mis en cohérence dans un document structuré susceptible de restituer une approche métier des actions à mener dans le domaine.

Un guide comparable dans sa structure au « guide d'analyse des offres » de la DAJ ou encore un vade-mecum reprenant l'ensemble des procédures possibles avec les actions à mener, accompagnées de directives et/ou de recommandations ainsi que des exemples de cas pratiques, serait utile à l'exercice de cette nouvelle fonction au sein d'une direction d'envergure telle que la DASES ».

Tout en retenant cette demande dans son principe, on notera à nouveau (cette observation a déjà été faite) que lors de la mise en place du CIL en 2006 **un ensemble documentaire beaucoup plus complet** avait été mis en ligne, à l'époque sur le site du Secrétariat général.

Cette rubrique comprenait une dernière question : « l'agent en charge de la protection des données personnelles dispose-t-il en retour des informations qui lui paraissent nécessaires ? ».



A peine plus de la moitié des directions ont répondu, majoritairement par la négative. Les entretiens ont fait apparaître que le CIL n'envoyait pas systématiquement de retour régulier des fichiers aux directions, sauf exception (la DRH par exemple). Ce point peut être facilement corrigé, à partir du moment surtout où l'ensemble du réseau de ses correspondants sera parfaitement identifié et officialisé.

4.2. Le recensement des fichiers et des traitements – l'analyse des risques

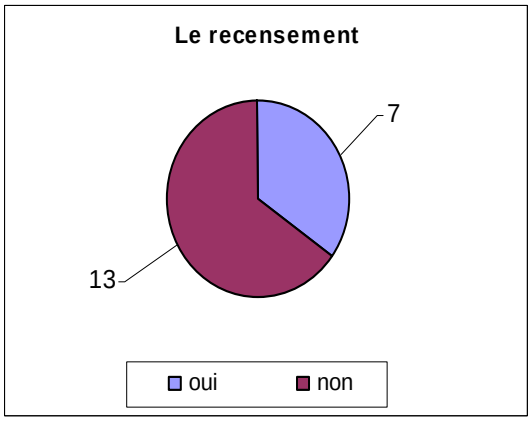
Les deux premières séries de questions étaient relatives au recensement des fichiers et des traitements.

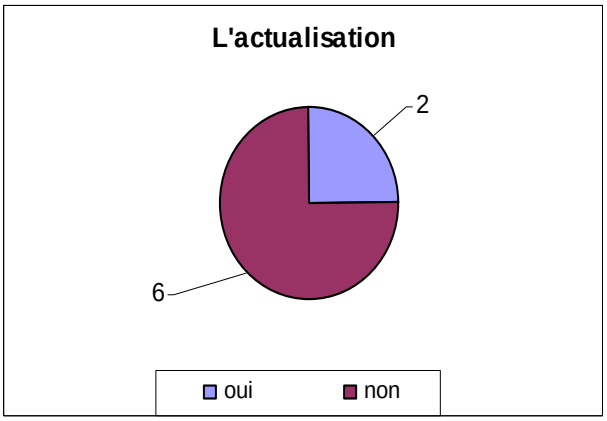
4.2.1. Les fichiers

Les deux premières questions étaient les suivantes :

- **Existe-t-il au sein de la direction un recensement de tous les fichiers sur support informatique qui contiennent des données personnelles qui à ce titre entrent dans le périmètre de la CNIL ?**

- **Une actualisation de ces deux recensements est-elle transmise régulièrement (annuellement) au CIL ?**





La majorité des directions ne dispose pas d'un recensement des fichiers contenant des données personnelles et deux seulement (la DRH et la DDATC) actualisent régulièrement cette documentation. **Il est à noter que certaines directions considèrent que ces tâches reviennent au CIL et ne voient pas l'utilité de l'effectuer en interne. Ce point devra être tranché sur un plan d'ensemble.**

La question suivante portait sur la répartition des fichiers par nature :

Pouvez-vous donner une répartition des fichiers en pourcentage, entre ceux qui contiennent des données personnelles sur les agents de la Ville et ceux qui contiennent des données personnelles sur les usagers des téléservices de l'administration électronique (par internet ou tout autre moyen de communication numérique) ?

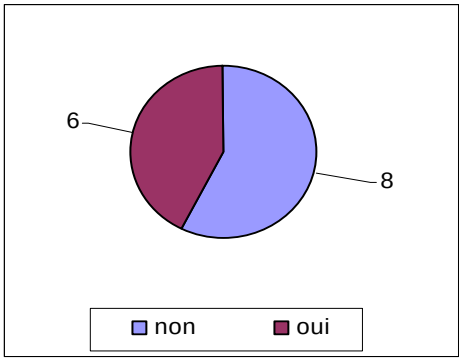
Fichiers	Pourcentage
contenant des données personnelles sur les agents de la Ville	%
contenant des données personnelles sur les usagers des démarches administratives en ligne et des téléservices électroniques de la Ville	%
TOTAL	100 %

Les réponses des 10 directions ayant répondu sont les suivantes :

DALIAT	Agents de la Ville	100 %		
DPE	" "	95 %	usagers	5 %
DLH	" "	60 %	usagers	40 %
DJS	" "	80 %	usagers	20 %
DEVE	" "	90 %	usagers	10 %
DPVI	" "	10 %	usagers	90 %
DFPE	" "	90 %	usagers	10 %
DDATC	" "	5 %	usagers	95 %
DRH	" "	100 %		
DSTI	" "	100 %		

Fort naturellement certaines directions ont des fichiers qui ne contiennent que des données relatives aux agents (DRH…) d'autres essentiellement des fichiers d'usagers (DDATC…), en fonction de la nature de leurs activités. Il ne s'agit manifestement que d'estimations, à prendre avec prudence, comme d'ailleurs le recensement lui-même, et que confirment les réponses à la question suivante :

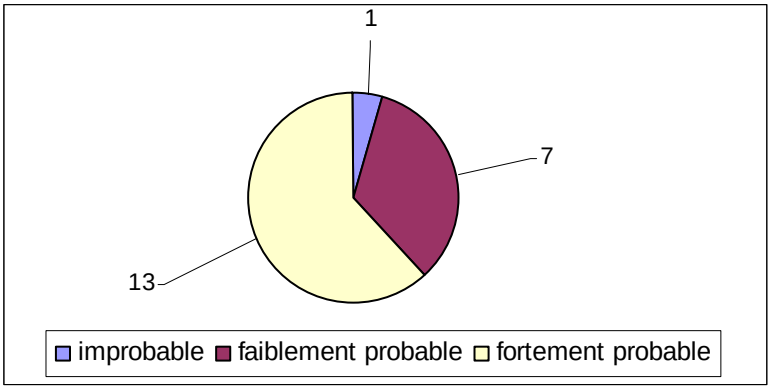
« La déclaration de l'ensemble de ces fichiers est-elle exhaustive par rapport à la réglementation de la CNIL ? ».



Sur quatorze réponses, une minorité seulement « garantit » l'exhaustivité des fichiers.

La deuxième question relative aux fichiers portait sur l'existence éventuelle de fichiers « locaux » non déclarés ; trois réponses étaient possibles (improbable, faiblement probable, fortement probable).

Pourrait-il exister des FICHIERS développés « localement » dans les services avec des outils bureautiques standard qui traiteraient de données personnelles et qui ne seraient pas recensés auprès du CIL ?



Seule une direction (la DA) considère ce risque comme improbable, les **avis se partagent pour le reste entre une minorité qui l'estime faible et une majorité qui l'estime forte**.

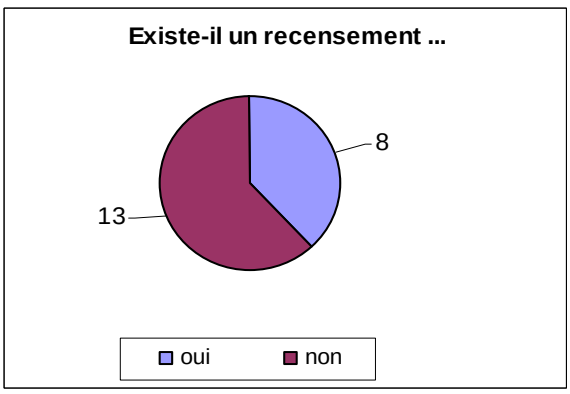
Ces résultats sont confirmés par les entretiens réalisés par les rapporteurs : les directions rencontrées estiment toutes qu'il est au moins possible, voire probable ou certain, que de tels fichiers existent.

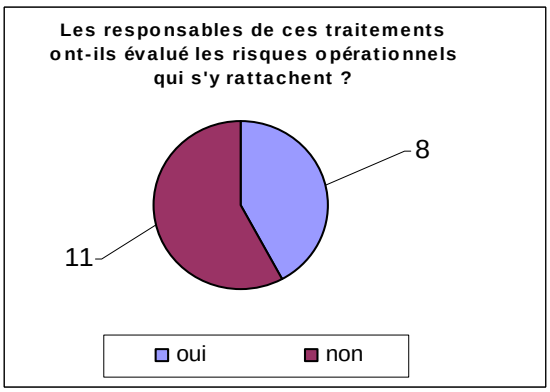
Le constat implique d'élaborer des solutions reposant non seulement sur un renforcement de l'invitation à déclarer, mais aussi sur une sensibilisation générale aux contenus, incitant notamment les utilisateurs à s'interroger sur l'utilité réelle des informations nominatives.

<u>Le recensement des traitements</u>

Cette partie du questionnaire portait principalement, à l'exception de la dernière question, **sur les traitements exploités sur les serveurs de la DSTI.**

Les deux premières questions étaient relatives à l'existence d'un recensement des traitements, exploités sur ces serveurs et utilisant des fichiers contenant des données personnelles, **et à l'existence d'une évaluation des risques**.



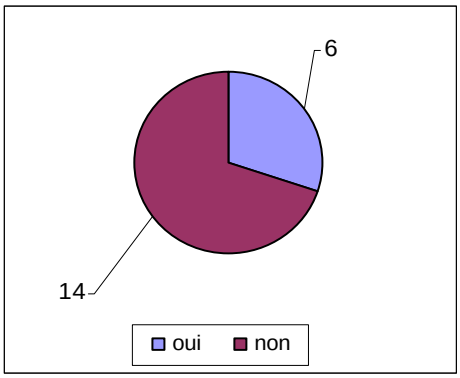


Les résultats sont cohérents entre eux et montrent qu'il existe encore des progrès importants à faire tant en matière de recensement qu'en matière d'évaluation des risques (positives ou négatives, les réponses sont évidemment corrélées).

A noter qu'ensuite une question intitulée « si oui [si les risques opérationnels ont été évalués…], existe-t-il un recueil de bonnes pratiques pour contrôler ces risques ?» n'a recueilli que six réponses dont une seule positive (la DSTI).

Les trois questions suivantes étaient un peu plus techniques.

- **Parmi ces traitements, existe-t-il des interconnexions avec des fichiers en provenance d'organismes extérieurs à la Ville ?**



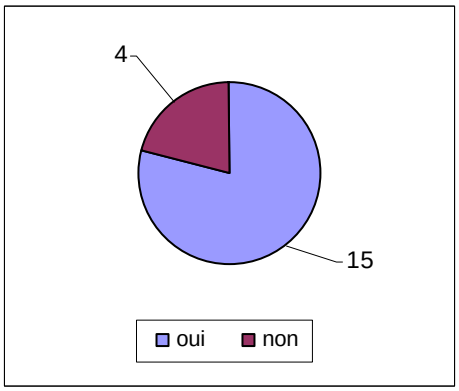
Les six directions qui ont répondu par l'affirmative sont la DASES, la DASCO, la DFPE, la DDATC, la DICOM et la DRH.

Le sujet est bien maîtrisé par les responsables dans la mesure où il s'agit de **traitements bien définis relatifs à leur activité** (inscriptions scolaires avec l'Académie pour la DASCO, RGF et organismes sociaux pour la DRH…) **qui ressortent de leur « cœur de métier ».**

A une question complémentaire **sur l'utilisation du NIR** (numéro d'identification des personnes physiques « n° SS »), les réponses sont également claires, cinq directions utilisent cet identifiant.

La troisième question « technique » était la suivante :

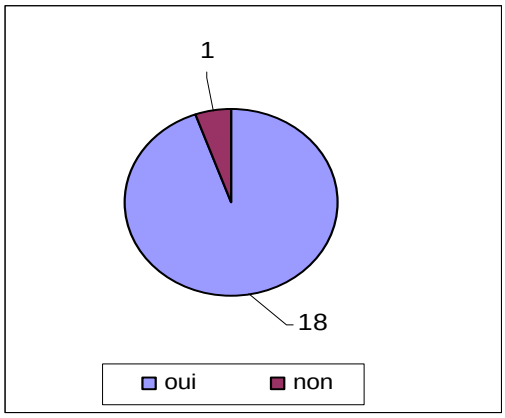
- **Existe-t-il des traitements à la demande qui utilisent des infocentres à la Ville (extraction, enrichissement de fichiers) et qui font intervenir des données personnelles ?**



Les réponses sont très majoritairement positives, **faisant apparaître un taux élevé d'utilisation d'infocentres** à la demande utilisant des données personnelles : quatre directions seulement ne sont pas concernées (DPA, DPP, DA, DICOM).

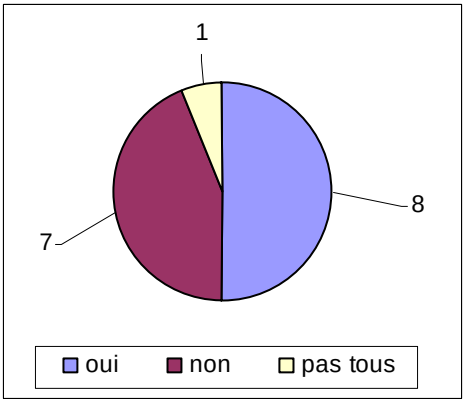
En complément était demandé :

- **« Existe-t-il des traitements de fichiers qui sont réalisés en interne à la direction, avec des outils bureautiques (WORD, EXCEL, ACCESS, etc) sans faire appel aux ressources de la DSTI, et qui portent sur des données personnelles ? ».**



La quasi unanimité des directions a répondu par **l'affirmative**. Seule la DA a émis une réponse négative.

A la question « **si oui, ont-ils été déclarés dans le recensement annuel général transmis au CIL** », les réponses se partagent à peu près à égalité.

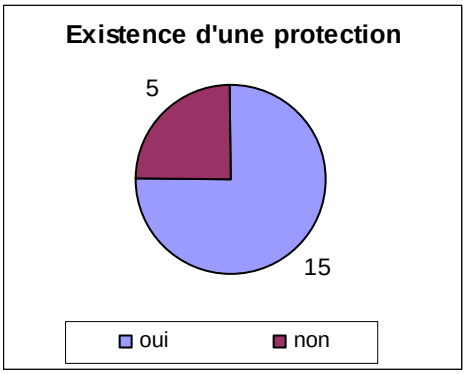


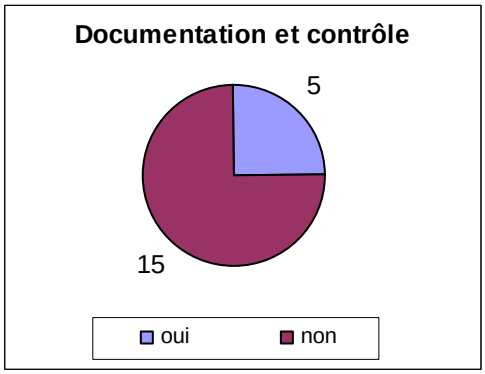
On notera que trois directions (la DA, la DASES et la DRH) qui ont répondu par l'affirmative à la question précédente n'ont pas répondu à celle-ci…

4.2.2. La confidentialité des fichiers accessibles par le réseau interne

Une batterie de quatre questions était proposée :

Pour les fichiers accessibles via le réseau, est-il prévu systématiquement dans les applications un dispositif logique (ex : mot de passe) et/ou physique (ex : clé électronique, badge) pour contrôler la non divulgation de données personnelles en fonction des habilitations liées aux profils utilisateurs ?





Trois directions sur quatre ont bien mis en place la protection évoquée mais trois sur quatre également ne « documentent » pas systématiquement et n'effectuent pas de contrôle régulier. Lors des entretiens réalisés par les rapporteurs tous leurs interlocuteurs ont cependant reconnu l'impérieuse nécessité d'effectuer et de suivre ce premier niveau de contrôle.

L'un des moyens de contrôle les plus efficaces consiste à disposer dans les traitements **d'un fichier « log » qui retrace l'historique des accès**, et permet ainsi de détecter toutes les anomalies (liées par exemple à des horaires anormaux de connexion…).

Une question était donc posée sur ce thème :

A votre connaissance, quel est le pourcentage du nombre de traitements qui intègrent nativement des fichiers « logs » pour tracer l'historique des accès aux fichiers ?

Traitements qui intègrent …	… des fichiers « logs »
sur des fichiers contenant des données personnelles sur les agents de la Ville	%
sur des fichiers contenant des données personnelles sur les usagers des téléservices de l'administration électronique de la Ville	%

Là aussi l'ensemble des directions avec lesquelles des entretiens ont été réalisés a reconnu l'intérêt de ce dispositif qui permet de savoir qui a accédé aux données, et quand. Mais **six seulement ont signalé bénéficier d'une telle protection**, à 100 % pour trois d'entre elles (DU, DALIAT et DPVI), à un moindre degré pour les trois autres (DLH, DFPE, DDATC).

Des procédures de contrôle ont-elles été mises en place pour prévenir les « fuites » non autorisées de données personnelles vers l'extérieur ?

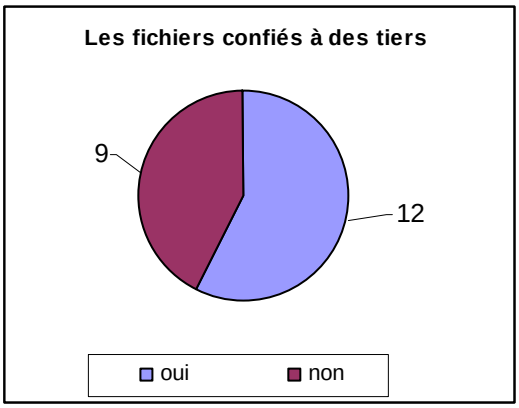
La réponse des services est à **100 % négative** ; aucune procédure spécifique n'a été mise en place (18 réponses).

4.2.3. Les fichiers et traitements confiés à des organismes extérieurs

Trois questions et sous-questions étaient proposées :

Des services sont-ils conduits, régulièrement ou occasionnellement, à confier des fichiers contenant des données personnelles sur les agents de la Ville ou sur des usagers des services de la Ville à des tiers privés (ex : routage presse) ou publics (organismes sociaux) ?

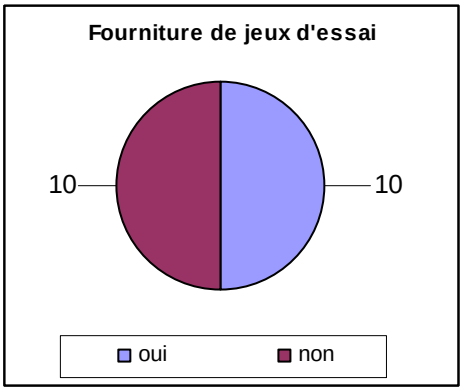
Si oui, ces échanges sont-ils contrôlés par un cadre juridique très précis (confidentialité, restitution, destruction, etc) permettant de contrôler les risques associés ?



La proportion des directions concernées par le sujet est importante, puisque plus de la moitié des services répondent par l'affirmative. A la sous-question du cadre juridique de suivi, la plupart répondent par l'affirmative (six réponses positives pour deux négatives).

Dans le cadre de la maintenance des applications informatiques de la direction, existe-t-il des cas où vos services sont conduits à fournir des jeux d'essais contenant des données personnelles ?

Si oui, cette fourniture est-elle contrôlée par un cadre juridique très précis (confidentialité, restitution, destruction, etc) permettant de contrôler les risques associés ?



L'échantillon se partage ici rigoureusement en deux. Sur les dix directions répondant par l'affirmative, huit affirment contrôler ces procédures dans un cadre sécurisé.

Enfin la dernière question de la série portait sur l'éventualité de l'hébergement de fichiers **dans des centres informatiques localisés dans des pays tiers**. Aucune direction de la Ville ne paraît être dans ce cas, ce que la DSTI confirme. Le risque peut donc être écarté[5].

[5] actuellement, car comme l'ont signalé nos interlocuteurs extérieurs, le risque des sous-traitances « en cascade » se développe et peut se réaliser à l'insu du donneur d'ordre si les précautions requises au niveau du cahier des charges ne sont pas prises

4.3. L'archivage et la destruction des fichiers

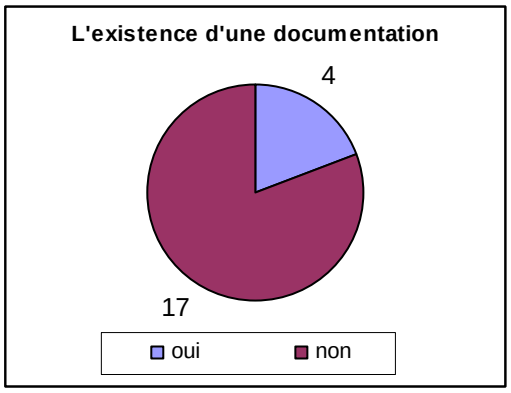
A quelques exceptions près, comme on va le voir, cette question est peu prise en compte ; les directions signalent l'absence de document ou d'instruction de référence sur cette question. Notre CIL signale d'ailleurs que la destruction ou l'anonymisation sont rarement prises en compte dans les logiciels du marché.

Le questionnaire abordait les points suivants :

Existe-t-il une documentation de référence définissant la durée maximale de conservation des fichiers déclarés auprès du CIL (ou de la CNIL pour les plus anciens) ?

Si oui, cette durée maximale est-elle contrôlée ?

Au-delà de la durée maximale de conservation, comment la procédure de destruction des archives numériques est-elle contrôlée ?



Dans l'écrasante majorité des services, il n'y a pas de documentation définissant la durée maximale de conservation. **Parmi celles qui en disposent, on trouve toutefois la DRH et la DASCO, très concernées par la problématique de la durée de conservation d'éléments « sensibles », qu'ils soient relatifs aux agents municipaux ou aux jeunes scolaires**. Seule la DASCO toutefois contrôle de manière organisée et systématique le bon respect de cette durée maximale, y compris jusqu'à la procédure de destruction.

Enfin, à la deuxième question, « les procédures d'archivage des fichiers numériques recensés comme relevant du champ de compétence de la CNIL ont-elles été documentées et diffusées », trois directions seulement répondent par l'affirmative (DLH, DJS, DASCO). **Ce sujet est à l'évidence complètement à reprendre** : la durée de conservation est un élément essentiel de la sécurité et du « droit à l'oubli ».

5. L'ORGANISATION D'AUTRES ENTITES (……), LES RECOMMANDATIONS DE LA CNIL, L'ASSOCIATION FRANÇAISE DES CORRESPONDANTS A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL (AFCDP)

Les rapporteurs ont estimé indispensable de recourir à l'évaluation comparative (benchmarking) en examinant les expériences d'entités dont l'activité et les caractéristiques étaient susceptibles d'offrir des enseignements utiles. L'un des CIL rencontrés……. étant par ailleurs président de l'Association Française des Correspondants à la Protection des Données à Caractère Personnel (AFCDP), il a également été possible de faire un point sur l'activité de cette structure à laquelle notre CIL a fait adhérer la Ville.

5.1. ……..

Le titre qui précède et les paragraphes qui suivent ont été occultés conformément à l'engagement pris auprès des entités ayant participé à l'évaluation comparative (« benchmarking »).

5.2. ……..

Le titre qui précède et les paragraphes qui suivent ont été occultés conformément à l'engagement pris auprès des entités ayant participé à l'évaluation comparative (« benchmarking »).

5.3. ……

Le titre qui précède et les paragraphes qui suivent ont été occultés conformément à l'engagement pris auprès des entités ayant participé à l'évaluation comparative (« benchmarking »).

5.4. L'Association Française des Correspondants à la Protection des Données à Caractère Personnel (AFCDP)

Son président actuel est donc le CIL d'AG2R La Mondiale. Cette structure, **à laquelle notre correspondant a fait adhérer la Ville de Paris**, se donne pour objectifs :

- **de promouvoir la fonction de Correspondant Informatique et Libertés** et d'en faire un métier ;
- de proposer **un cadre d'échanges** en développant un réseau en France et à l'international ;
- **de concevoir des outils, méthodes et pratiques** utiles aux correspondants informatique et libertés ;
- **de défendre la fonction**, en suivant le cadre juridique de celle-ci, en ayant la primeur de l'information, en agissant pour faire valoir la position des professionnels.

Elle est ouverte aux personnes physiques, aux personnes morales et aux professions libérales. Elle a vocation à regrouper, au-delà des correspondants informatique et libertés, toutes les personnes intéressées par le sujet.

Elle regroupe à ce jour environ 300 adhérents sur 1 500 entités et entreprises dotées d'un CIL (elle a été créée en 2004) et **est en croissance régulière**. Pour l'instant elle est encore dotée de peu de moyens (un salarié à temps partiel) mais devrait progressivement se renforcer. On notera qu'elle dispose déjà **d'un site Internet (afcdp.net)** bien fait sur lequel on trouve notamment des fiches pratiques, une lettre d'information, et d'une manière générale l'actualité relative au sujet (la page de garde est reproduite en annexe 4).

L'association se veut avant tout un lieu d'échanges ; les réunions mensuelles permettent aux membres de se rencontrer, de partager les questions et les difficultés rencontrées, tant à Paris qu'en région, **répondant ainsi à l'un des problèmes rencontrés par les CIL qui est l'isolement** (ils sont par définition uniques dans leur structure). Des groupes de travail réfléchissent sur des thèmes donnés (la perte de données nominatives, dont un projet de loi présenté au Sénat envisage de rendre la déclaration obligatoire, les données de santé, la durée de conservation, le bilan annuel…) et élaborent des fiches (comment gérer un probable contrôle de la CNIL ?).

L'AFCDP s'est aussi fait reconnaître comme **un interlocuteur incontournable de la CNIL** et des pouvoirs publics.

L'existence de cette structure a paru importante aux rapporteurs ; elle apporte un véritable soutien et une réelle assistance aux CIL en leur permettant de confronter leurs problèmes, d'évaluer les solutions possibles, de partager des instruments à caractère pratique (guides, fiches de procédure et de conseils…). Elle est unique dans son domaine, elle est aussi la seule à permettre à une entité comme la Ville de Paris de rencontrer des représentants de grands groupes d'une taille comparable à la sienne et par là même d'opérer des comparaisons utiles.

5.5. Les recommandations de la CNIL

Les rapporteurs ont été reçus par **le chef de service des correspondants**, rattaché à la direction des relations avec les usagers et du contrôle.

L'échange a bien évidemment porté sur **les risques particuliers des collectivités locales**, et donc encourus par la Ville : les thèmes majeurs recensés par la CNIL sont le suivi des populations à risque, la police municipale, l'éducation et les affaires scolaires, les fichiers politiques et enfin les données cadastrales.

Une administration locale moderne doit présenter à l'usager **les éléments d'une communication éthique :**

- avec une bonne disponibilité du service offert, et **des informations claires, facilement accessibles, sur les droits d'accès ;**
- en apportant **un soin particulier à la sécurité des données**, et en s'obligeant à notifier au public concerné les failles de sécurité lorsque celles-ci sont révélées.

On rappellera sur ce dernier point qu'une proposition de loi est actuellement débattue sur ce sujet.

Les rapporteurs ont demandé à leur interlocuteur s'il était envisageable de coéditer sur le site Internet de la Ville un certain nombre d'informations présentes sur le site Intranet de la CNIL, afin de récupérer au mieux et au plus vite les informations relatives au domaine.

Cette approche n'est pas envisageable, pour deux raisons principales : la protection de l'intégrité des données présentes sur le site Intranet de la CNIL, et sur un plan matériel, la saturation des équipes de la direction des services informatiques de la commission. Par contre, la Ville a toute liberté **de reprendre les informations présentes sur le site Extranet ouvert aux CIL**.

La problématique du choix du CIL et de ses moyens a été longuement abordée. ……
La phrase ci-dessus a été occultée conformément aux dispositions de la loi du 17 juillet 1978 relative à l'accès aux documents administratifs.

Les recommandations de la CNIL sont les suivantes :

Il faut être conscient qu'il s'agit d'une étape délicate car il ne faut pas perdre l'expérience capitalisée depuis la première nomination intervenue en 2006.

Le candidat **doit être choisi suffisamment à l'avance**, indépendamment des délais liés à sa désignation officielle. La CNIL pourra ainsi lui proposer des modules de formation, réalisés par elle-même ou à l'extérieur. Un « tuilage » de six mois paraît constituer la bonne durée. Cette période permet aussi à l'intéressé de faire connaissance avec les services de la CNIL et l'AFCDP.

Le choix de la personne doit satisfaire à **plusieurs critères** :

L'ancienneté dans la structure, avec la connaissance des interlocuteurs, **l'aptitude** à **communiquer et à travailler en équipe, les compétences informatiques et/ou juridiques…** La CNIL n'impose pas de profil déterminé, mais elle constate que les candidats sont fréquemment issus des secteurs de l'audit, du contrôle qualité, du contrôle interne et de la direction des risques lorsqu'elle existe.

La nomination du nouveau CIL doit être matérialisée **par une lettre de mission officielle** lors de son entrée en fonction : cela permet d'assurer sa crédibilité et témoigne de la volonté politique de la collectivité.

Il est recommandé de créer un comité de pilotage des projets « informatiques et libertés » pour identifier et communiquer sur les points d'action du CIL :

- le recensement permanent,
- l'instruction des droits d'accès et des réponses,
- le travail de conseil (consultations préventives par les services)
- le devoir d'alerte,
- la tenue du registre et le bilan annuel.

Cette approche permet de mieux capitaliser l'expérience acquise au fil des dossiers (gestion de la connaissance), **dans la mesure où le CIL est très seul dans sa fonction.**

Par ailleurs, le CIL a **un travail d'information des instances représentatives du personnel** à assurer : il faut y consacrer le temps nécessaire et veiller à la forme de cette information préalable aux nouveaux traitements et fichiers.

Il est important de prévoir une information individuelle des agents à l'occasion du changement de CIL, toujours pour soutenir sa crédibilité, en rappelant l'existence des procédures de demande de droit d'accès et de rectification en provenance des agents.

Il a été rappelé que notre CIL doit et devra disposer de moyens nécessaires pour accomplir sa mission (la CNIL bien sûr ne rentre pas dans les détails).

Bien que le choix du CIL demeure de la responsabilité unique de la Ville – la CNIL n'a pas, rappelons le, de pouvoir d'agrément, même si la désignation du correspondant est encadrée par une procédure – **la commission s'intéresse donc de très près à celui-ci**, gage évidemment si ce choix est pertinent d'une collaboration fructueuse et de bonnes relations.

Dernier élément à signaler, il nous a été bien précisé que l'éventuelle publication du présent rapport sur Internet (sur l'opportunité de laquelle la CNIL ne se prononce évidemment pas) serait suivie de son examen attentif par la commission. Si des infractions venaient à y être exposées, **elles entraîneraient donc un contrôle et des sanctions.**

6. PROPOSITIONS DES RAPPORTEURS

6.1. La mise en place d'un réseau de « référents - CIL » dans les directions

L'action du CIL doit pouvoir être relayée efficacement au sein des directions grâce à la désignation officielle d'un point d'entrée unique, le « référent CIL ».

La diffusion du questionnaire d'enquête a permis de vérifier que cette fonction était bien comprise : plusieurs d'entre elles ont en effet saisi l'occasion pour désigner leur CIT comme référent, voire un échelon supérieur lorsqu'un contexte particulièrement sensible le justifiait (cf. la DICOM).

Il ne s'agit pas de confier au référent des responsabilités qui incombent normalement au CIL : son rôle principal sera de rassembler les informations nécessaires à la vérification de la conformité de sa direction par rapport à la réglementation CNIL, d'être un guide pour les responsables de projet en interne et un relais pour les actions de formation et de consolidation initiées par le CIL.

Certaines directions pourront préférer une responsabilité collégiale associant le CIT et le responsable des affaires juridiques (cf. la DPE) ou celui des ressources humaines (cf. la DJS) en fonction de leurs spécificités.

Il est souhaitable que la désignation des référents au sein des directions soit officialisée auprès de l'ensemble des agents (cf. DPE).

6.2. La création d'outils de formation et le développement d'une politique de communication

Les directions ont bien conscience que, face à l'extension croissante de l'usage de l'informatique, elles ne pourront jamais exercer en permanence un contrôle strict et exhaustif des pratiques en matière de gestion automatisée des données personnelles.

Dans ces conditions, une bonne prévention des risques passe en premier lieu par une action d'information et de sensibilisation permanente, notamment au niveau des cadres : cette démarche doit être renouvelée à intervalles réguliers, notamment pour faire face au turn-over naturel des agents. Une sensibilisation des agents nouvellement recrutés doit être également mise en place.

Pour ce faire, le CIL doit pouvoir offrir une panoplie d'outils pédagogiques adaptée aux profils des demandes des directions, avec en complément l'animation d'un site dédié à ce thème sur l'Intranet de la Ville : ce site doit par principe être indépendant de celui de la DSTI (on rappellera qu'en 2006 il figurait d'ailleurs dans l'intranet du Secrétariat Général ; il pourrait figurer dans « Intraparis » « Métiers »).

Les outils pédagogiques peuvent être principalement :

- **des guides individuels sur support papier** pour les différentes catégories d'acteur (encadrement administratif, chefs de projets, exploitants, CIT, etc.)
- des sessions de formation inscrites au catalogue de la DRH[6].
- des modules d'apprentissage en ligne (« e-learning ») téléchargeables à partir de l'Intranet.

[6] L'Institut supérieur d'électronique de Paris (ISEP) est l'une des rares écoles à proposer une formation au métier de correspondant informatique et libertés dans le cadre d'un master intitulé « Management et protection des données à caractère personnel »

Ces supports devront être conçus et mis en place en étroite collaboration avec les directions, et notamment les référents.

Le site Intranet a vocation à regrouper toutes les informations nécessaires à tous les services de la Ville, et principalement aux référents et chefs de projet informatiques, en complémentarité avec le site de la CNIL : règles et normes applicables, actualités, évolution de la jurisprudence, projets à la Ville, etc.

6.3. L'amélioration des échanges d'information avec le CIL

Les directions jugent très positivement les modalités de collaboration avec le CIL : déclarations par courriel, recensement des fichiers et traitements, saisine sur les nouveaux projets, etc.

Cependant les résultats de l'enquête ont montré que cette collaboration pouvait être étendue et enrichie avec de nouveaux outils.

La demande porte essentiellement sur l'accès aux informations collectées par le CIL. Celui-ci a fait réaliser par la DSTI une base de données regroupant toutes les déclarations déjà effectuées par les directions, avec deux volets :

- un descriptif simple des fichiers et des traitements déclarés,
- des informations sur les événements ayant trait à la vie du projet, pour les besoins propres du CIL (avec un volet documentaire intégrant des commentaires personnels et des documents scannés).

Les directions souhaitent pouvoir accéder facilement et de façon indépendante au premier volet : elles auraient ainsi la possibilité de vérifier que le recensement de leurs déclarations est bien à jour et cela leur éviterait de gérer parfois leur propre base de données, avec les risques de désynchronisation que cela peut entraîner.

Bien évidemment le deuxième volet ne serait pas accessible aux directions et resterait réservé au CIL pour son propre usage.

Le contexte de gestion de crise, tel que la pandémie grippale H1N1, a fait surgir une préoccupation spécifique émanant de certaines directions (cf. la DFPE) : l'urgence de diffusion des nouvelles règles exceptionnelles s'appliquant à l'usage des données personnelles entre les services de l'État, la CNIL et les responsables opérationnels au sein de la collectivité. **Cette demande justifie une petite étude pour déterminer les solutions organisationnelles et techniques les plus efficaces qu'il conviendra d'activer en pareilles circonstances.**

6.4. L'articulation des responsabilités entre la DSTI et les directions métiers, les propositions de la DSTI

Le principe admis par la DSTI est que les directions métiers, en tant que MOA, doivent assumer l'entière responsabilité des actions à mener concernant la protection des données personnelles : la DSTI peut offrir un rôle de conseil si la direction en fait la demande, cette approche étant justifiée par le fait que les MOA sont les mieux placées pour identifier les risques s'attachant à leurs projets et expliciter les niveaux de protection qui doivent être mis en oeuvre en conséquence.

De façon symétrique, les directions estiment qu'elles ne disposent pas en interne des compétences techniques suffisantes pour embrasser l'ensemble des questions soulevées par cette problématique.

Cette séparation des rôles doit donc être mieux explicitée, en tirant profit de l'expérience acquise, afin qu'il ne s'instaure pas une sorte de zone grise où chacun pense que c'est l'autre qui a en charge telle ou telle responsabilité opérationnelle.

Cela passe par la rédaction d'une sorte de charte déontologique explicitant et précisant bien le mode de collaboration qui doit s'instaurer entre la DSTI (études, production, sécurité) et les directions métiers tout au long des cycles de vie de chaque projet (création, maintenance, exploitation, déploiement, etc.).

La responsabilité de cette action pourrait être confiée à la Mission Sécurité de la DSTI, qui serait ainsi de facto le référent général du CIL pour le compte de la DSTI.

La DSTI propose de renforcer la prise en compte de la loi dans le cycle de vie des projets.

Elle souhaite ainsi instituer un processus garantissant une parfaite conformité des applications réalisées avec leur déclaration CNIL. Lors de la mise en production de l'application, un document serait adressé au CIL pour tous les projets importants.

D'autre part, un corpus d'exigences dans les marchés pour la protection des données personnelles devrait être élaboré ; il serait défini par la DSTI en liaison avec le CIL.

6.5. Les risques liés à la sous-traitance informatique et aux échanges de fichiers avec l'extérieur

La Ville est déjà conduite à confier l'exploitation d'un petit nombre de fichiers contenant des données personnelles à des tiers privés (routage, maintenance des applications) et à procéder également à des échanges avec d'autres administrations (CAF, RGF, CPAM, Rectorat, etc.) : pour les applications développées par la DSTI, des clauses standards sont introduites dans les marchés, notamment pour les sociétés en charge de leur maintenance.

Cette approche pourrait être généralisée en diffusant auprès des directions un vade-mecum standard sur les clauses types qui devront être insérées systématiquement dans les marchés conclus avec des prestataires privés ou dans les conventions régissant les échanges de fichiers avec des structures publiques.

Comme cette tendance de l'externalisation ne pourra que s'amplifier à l'avenir, avec par exemple le développement des offres de service incluant à la fois le droit d'utilisation des progiciels et leur exploitation sur les propres machines de l'éditeur, cette question mérite une vigilance accrue de la part du CIL.

6.6. L'intégration du référentiel général de sécurité pour les télé-services

Le récent décret de février 2010 précise les règles auxquelles les systèmes d'information publics doivent se conformer pour assurer la sécurité des informations. Le texte explique les démarches à suivre pour protéger les systèmes d'information, et définit les sécurités exigées. D'autre part, le texte contient des développements importants sur la qualification et les conditions d'agrément des prestataires ; il devrait donc faire l'objet d'une assez large publicité auprès des services de la Ville.

6.7. L'évaluation des risques et le contrôle interne

La mise en place de réglementations « prudentielles » pour prévenir la survenue de risques conduit fréquemment les organisateurs à prévoir conjointement une fonction de contrôle interne pour s'assurer régulièrement de leur bonne application (l'exemple vient des normes comptables dans le secteur bancaire).

Cette tâche pourrait être confiée à l'Inspection générale[7], sous la forme d'audits flash conduits selon un protocole à définir en collaboration avec le CIL, avec une programmation annuelle.

Il s'agirait de vérifier notamment dans les directions que :

- les procédures de confidentialité sont bien respectées par les agents dans les domaines sensibles (ex. : la GRH, l'état civil, les télé-services, la santé, etc.)
- des fichiers de gestion « sauvages » n'ont pas été créés sans déclaration auprès du CIL,
- l'encadrement possède toujours un bon niveau d'information et de sensibilisation sur le sujet,
- les procédures de purge des fichiers sont correctement exécutées,
- etc.

En parallèle, un petit nombre de directions particulièrement exposées compte tenu de la nature de leurs activités pourraient engager une réflexion sur l'importance de leurs risques spécifiques vis-à-vis de la CNIL, en partant du recensement des grands métiers qu'elles exercent conformément aux missions qui leur sont confiées.

Cette recommandation vise également toutes les directions qui gèrent des implantations administratives nombreuses et déconcentrées, comme la DJS, la DFPE, la DASCO, la DASES, etc.

6.8. La durée de conservation des fichiers avec des données personnelles et leur destruction, le droit à l'oubli et l'archivage des fichiers numériques

Ces trois points de la réglementation sont loin d'être pris en compte de façon satisfaisante par l'ensemble des services de la Ville : il convient donc que le CIL et la DSTI engagent rapidement une opération « vérité » globale pour clarifier la situation des directions par rapport aux exigences de la CNIL sur cet aspect particulier de la réglementation, afin de pouvoir élaborer ensuite un plan d'action visant à rétablir une situation plus conforme, suivant ainsi les propositions de la DSTI dans sa réponse au rapport provisoire.

[7] ..... *Cette note a été occultée conformément aux dispositions de la loi du 17 juillet 1978 relative à l'accès aux documents administratifs.*

6.9. Le positionnement administratif et hiérarchique du CIL, son profil d'expérience et ses moyens d'action

Il convient de distinguer deux sujets :

- la perspective du départ relativement rapproché du CIL impose une réflexion sur sa succession,
- à la lumière de ce qui se pratique ailleurs, et compte tenu des recommandations formulées dans le présent rapport, la gestion des moyens doit être réexaminée.

Sur le premier sujet, on a vu que la question du profil d'origine professionnelle de la personne restait relativement ouverte. Informaticien ou juriste, le nouveau correspondant complètera, en tant que de besoin, sa formation et ses connaissances. Il faut cependant insister sur la nécessité de faire appel à **un fonctionnaire expérimenté, connaissant bien les services municipaux** et d'un niveau hiérarchique suffisamment élevé compte tenu du positionnement de la fonction et de ses caractéristiques. **Le CIL dépend du responsable des traitements, qui est le Maire** ; il doit pouvoir sans difficulté dialoguer avec le Cabinet, le Secrétariat Général, les directeurs. La situation « statutaire » actuelle, celle de sous-directeur, est correcte, un niveau identique ou équivalent doit pouvoir être maintenu. Le CIL doit être connu des services et des personnels ; la DICOM pourrait à cet égard entreprendre les actions de communication nécessaires. Enfin, une présentation officielle aux organisations syndicales pourrait être organisée en lien avec la DRH.

Le CIL – c'est une recommandation de la CNIL – doit être destinataire d'une lettre de mission explicitant ses domaines d'intervention et ses moyens. La rédaction de celle-ci devra être l'occasion de mettre au clair les responsabilités respectives du CIL et des directions sur l'actualisation de la documentation.

En matière de moyens, notre correspondant est actuellement seul. Compte tenu des recommandations du rapport et pour les mettre en œuvre, il serait nécessaire de lui adjoindre une personne dont le profil d'assistant aurait en particulier vocation à tenir le fichier des déclarations et modifications, et à gérer les correspondances courantes avec les directions, permettant ainsi au CIL de dégager du temps pour se consacrer à des tâches qui sont aujourd'hui incomplètement assurées : **édition et diffusion d'un rapport annuel, actions de formation** auprès des directions et propositions de **contrôle** en collaboration avec l'Inspection Générale.

* *
*

Toutes les mesures explicitées précédemment ont pour but de lutter contre l'affaiblissement naturel de l'attention portée à ces questions, qui il faut bien le reconnaître ne peuvent constituer en permanence la priorité absolue des gestionnaires.

Aussi, les rapporteurs proposent que le CIL puisse engager des actions régulières pour remobiliser l'ensemble des directions sans toutefois les lasser.

Au cours des entretiens, les CIT ont manifesté le souhait qu'**une sorte de conférence annuelle des référents** puisse être organisée, avec des sessions traitant des questions d'actualité, des ateliers pour échanger les expériences entre les directions, des témoignages sur les expériences extérieures à la Ville, etc.

Cette action viendrait en complément d'une opération de consolidation du recensement des fichiers conduite chaque année, comme cela est prévu dans les missions du CIL.

Liste des personnes rencontrées

Secrétaire général adjoint
Directeur de la DSTI
Correspondant Informatique et libertés
Administrateur, Directeur adjoint (DSTI)
Mission sécurité (DSTI)

* *
*

La conférence des correspondants informatique et télécommunications (CIT) des différentes directions

* *
*

Chef du bureau juridique et foncier (DPE)
Bureau juridique et foncier (DPE)
Sous-directeur de l'administration générale et de la prévision scolaire (DASCO)
Sous-directeur de l'administration générale et de l'équipement (DJS)
Attachée d'administration, Chef de service des ressources humaines (DJS)
Sous-directeur du réseau ressources humaines et des systèmes d'information (DRH)
Chef du département des systèmes d'information (DRH)
Sous-directrice des ressources (Direction des familles et de la petite enfance – DFPE)

* *
*

Correspondant informatique et libertés de (……)
Correspondant informatique et libertés de (……..)
Directeur, correspondant à la protection des données de ……..,
Président de l'association française des correspondants à la protection des données personnelles (AFCDP)
Chef du service des correspondants - Direction des usagers et du contrôle – Commission nationale informatique et libertés (CNIL)

PROCEDURE CONTRADICTOIRE

Le rapport provisoire d'audit des fichiers informatiques de la Ville et du Département de Paris a été envoyé le 20 avril 2010 à Messieurs …, Secrétaire général adjoint, …, Directeur des systèmes et technologies de l'information, et …, Sous-directeur, correspondant Informatique et Libertés.

- Courrier du 27 mai 2010 du Secrétaire général adjoint
- Courrier du 27 mai 2010 du Correspondant Informatique et Libertés
- Courrier du 31 mai 2010 du Directeur des systèmes et technologies de l'information

Courrier du 27 mai 2010 du Secrétaire général adjoint

MAIRIE DE PARIS

5467

Le Secrétaire Général adjoint

Affaire suivie par

Paris, le 27 MAI 2010

NOTE à l'attention de : **Madame**
Directrice de l'Inspection Générale

Objet : Réponse à la transmission du rapport provisoire d'audit des fichiers informatiques de la Ville et du Département de Paris (n°09-23)

L'examen du rapport visé en objet, qui traite me semble-t-il le sujet de manière satisfaisante et dont je partage globalement l'analyse et les préconisations, appelle de ma part les commentaires suivants :

En ce qui concerne votre analyse, je retiens que vous signalez le besoin de relais CIL dans les directions (la moitié des directions n'en disposent pas) afin de faciliter le travail du CIL de la collectivité.

Je note également un besoin d'information et de formation au vu des constats suivants :

- Les supports pédagogiques diffusés par le CIL sont assez peu connus et incomplets (ils étaient à l'origine sur le site intranet du SG et sont désormais sur celui de la DSTI) ;
- Un quart des directions interrogées répondent « oui » à la question : « l'encadrement de la direction a-t-il connaissance des responsabilités et des sanctions pénales, financières et administratives encourues en cas d'infraction ? » ;
- Deux directions seulement (DRH/DSTI) ont des procédures de contrôle interne pour assurer la maîtrise des risques liés à la protection des données personnelles ;
- Aucune direction ne dit avoir mis en place des procédures de contrôle pour prévenir les fuites non autorisées de données personnelles vers l'extérieur ;
- Peu de directions recensent leurs fichiers contenant des données personnelles, pensant que c'est au CIL de le faire ;
- Dans l'écrasante majorité, il n'y a pas de documentation définissant la durée maximale de conservation des fichiers.

Par ailleurs, il me semble que le principal point faible de la Mairie parmi ceux que vous relevez, est l'absence de politique active et coordonnée relative à l'archivage des données.

Enfin, j'ai bien noté que lors d'un entretien avec la CNIL, il vous a été précisé que « l'éventuelle publication du présent rapport sur Internet serait suivie de son examen attentif par la commission. Si des infractions venaient à y être exposées, elles entraîneraient donc un contrôle et des sanctions.»

En ce qui concerne vos préconisations, j'ai relevé les principales propositions suivantes :

- Mise en place d'un réseau de référents CIL au sein de chaque direction et définition précise des rôles respectifs des correspondants CIL des directions et du correspondant CIL de la collectivité, cela semblant être actuellement une source de confusion ;
- Amélioration des échanges d'information entre les directions et le CIL ;
- Création d'outils de formation et développement d'une politique de communication. Des réunions régulières du réseau (comme cela se fait dans les organismes que vous avez visités) semblent nécessaires afin de diffuser l'information et d'échanger ;
- Evaluation des risques et contrôle interne ;
- Information sur la durée de conservation des fichiers avec des données personnelles. Cette recommandation dépasse le seul sujet de la protection des données personnelles et paraît aussi la plus difficile à mettre en œuvre ;
- Formalisation des responsabilités entre la DSTI et les directions métiers, la DSTI considérant que les directions doivent assumer l'entière responsabilité des actions à mener concernant la protection des données personnelles.

Enfin, je note que vous suggérez de renforcer le CIL en lui adjoignant un collaborateur (catégorie B), en lui confiant officiellement le rôle de CIL pour le CASVP et que vous proposez de réfléchir au remplacement prochain du CIL en prévoyant une période de tuilage avec son successeur.

Tels sont les éléments que je souhaitais porter à votre connaissance.

Courrier du 27 mai 2010 du Correspondant Informatique et Libertés

MAIRIE DE PARIS

Affaire suivie par : -
Tél : 01 43 47 62 88 -

Paris, le 27 mai 2010

Note à l'attention de Madame la directrice de l'Inspection générale

Objet : Remarques sur le rapport provisoire n° 09-23

PJ : Remarques (27/05/2010)
Document adressé à madame la Secrétaire générale recommandant une mission d'inspection (15/06/2009)

Note du 20 avril 2010

Je vous remercie de l'envoi du rapport préliminaire de vos services concernant le cadre des fonctions de correspondant Informatique et Libertés.

Les remarques que je peux émettre sont jointes en annexe à la présente note.

J'en reprendrai les principaux éléments en formulant des souhaits pour une évolution des moyens et de la communication.

Fort d'une organisation pour le respect, dès son origine, des dispositions de la loi Informatique et Libertés la Ville a, par la désignation d'un CIL, resserré le dispositif et lui a donné de la cohérence.
Cependant l'absence d'un espace visible dédié sur l'Intranet et sur le site « paris.fr » a fortement limité l'impact de la mesure. Je renouvelle donc mon souhait de mise en place de cet espace.

La désignation d'un correspondant officiel par direction est une solution à envisager tout en sachant que les projets sont souvent suivis par d'autres personnes. Le gain à en attendre est une continuité dans les procédures (ex DASCO et DPE) non affectée par des mutations.

Lors de l'accueil des nouveaux fonctionnaires il serait envisageable de faire une séance de sensibilisation tant au respect de la loi informatique et libertés qu'à celle relative aux relations des citoyens avec leur administration (CADA). Un module peut être créé pour les fonctionnaires en poste et s'adossant à l'espace dédié sur l'Intranet.

Le CIL doit être contacté dès le projet de réalisation d'une application ou de fichier afin de déterminer le cadre précis de l'utilisation des données à caractère personnel.

La reconnaissance en interne du CIL et du correspondant CADA est une sécurité pour la Ville, cela implique que le fonctionnaire chargé de ces fonctions a une bonne connaissance de l'organisation et dispose d'un réseau de contacts permettant de réagir rapidement. Les instances CNIL et CADA imposent des délais très courts pour répondre y étant elles même soumises de par la loi.

Tels sont les éléments dont je souhaitais vous faire part.

Sous-Directeur
Correspondant CNIL et CADA

227 rue de Bercy 75012 Paris

15/06/2009

La situation de la Ville de Paris en tant qu'administration « capitale » m'a conduit à une réflexion particulière quant à son implication dans le respect de la loi Informatique et Libertés.

L'analyse ci-après me conduira à vous proposer un mode d'action.

La Ville de paris s'est attachée depuis la publication de la loi du 6 janvier 1978 à instaurer dans les services une démarche administrative pour le respect du droit à la protection des données personnelles qui sont contenues dans les dossiers, papier ou informatisés.

A l'époque chaque direction avait reçu pour instruction de désigner une personne pour conseiller lors de la mise en œuvre des applications. Ce travail n'a pas été vain.

La loi du 6 août 2004 et son décret d'application du 20 octobre 2005 ont, précisé le domaine d'intervention de la CNIL dont son pouvoir de contrôle et de sanction et créé la fonction de Correspondant informatique et libertés (CIL).

La ville de Paris a désigné en 2006 un correspondant parmi ses cadres expérimentés ayant le rang de sous directeur et œuvré dans différents domaines dont la gestion du personnel et l'informatique.

La mise en œuvre du fichier des applications a été facilitée par l'existence d'éléments détenus dans les directions et une récupération des déclarations détenues par la CNIL. Une communication précise a été faite en direction des services. Il a été noté que ceux-ci ont accueilli très favorablement la désignation du correspondant et ont répondu aux sollicitations.

Plusieurs actions ont été menées, par la suite, pour s'assurer de l'exhaustivité du recensement des fichiers et applications. Le nombre actuel est de plus de 590 (CASVP inclus).

Chaque mois de nouveaux éléments sont ajoutés ou actualisés.

Les services ont pris pleinement conscience de leur responsabilité et associent le correspondant aux projets.

Cependant le travail effectué se heurte à certaines limites. Le rapport de la CNIL suite au contrôle de la DEVE en est un condensé.

La première est l'ancienneté de certaines applications dont certaines fonctionnalités ne sont plus utilisées voire ne l'on jamais été. Il faut analyser une application tout au long de son cycle de vie.
Ce fut le cas du contrôle effectué par la CNIL à la DEVE alors que l'usage du logiciel existait depuis de nombreuses années sans qu'une utilisation anormale ait pu être retrouvée.

La seconde est le développement des outils informatiques de recoupement de données soit en utilisant la bureautique soit les info centres. Dans ce cas un agent peut, de façon durable être détenteur de données dont le regroupement ou l'analyse ne se justifie qu'à un moment donné. La conservation de tels agrégats présente des risques.

La troisième est le respect du droit à l'oubli donc à l'anonymisation des archives. Cet aspect est fondamental pour la CNIL. Une politique d'archivage numérique doit être définie.

La quatrième porte sur les mesures de sécurité pour l'accès aux données par une connexion simplifiée. Au fil des mois par commodité et par une baisse de la vigilance elles sont de moins en moins respectées (mots de passe). C'est également le cas pour des transferts d'informations qui peuvent être réalisés en clair (pièces jointes aux courriels et fax). Ceci sera d'autant plus important à prendre en compte que la ville développera les télé procédures et services.

Ces points sont probablement ceux qui exposent le plus la Ville à des remarques lors d'un contrôle de la CNIL. De toutes façons, qu'il y ait contrôle ou non, les mesures de sécurité doivent être correctement appliquées.

Instruite de l'expérience de la DEVE, conscient du rôle accru de la CNIL dans les contrôles et de la volonté de son Président d'exercer cette partie de ses compétences de façon plus étendue sur les collectivités locales je pense qu'une action permanente d'inspection peut être envisagée au sein des services municipaux.

Ma proposition consiste à vous demander de confier à l'Inspection générale une mission lui pour analyser les pratiques de chaque direction et formuler des recommandations.

Afin d'être au plus près du respect de la loi Informatique et Libertés tout en prenant en compte la réalité quotidienne du fonctionnement des services je suggère d'associer le correspondant informatique et libertés.

Cette démarche, administrative de la ville et juridique du correspondant, permettra de conforter les services dans la nécessité du strict respect de la protection des données personnelles.

La ville de Paris peut afficher la confiance qu'elle inspire car il est très rare qu'elle soit mise en cause et les demandes des administrés et agents concernant la protection de leurs données personnelles sont exceptionnelles.

Prouvons notre vigilance.

Remarques formulées suite à la lecture du rapport préliminaire de l'Inspection générale.

Ref : 09-23

Page 5 :

S'agissant de l'incident GESPER+ Il me semble qu'il faudrait indiquer qu'il s'agit à l'origine d'un logiciel du marché qui fonctionnait en monoposte.
Cela impliquait une totale indépendance de gestion des informations sur les différents sites.
Ce mode de fonctionnement avait provoqué des remarques du personnel et de certaines organisations syndicales.
La finalité du logiciel était de gérer les roulements sur 14 semaines.
Une faible partie des possibilités techniques étaient utilisée.

La volonté de mise en réseau de l'application a soulevé dans certains centres une réticence voire une opposition.

Lors du regroupement des données aucune anomalie n'a été constatée. Seules des faiblesses d'utilisation ont été mises en évidences tant par le service que par la CNIL.
Le service a immédiatement, avant même le contrôle de la CNIL, préparé les modifications à apporter au logiciel ; soumises ensuite à la CNIL certaines ont été estimées trop restrictives.

La version d'origine de GESPER+ a été soumis à la CNIL en 1999 et non en 2008.
La déclaration avait cependant fait l'objet du recensement adressé par le CIL à toutes les directions pour vérifications et mises à jour.

Page 7 :

Les fichiers manuels, qui n'étaient pas inclus dans la loi de 1978 l'ont été dans celle de 2004.

Les fichiers manuels ne sont pas dispensés de déclaration. Ils doivent être recensés comme les autres. Il est cependant évident que la quasi-totalité a été remplacée par des solutions informatiques.

Page 13 :

Le rapport annuel a été remplacé par un rapport mensuel à madame la Secrétaire Générale. Il ressort de la lecture des modèles de rapport annuel que la valeur ajoutée est faible car trop éloignée d'un événement.

La CNIL et l' AFCDP réfléchissent actuellement sur une formulation plus adaptée. Cela sera probablement nécessaire si la loi prévoit l'envoi systématique à la CNIL.

Le rapport mensuel permet de suivre l'actualité, de solliciter une intervention des autorités et de donner du sens à la démarche de la Ville dans la protection des données personnelles.

S'agissant de l'information il faut citer en premier le CTP central de juin 2006 qui a officialisé la création du CIL. L'information préalable des organisations représentatives des personnels est un point de passage obligé.

Monsieur avait donné son accord pour la création d'une page spécifique pour le CIL et l'information sur les obligations.
Ce point n'a pu être mis en œuvre face au refus réitéré des responsables du site web et Intranet. Ceci explique la difficulté relative mais réelle de trouver les informations. Cela n'a pas permis de développer cette rubrique au profit des personnes devant gérer des fichiers comportant des données personnelles.

Par ailleurs, comme le souligne le rapport les information sont été supprimées dans Intranet sans en informer le CIL.

Lors de la nomination le CIL a récupéré le fichier de la CNIL. Il était en mode texte et du être intégralement repris en saisie manuelle.
Ce travail effectué pour chaque application recensée a fait l'objet d'une fiche reprenant tous les éléments détenus par la CNIL.
Ces fiches ont été adressées aux CIT des directions pour vérification et mise à jour.
Le taux de retour a été satisfaisant et a surtout permis de nouer les premiers contacts.

Ils ont été suivis de plusieurs interventions du CIL dans les réunions regroupant les CIT puis dans le COSI. S'agissant de cette dernière instance le CIL intervient dès qu'un élément nouveau apparaît.

La demande d'intervention de la CNIL sur des projets a effectivement été limitée à quelques cas. Cependant le CIL a eu recours à des consultations informelles avec le service réservé aux CIL afin d'affiner son analyse sur des dossiers particuliers.
Il a également suivi les cycles de formation dispensés par la CNIL portant sur différentes thématiques.

Il ressort que les problèmes de la Ville de Paris sont assez souvent particuliers en raison des volumes et de l'organisation par arrondissement sans oublier la double compétence ville et département. La participation à certains travaux d'APRONET, association regroupant les CIL des conseils généraux a mis en évidence certaines particularités.

Page 17 :

S'agissant des « télé services » il faut préciser que l'avis préalable de la CNIL est obligatoire.

Peut on préciser le sens de la phrase commençant par : « Il ne faut cependant pas,….. ».

Page 19 :

Dernier paragraphe : les CIT ont été choisis comme constituant le premier maillage du réseau du CIL. Ils ont une connaissance des problèmes des directions. Ce maillage s'est ensuite étendu aux responsables des projets et ensuite aux personnes gérant au quotidien les informations contenues dans les fichiers.

Le réseau de spécialistes s'est ainsi étendu aux utilisateurs.

Page 20 :

Sur la formation je reprends les restrictions qui ont été imposées au CIL quant à l'usage d'Intranet pour donner en ligne les modes d'emploi complet et évolutifs.

Par ailleurs, dans plusieurs cas le CIL a pu constater que les informations (même issues du SG) n'étaient pas diffusées ou que l'importance des questions CNIL n'a pas été véritablement prise en compte.

Le CIT référent CIL ne peut se substituer au CIL ne serait-ce que par sa dépendance hiérarchique. Il ne peut être qu'un point d'accès vers le CIL ou pour le CIL.
Le CIL a eu à plusieurs reprises l'occasion de s'opposer à des projets ou d'en demander la modification, voire des ajouts de fonctionnalités comme la purge et l'anonymisation.

Page 21 :

L'évaluation des risques par les directions est d'autant plus faible que celles-ci comportent des unités décentralisées. L'exemple récent du centre Michelet (reconnaissance par empreintes) est là pour en témoigner. La notion de dépendance d'une voie hiérarchique est parfois atténuée.

Page 24 :

S'agissant de l'opinion de la DAC il faut noter que la responsable informatique est nouvelle et que des liens étroits avaient été liés avec la personne précédente. S'agissant de la DJS il y a peu d'affaires mais il y a toujours eu un contact.

Par contre la stabilité des agents (DASCO et DPE) permet d'utiliser les documents réalisés dès le début par le CIL pour déclarer ou modifier une déclaration.

Le retour d'informations se fait par e-mail ; comme la saisine du CIL. Il y a toujours un retour mais est il communiqué à l'environnement et archivé dans le dossier ?
Pour des cas plus délicats le CIL se rend sur place et demande une démonstration (Laboratoire Saint Marcel, Centre Charles Moureux, DRH).

Page 25 :

S'agissant de recensement tout fichier comprenant des données personnelles doit être recensé (à distinguer de la déclaration). En effet tout citoyen est en droit de connaître s'il est dans un ficher et quelles sont les données le concernant. Cela suppose une centralisation de la liste des fichiers. C'est d'ailleurs un des buts de la liste tenue par le CIL.

Il y a une confusion pour les services qui croient que les dispenses et autres procédures allégées suppriment l'enregistrement.
Il n'en est rien du fait qu'un contrôle doit être fait sur ces fichiers en amont pour vérifier s'ils entrent bien dans la catégorie indiquée.

Il est cependant illusoire de croire à la réalité et à l'efficacité d'un recensement exhaustif. Il faut se rattacher à la notion de métier et de dépendance du ficher par rapport au métier. C'est la position d'

S'agissant de l'actualisation on constate que les application ont une stabilité dans le temps. Celles qui ont le plus évoluées concernant la DASES, la DDATC et dans une moindre mesure la DRH.

Le facteur déclenchant est souvent d'ordre législatif ou réglementaire.

Les applications « locales » et « spécifiques » évoluent peu ou alors sont remplacées.

Page 26 :

Dans le tableau je m'étonne de ne pas voir figurer la DU, la DF et la DICOM.
Ces trois directions ont des données concernant le public.
Je rappelle que la DU fait deux fois par semaine des publications sur le BMO et Internet. D'ailleurs celles-ci ont généré des plaintes en cours de traitement.

Je signale également une plainte récente d'un agent dont le nom figure sur des résultats de concours publiés au BMO et par voie de conséquence sur Internet.

Il faut revoir notre mode de publication d'informations comportant des éléments personnels en se limitant aux données obligatoires. La version papier devient alors le seul support complet.

Pour la DDATC je m'étonne de la proportion du fait de l'Etat civil et des conseils de quartier sans oublier les mairies.

Page 27 :

Faute de frappe dans le tableau de droite.

Page 28 :

Il aurait fallu citer les directions et applications utilisant le NIR. C'est un point majeur de la compétence de la CNIL. L'application relève soit de l'autorisation soit de l'avis. En aucun cas le CIL peut autoriser.

Seule la MDPH, pour laquelle je suis correspondant mutualisé peut utiliser le NIR dans une application récente car le texte de loi le prévoit.

Page 31 :

Pour l'export de données j'ai soumis récemment à la CNIL pour avis la mise en place de relations avec La CNIL étudie cette question en ce moment et la proposition de loi actuellement en discussion veut clarifier la qualification de l'adresse IP en la réputant donnée personnelle.

Un projet de commercialisation de données publiques est soumis au Conseil de Paris. Il convient de s'assurer des modalités de réemploi et de la conformité avec la loi I&L pour les données personnelles (art 12 ordonnance de 2005). Le Cil doit être associé.

Page 32 :

La destruction de données ou l'anonymisation sont rarement pris en compte dans les logiciels du marché.

J'ai du pour le projet SALSA imposer le traitement de cette question alors que les conseils généraux qui l'utilisent ont fait l'impasse. Ceci est très étonnant.
Il a en été de même pour « facile famille ».

Courrier du 31 mai 2010 du Directeur des systèmes et technologies de l'information

MAIRIE DE PARIS Direction des Systèmes et Technologies de l'Information

N/Ref : D10001093

Paris, 31 mai 2010

NOTE à l'attention de : Madame
Inspection Générale

INSPECTION GENERALE DE LA VILLE DE PARIS
- 2 JUIN 2010
N° 186

Objet : **Réponses au rapport provisoire d'audit de fichiers informatiques de la Ville et du Département de Paris (n°09-23)**

Je vous remercie de l'envoi du rapport préliminaire de vos services concernant d'audit de fichiers informatiques de la Ville et du Département de Paris.

Le rapport complété des remarques formulées par Monsieur , Correspondant Informatique et Libertés, dresse un état des lieux fidèle de la situation de la Ville au regard de la loi informatique et Libertés, et je partage pleinement le diagnostic sur les pistes d'amélioration identifiées.

Mes observations concernent les points suivants :

1- Il me semble que des risques existent pour certaines applications au niveau de l'archivage, de la purge (droit à l'oubli) des données ainsi que des champs en saisie libre : ils pourraient exposer la Ville à de nouvelles difficultés au vu du développement croissant des télé-services et de la sous-traitance. Les mesures complémentaires évoquées dans le rapport sont pertinentes mais il me semble qu'elles gagneraient à être accompagnées par un plan d'action global au niveau de la DSTI (pour l'archivage et les purges) validé annuellement par le CIL.
2- La désignation de référents I&L est une proposition intéressante mais qui peut se révéler suffisante pour instruire et résoudre les difficultés. La piste du renforcement de la prise en compte de la Loi Informatique et Libertés dans le cycle de vie des projets, devrait être explorée en parallèle. En particulier, il conviendrait d'élaborer un document de synthèse !&L pour chaque application à réaliser qui serait intégré aux dossiers de lancement des projets en CL@P ou en CSSI.
3- Un processus garantissant une parfaite conformité des applications réalisées avec leur déclaration CNIL devra être défini. Par exemple lors de la mise en production de l'application, une analyse de conformité sera effectuée et formalisée dans un document adressé pour accord au CIL pour les projets importants et au référent I&L pour autres applications.
4- En collaboration avec la DA, un corpus d'exigences dans les marchés pour la protection des données nominatives notamment pour les phases de recette et de reprise de données sera élaboré. Ce cadre pourrait utilement être défini techniquement par la DSTI en coordination étroite avec le CIL.
5- La refonte de l'application CATIA en 2011 sera l'occasion de disposer d'un inventaire exhaustif des applications opérées par la DSTI facilitant le suivi de la conformité des applications à leur déclaration CNIL dont un rapport sera adressé pour accord au CIL et aux référents concernés.
6- Outre l'assistance juridique de la DAJ évoquée dans le rapport, l'audit régulier des systèmes les plus sensibles ou ayant fait l'objet d'un incident par l'Inspection Générale voire un échantillon représentatif des autres traitements me semblent extrêmement opportunes car elles permettront de mesurer le niveau d'exposition aux risques et de maintenir un niveau de vigilance suffisant.

Directeur des Systèmes et Technologies de l'Information

DSTI - 227 rue de Bercy - 75570 Paris Cedex 12
Tél. : 01 43 47 65 43- Fax : 01 43 47 68 65