



Le correspondant CNIL à la protection des données personnelles (CDP) : Responsabilités, indépendance et protection

Actes du séminaire du 21 mars 2006

INTRODUCTION

Une des grandes caractéristiques de notre société de l'information et de la communication est la généralisation du stockage de fichiers informatiques aussi bien pour les consommateurs que pour les salariés. La loi du 6 août 2004 et le décret d'application du 20 octobre 2005 ont mis en place une institution très originale dans l'entreprise, le correspondant aux données personnelles (CDP), appelé aussi le correspondant Informatique et libertés (CIL). Dorénavant les entreprises peuvent se voir dispensées de déclaration de certains fichiers à la CNIL, à condition de désigner ce référent.

Dans notre pays très jacobin, cette institution constitue un changement culturel important et suscite quelques questions :

- > Quel est le bon profil d'un CDP, quelles compétences doit-il réunir, qui sont les premiers CDP nommés ?
- > Quelles sont les prérogatives du CDP et comment garantir son indépendance, condition nécessaire à la bonne marche du poste ?
- > De quelles protections et de quel droit d'alerte dispose le CDP ?
- > Plus largement, de quelles protections bénéficient les personnes qui porteront recours devant le CDP ?

Nous avons la chance de recevoir ce soir Nathalie Metallinos, madame CDP à la CNIL et Jean-Emmanuel Ray, professeur à Paris 1 et à Sciences Po Paris, spécialiste des TIC en droit social mais aussi ardent défenseur du droit à la déconnexion, qui présentera quelques traits critiques de la fonction de CDP, ce qui nous permettra de comprendre les difficultés d'exercice de cette nouvelle fonction et ouvrira la discussion sur les règles qui doivent permettre d'en encadrer l'exercice pour garantir la protection des salariés et des données individuelles mais aussi la cohabitation de cette nouvelle institution avec les organisations syndicales et les instances de représentation du personnel.

Nathalie Metallinos, cinq mois après le décret d'application, pourriez-vous nous présenter les grandes innovations du CDP et les profils des premiers CDP nommés, que vous avez réunis récemment ?

Jean-Emmanuel Ray, vous avez esquissé un portrait exigeant du CDP qui est un mouton à cinq pattes chargé d'insuffler une culture « Informatique et libertés » : vous nous exprimerez vos interrogations.

Le temps sera aussi laissé au débat car les questions sont nombreuses sur cette nouvelle institution ainsi que sa cohabitation avec les organisations syndicales et les représentants du personnel, également garants de la protection des libertés individuelles et collectives dans l'entreprise.

Le point de vue de la CNIL

Nathalie METALLINOS

Juriste, responsable de la cellule « correspondants aux données personnelles » de la CNIL

Je vous présenterai d'abord le décret et son esprit, avant de faire un rapide portrait de la petite centaine de CDP qui ont déjà été nommés.

Je souhaite, à travers cette présentation, vous convaincre :

- > de l'importance du changement de culture à l'œuvre en matière de préservation des données individuelles,
- > de la grande richesse de la fonction de CDP,
- > des conséquences sur le profil des correspondants.

L'esprit de la nouvelle loi Informatique et libertés : un changement de culture

Avant de détailler la fonction de correspondant à la protection des données, j'aimerais revenir sur l'esprit de la nouvelle loi informatique et libertés et ce qu'elle comporte de changement culturel.

Ce qui est primordial dans la nouvelle loi, c'est l'idée qu'il faut passer d'un système légal centralisateur, où l'on déclare les traitements « pour être en règle », à un système qui permette à ceux qui mettent en œuvre et manipulent des traitements informatiques de prendre conscience de la portée de certaines informations détenues au regard du respect de la liberté individuelle et d'agir ainsi en acteurs responsables. C'est dans cet esprit qu'a été créée la fonction de correspondant aux données personnelles. Il faut ici rappeler que, s'il s'agit pour la France d'une innovation, nous n'avons pas pour autant décidé seuls d'une révolution culturelle. Ce dispositif responsabilisant a déjà fait ses preuves, sous différentes modalités pratiques, dans d'autres pays européens (Allemagne, Pays-Bas, Suède...) : nous ne partons pas totalement à l'aventure et bénéficions ainsi de l'expérience de nos voisins européens.

Ce préambule sur l'esprit de la loi est important car il permet d'éviter d'emblée deux faux débats :

- > le CDP n'est pas « l'œil de Moscou » au service de la CNIL ;
- > ce n'est pas non plus « la bonne conscience » des entreprises ou organisations qui se contenteraient de nommer un CDP pour alléger leurs formalités déclaratives.

C'est notamment pour ces deux raisons que la nomination d'un correspondant à la protection des données personnelles est facultative : il s'agit d'une démarche volontaire effectuée par les organisations et acceptée par les personnes nommées. C'est un gage de l'implication de ces organisations en faveur du changement culturel proposé par la nouvelle loi Informatique et libertés.

Le CDP n'est donc pas là pour bloquer le travail des responsables des traitements mais pour veiller à ce que la loi soit bien comprise et respectée. Il doit donc être aussi force de proposition pour que les systèmes d'information soient performants dans le respect de la loi Informatique et libertés. Il s'agit de mettre l'informatique à sa place, au service de l'homme et non l'inverse.

La richesse de la fonction de correspondant aux données personnelles

Le rôle de CDP tel que nous l'entendons est d'une grande richesse. Le CDP a de fait trois fonctions majeures : il est garant de la loi, ambassadeur de l'esprit de la loi et force de proposition.

- > En tant que garant de la loi Informatiques et libertés, la première tâche du CDP consiste à recenser l'ensemble des traitements automatisés et à s'assurer que les personnes concernées sont correctement informées de leur droit vis à vis des informations détenues. Ce recensement, qui doit pouvoir être présenté à la CNIL, doit être réalisé dans les trois mois suivant sa nomination et tenu à jour.

Le CDP doit aussi se charger des formalités liées aux traitements qui demeurent soumis à une obligation de déclaration.

C'est aussi lui qui, dans le respect du secret professionnel, traitera les demandes de renseignements et les éventuelles plaintes internes à l'organisation au sujet du respect de la loi sur la protection des données individuelles. Il jouera alors un rôle de médiateur entre les « plaignants » et le responsable des traitements ; il pourra aussi en cas de difficultés saisir la CNIL.

- > Toutefois, l'apport essentiel de cette nouvelle fonction réside dans le rôle d'ambassadeur de la culture Informatique et libertés que le CDP doit jouer. Sur cet aspect, le CDP doit agir en amont des difficultés pour les éviter. Il lui revient donc d'informer et de mener toute action pédagogique qu'il jugera utile pour sensibiliser ses collègues à la protection des données. Sur cet aspect, comme pour l'ensemble des tâches qu'il a à accomplir, le CDP est autonome : il n'a pas à attendre d'être

missionné par le responsable des traitements ou la direction pour mettre en place ses actions de sensibilisation et promotion de la loi. La CNIL tient beaucoup à cette fonction d'ambassadeur/pédagogue. La plupart des salariés n'est bien souvent pas conscient de l'importance de la préservation des données personnelles : aussi bien en ce qui concerne la préservation de leurs propres données que de la portée des informations qu'ils peuvent eux-mêmes détenir et recueillir sur des collègues, des subordonnés, des clients, des fournisseurs... Au delà des traitements automatiques, c'est l'ensemble des pratiques de recueil et de tri des données qu'il faut interroger. Les actions de sensibilisation menées par les CDP doivent permettre à chaque salarié d'adopter le réflexe « Informatique et libertés » et donc de prévenir les dérapages liés à la méconnaissance du sujet.

- > Enfin, le CDP est aussi force de proposition. Après avoir mené le recensement des traitements et contribué à la sensibilisation de l'ensemble des salariés, le correspondant aux données personnelles est aussi sollicité pour mener des audits sur les pratiques de recueil et de traitement des données ; il peut être amené à formuler des propositions afin que les traitements soient en conformité avec la loi. Pour être efficaces dans ce domaine ; les propositions émises par le correspondant doivent à la fois tenir compte des besoins exprimés par les personnes cherchant à mettre en place un système de récolte des informations et des droits des individus garantis par la loi.

La fonction de correspondant aux données personnelles est une fonction stratégique et complexe qui nécessite à la fois une prise en compte organisationnelle de la nécessaire autonomie du CDP et un profil individuel marqué par quelques savoir-faire et savoir-être indispensables à la bonne tenue du poste.

Spécificités liées à la fonction et profil des CDP

Parce que le CDP est amené à poser un regard critique sur les traitements mis en place dans l'organisation et sur les projets en cours, il doit pouvoir porter un regard neutre et non partisan sur ceux-ci. Bien évidemment, parce qu'il est impossible d'être juge et partie, le CDP ne peut donc pas être le responsable des traitements. Voilà donc une fonction très technique (il faut bien comprendre les processus et les spécificités techniques des traitements en question) qui nécessite aussi une grande autonomie. La loi prévoit ainsi que le CDP bénéficie d'une grande indépendance : en clair, une fois nommé, le CDP « s'auto-missionne » et personne au sein de l'organisation ne peut interférer dans ses missions. Le

décret d'application qui fixe les conditions de la nomination et le cas échéant de la révocation du CDP ainsi que des conditions d'exercice de la fonction est assez précis pour permettre l'exercice serein de cette indépendance. Je vous ferai grâce de la lecture du décret, mais je rappelle quelques points importants :

- > Sur la nomination du correspondant. il faut rappeler le caractère facultatif d'une telle nomination ; les instances représentatives du personnel doivent être informées ainsi, bien évidemment, que la CNIL.
- > Sur les conditions d'exercice de la fonction. Je ne reviendrai pas davantage sur des points que j'ai développés concernant la nécessité de ne pas être juge et partie, mais je rappelle tout de même que le décret est précis sur ce qu'il faut entendre par « indépendance » : le CDP ne reçoit aucune instruction sur ce qui relève de ses missions. Je précise, et la question reviendra sûrement dans le débat, que le correspondant n'est pas un salarié protégé. En revanche, et pour s'assurer que le CDP bénéficie de l'indépendance nécessaire, l'employeur ne peut pas dessaisir le correspondant de ses responsabilités sans en avoir informé la CNIL et reçu un avis, certes non contraignant, de celle-ci. Je rappelle aussi que la nomination d'un correspondant à la protection des données n'exonère pas l'organisation et son représentant légal de poursuites pénales et civiles en cas de manquements constatés à la loi.

D'un point de vue organisationnel, tout doit donc être fait pour assurer au correspondant l'indépendance et les moyens nécessaires à la réalisation de ses missions.

Du point de vue de la gestion des ressources humaines, il faut aussi s'assurer que le correspondant ait les qualifications nécessaires pour endosser ses responsabilités. C'est aussi important pour l'organisation puisque sa responsabilité juridique reste engagée.

J'ai déjà mentionné que le CDP devait avoir des compétences techniques en matière informatique et de gestion des systèmes d'information mais, de par sa fonction de garant de la loi, il doit aussi avoir des compétences et en tout état de cause un goût prononcé pour la matière juridique : comment mener à bien son rôle d'ambassadeur de la loi s'il n'en est pas familier ? D'autre part, le correspondant doit aussi avoir une certaine expérience ou du moins une certaine appétence pour la pédagogie et la diplomatie.

En termes de « savoir-être », le CDP ne doit agir en « shérif solitaire » : il ne doit pas perdre de vue l'intérêt de l'organisation qui l'emploie (ou le missionne dans le cas d'un CDP extérieur à l'organisation). Les correspondants à la protection des données personnelles doivent ainsi faire preuve d'indépendance et donc ils doivent pouvoir le cas échéant

s'affirmer face aux cadres dirigeants, mais il doit aussi faire preuve de discernement et évidemment de discrétion face aux informations qu'il aura lui aussi à traiter.

Ce portrait idéal du CDP que je viens de dresser fait dire, je le sais, à Jean-Emmanuel RAY que nous cherchons un mouton à cinq pattes... Je conclurai en rappelant qu'il y a déjà une centaine de correspondants qui découvrent leur nouvelle fonction. Nous les avons récemment réunis et je dois dire qu'ils ont des profils assez diversifiés. Ce sont des personnes qui ont de l'expérience et qui proviennent le plus souvent des fonctions informatiques, actuellement 45% ou bien des fonctions juridiques, 30 à 40%. Il est évidemment beaucoup trop tôt pour tirer des conclusions quant aux profils qui donnent pleinement satisfaction. L'objectif de la cellule dont je suis responsable est d'accompagner au mieux le développement de cette nouvelle fonction qui se crée et s'organise.

Le CDP, premières questions

Jean-Emmanuel RAY

Juriste, professeur à Sciences Po et à Paris 1

Tout d'abord je souhaite saluer madame METALLINOS dont l'intervention permet de parfaitement situer les contours de la fonction de CDP. Elle ne peut pas le dire, mais elle est à elle seule la cellule de la CNIL « correspondants aux données personnelles ».

Car il ne faut pas imaginer que la CNIL est une haute autorité dotée de moyens super-puissants... Ils sont environ 80 agents permanents, autant vous dire que leurs moyens sont limités pour mettre en œuvre les investigations nécessaires pour s'assurer de l'application de la loi. Au fil des ans et de la croissance, exponentielle, des informations traitées, la CNIL est finalement devenue un bureau d'enregistrement des déclarations. Je suis féroce, j'exagère à peine et l'on sait que les traitements « *borderline* » mal protégés, non déclarés, sont légion, y compris pour les fichiers des organisations syndicales ou des comités d'entreprise.

Avant de reprendre quelques éléments de l'intervention de Nathalie METALLINOS, je voulais rappeler la pauvreté de la CNIL pour tempérer les propos sur la primauté du changement culturel. Il me semble qu'il s'agit avant tout d'alléger le flux de déclarations plus ou moins complètes et pertinentes qu'ont à traiter les agents pour qu'ils puissent enfin se concentrer aux problèmes de fond posés par la nécessité qu'il y a aujourd'hui de préserver les données individuelles, alors même que techniquement tous les abus semblent possibles.

Le propos général est un bon décret, qui prévoit « en délicatesse » les conditions nécessaires à l'indépendance du CDP mais demeurent trois zones d'ombre :

- Un cadeau pour les entreprises ? L'intérêt de la CNIL, c'est qu'il y ait beaucoup de désignations de CDP. La CNIL prévoit ainsi un régime de faveur pour les organisations dotées d'un CDP. Outre l'allégement des formalités, on peut envisager le traitement plus rapide des dossiers concernant les déclarations qui demeurent obligatoires, dès lors qu'il y a la désignation d'un interlocuteur privilégié. Ce cadeau pour les entreprises correspond à un transfert de charge de la part de la CNIL au CDP, charge pour lui d'établir et d'actualiser les traitements des déclarations mais aussi de coordonner ces listes dans les différents services de l'entreprise : RH, SI, services clientèles. Le CDP est aussi chargé de gérer les demandes d'autorisation ou de transfert de données personnelles hors de l'union européenne. Il faut rappeler que l'absence de déclaration de ces transferts peut entraîner une peine de 300 000 euros mais que la désignation du CDP n'exonère pas pour autant l'entreprise, même s'il

bénéficie d'une délégation de pouvoirs. Le CDP n'est pas là pour blanchir certains fichiers.

- Les qualifications des CDP en font un « mouton à cinq pattes » : il est tout à la fois, conseil, audit, pédagogue, médiateur mais doit aussi pouvoir mettre en garde les responsables du traitement contre d'éventuelles illégalités. Il faut donc prévoir de quelles formations et de quel appui ils auront besoin. Seront-ils en proximité de façon privilégiée avec la Direction des ressources humaines ou avec celle des Systèmes informatiques ? Par ailleurs le décret précise que la désignation doit s'accompagner de « tout élément relatif aux qualifications ou références professionnelles ». La CNIL pourrait donc contester le choix de certains CDP, insuffisamment qualifiés ;
- Face à la multiplication des traitements et des systèmes d'information de plus en plus intrusifs, le CDP est une petite goutte ; sera-ce suffisant pour insuffler à cette nouvelle institution un véritable changement culturel conforme à l'esprit Informatique et libertés ?
- Concernant la concurrence avec les IRP, il faut signaler qu'ils sont absents dans la loi et juste informés de la désignation du CDP. De plus, le CDP pourrait leur rappeler leurs obligations concernant la déclaration de leurs propres fichiers. Il peut néanmoins devenir un allié pour les questions d'utilisation d'internet ou courriels, mais aussi pour les listes électorales ou à l'occasion de l'organisation des votes électroniques.