

DONNEES PERSONNELLES

Citation : Eric A. CAPRIOLI, Avocat à la Cour de Paris, Docteur en droit et Isabelle Cantéro, Juriste, Responsable du Département Vie privée et données personnelles, Caprioli & Associés, Données personnelles, www.caprioli-avocats.com

Première mise en ligne : septembre 2006

Le Correspondant à la protection des données à caractère personnel : un nouvel arbitre pour l'entreprise

Eric A. CAPRIOLI, Avocat à la Cour de Paris, Docteur en droit et Isabelle Cantéro, Juriste, Responsable du Département Vie privée et données personnelles, Caprioli & Associés (Paris, Nice)

[www. caprioli-avocats.com](http://www.caprioli-avocats.com)

contact@caprioli-avocats.com

Plan

LE CORRESPONDANT A LA PROTECTION DES DONNEES DEVRAIT FACILITER LES DEMARCHES DES ENTREPRISES VIS-A-VIS DE LA CNIL

PAS DE PROFIL TYPE REQUIS, MAIS DES CONNAISSANCES EN INFORMATIQUE, EN DROIT ET SUR L'ENTREPRISE SONT RECOMMANDEES

LE CORRESPONDANT A LA PROTECTION DES DONNEES SERA-T-IL PRIS ENTRE " LE MARTEAU ET L'ENCLUME "

UN ROLE A GEOMETRIE VARIABLE ET DES RESPONSABILITES QUI RESTENT ENCORE A DETERMINER

DANS LES GRANDES ENTREPRISES LE C.P.D.C.P. S'IMPOSE, DANS LES PETITES CELA SE DISCUTE

I/ REGIME JURIDIQUE DE L'ENTREPRISE QUALIFIEE DE FOURNISSEUR D'ACCES

La loi n° 2004-801 du 6 août 2004^[1] relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel était très attendue. Elle transpose la directive européenne n°95-46 du 24 octobre 1995, en se pliant à la même logique de recherche d'un équilibre entre la circulation des données à caractère personnel et la sauvegarde de droits fondamentaux de la personne. Elle consacre le principe de libre circulation des données à caractère personnel au sein de l'Union européenne. Il faut tout de même rappeler que la désignation de ce type de correspondant existe depuis plus de vingt ans dans certains pays de l'Union Européenne et notamment en Allemagne.

Jusqu'à l'adoption de la nouvelle loi, toute collecte et traitement de données personnelles devaient faire l'objet d'une déclaration préalable auprès de la CNIL en fonction de sa finalité. Les responsables de traitement qui n'accomplissaient pas les formalités légales requises s'exposaient à des sanctions pénales. Récemment, le principe de l'obligation de déclaration préalable a eu d'importantes conséquences en matière sociale. Ainsi, un arrêt en date du 6 avril 2004^[2] de la chambre sociale de la Cour de cassation a précisé les conséquences juridiques, pour l'employeur, du défaut de déclaration auprès de la CNIL de la mise en œuvre d'un traitement automatisé de données à caractère personnel. L'arrêt confirme que le licenciement d'un salarié est sans cause réelle et sérieuse en raison du défaut de déclaration d'un système de contrôle automatisé des entrées et sorties des salariés à l'aide de badges. Le licenciement se fondait sur les refus répétés du salarié de se soumettre au contrôle mis en place. Pourtant, à la lecture de la décision, il apparaît que l'obligation de contrôle était consignée dans le règlement intérieur de l'entreprise. Or, le non-respect de l'obligation de déclaration du système incombant à l'employeur a pour effet de le priver de toute possibilité de sanction à l'égard du salarié contrevenant.

Les règles relatives à la protection des données sont d'ordre public ! En cas de non respect, ces règles sont pénalement sanctionnées.

En matière de données à caractère personnel, d'autres dispositions doivent être prises en compte par les acteurs de l'économie numérique, spécialement les données biométriques (empreinte digitales, iris,...)^[3] et celles collectées à des fins de prospection commerciale^[4]. Un arrêt de la Cour de cassation, chambre criminelle, du 14 mars 2006, vient de décider que l'aspiration d'adresse e-mails était contraire à la loi Informatique, Fichiers et Liberté^[5]. La décision se fonde sur la version de la loi antérieure au 6 août 2004, mais la solution vaut pour la nouvelle loi qui impose le consentement préalable des personnes. La collecte est jugée déloyale, dès lors qu'elle est faite à l'insu des " personnes physiques sur l'espace d'internet, ce procédé faisant obstacle à leur droit d'opposition. " .

Mais on peut citer d'autres domaines comme les alertes éthiques qui imposent une analyse où les questions relatives aux données personnelles se mêlent à la problématique du droit du travail (pour une ordonnance de retrait du dispositif d'alerte, voir TGI Libournes du 15 septembre 2005)^[6].

LE CORRESPONDANT A LA PROTECTION DES DONNEES DEVRAIT FACILITER LES DEMARCHES DES ENTREPRISES VIS-A-VIS DE LA CNIL

Parmi les changements majeurs qui sont intervenus, la loi nouvelle institue la faculté de désigner des correspondants à la protection des données à caractère personnel ("C.P.D.C.P.") ou mal dénommée par certains au travers de l'acronyme " C.I.L. " (Correspondant Informatique et Libertés). Cette mesure innovante, mais que l'on trouve à l'article 18 de la directive du 24 octobre 1995 (qui parle de " détaché à la protection des données à caractère personnel "), est destinée à faciliter les formalités préalables de mise en œuvre des traitements des données courantes. La désignation d'un " C.P.D.C.P. " concerne les données non sensibles qui font l'objet d'un traitement et qui sont soumises aux procédures de déclarations ordinaire et simplifiée. Ainsi, après avoir mis en place une véritable généralisation des pouvoirs de contrôle a posteriori de la CNIL (en dépit de son absence de moyens humains et financiers !), le nouveau dispositif allège les procédures de déclaration des traitements de données à caractère personnel. A l'instar de certains autres Etats membres comme l'Allemagne où la désignation de ce type de correspondant est obligatoire depuis plus d'un quart de siècle, la loi française institue un intermédiaire entre l'autorité de contrôle (la CNIL) et les responsables de traitements (entreprises, associations, administrations, collectivités territoriales,...). L'institution de " C.P.D.C.P. " constitue

justement une dispense au principe de déclaration obligatoire[7].

Le décret d'application du 20 octobre 2005[8] fixe le cadre juridique du " C.P.D.C.P. ". Son titre III, intitulé " Des correspondants à la protection des données ", comporte quatorze articles[9].

Le nouveau décret lève le voile sur certaines zones d'ombre de la loi. En l'occurrence, il est désormais établi que le correspondant peut être choisi à l'extérieur de la structure qui met en œuvre les traitements de données à caractère personnel. Mais le décret reste complexe et, chaque avancée comporte sa propre limite, une nouvelle zone d'incertitude.

Il convient toutefois de rappeler avec force que la protection des données à caractère personnel s'inscrit plus largement dans une démarche de mise en conformité (" compliance ") juridique que ce soit pour le respect d'une obligation légale (ex : Règlement CRBF 97-02 pour les banques)[10], pour le contrôle interne ou pour le respect des règles de droit. Mais il ne faut pas non plus occulter que le respect des règles " Informatique et Libertés " s'impose dans le cadre d'une politique de bonne gestion des droits et libertés des personnes qui sont en relation avec l'organisation en cause : salariés, clients et prospects, fournisseurs (pour l'entreprise), ...

Ainsi, les articles 42 à 45 traitent des modalités de la désignation du correspondant (dont la notification à la CNIL), les articles 46 à 51 des conditions d'exercice de sa mission, et enfin les articles 52 à 55 de la fin de la fonction.

PAS DE PROFIL TYPE REQUIS, MAIS DES CONNAISSANCES EN INFORMATIQUE, EN DROIT ET SUR L'ENTREPRISE SONT RECOMMANDEES

Pour les données à caractère personnel peu sensibles ou courantes (par exemple en matière de gestion du personnel), l'article 22-III de la loi dispense de la formalité de déclaration préalable les entreprises qui auront désigné un correspondant à la CNIL (" C.P.D.C.P. "). Cette faculté est applicable au secteur privé et à la sphère publique (administrations, établissements publics et collectivités locales[11]). La désignation du " C.P.D.C.P. " devra être notifiée à la CNIL, ainsi qu'aux instances représentatives du personnel (préalablement à la désignation et à la notification à la CNIL). Il convient de souligner que la personne désignée comme correspondant doit avoir donné son accord par écrit, lequel sera annexé à la notification (art. 43).

La dispense de déclaration préalable ne concerne pas les traitements de données sensibles (ex : les données biométriques ou relatives à la santé) qui relèvent du régime de l'autorisation ou encore les traitements qui procèdent à un transfert de données à caractère personnel hors des Etats membres de l'Union européenne[12].

La collecte et la gestion de données à caractère personnel relèvent de la sécurité des systèmes d'information en ce sens que les traitements informatiques doivent s'inscrire dans le respect des finalités déclarées et que l'entreprise doit protéger les fichiers constitués contre les atteintes et les accès non autorisés (art. 34 et 35 de la Loi). C'est pourquoi la protection des droits des personnes s'effectue par la mise en place de moyens techniques et organisationnels, ainsi que par des mesures de sécurité informatique.

La loi ne propose pas de véritable définition du correspondant : il s'agit d'une " personne bénéficiant des qualifications requises pour exercer ses missions ". Si rien n'est dit sur les qualifications

professionnelles du " C.P.D.C.P. ", on peut supposer qu'elles relèvent des domaines informatique et juridique, mais aussi de la connaissance du métier et de l'organisation de l'entité.

Cette fonction devrait concerner les groupes d'entreprises qui pourront désigner en interne un correspondant pour l'ensemble du groupe avec des intermédiaires dans chaque société filiale, ou un correspondant pour chaque société filiale, mais aussi les petites entreprises qui externaliseraient de façon mutualisée les fonctions de " C.P.D.C.P. ". Mais, le décret a fixé un seuil au-delà duquel l'externalisation de la fonction sera impossible. Ainsi, aux termes de l'article 44 du décret, la désignation d'un correspondant externe n'est en réalité envisageable que pour certaines structures relativement réduites, qui ont moins de cinquante personnes chargées de la mise en oeuvre ou ayant directement accès aux traitements automatisés de données.

Parmi les personnes externes à l'entreprise, il pourrait s'agir d'un avocat ou d'un conseil spécialisé en protection des données personnelles. De même, si l'impossible cumul des fonctions de responsable du traitement (ou son représentant légal) et celles du correspondant est affirmé (art. 46), rien n'est en revanche précisé quant aux autres incompatibilités dont on ne saurait nier l'existence. N'ouvre-t-on pas, en effet, une possibilité de " conflit d'intérêts " à désigner par exemple le DRH ou le DSI en qualité de correspondant, voire l'avocat qui est le conseil habituel de l'entreprise ?

LE CORRESPONDANT A LA PROTECTION DES DONNES SERA-T-IL PRIS ENTRE " LE MARTEAU ET L'ENCLUME " ?

La CNIL a notamment précisé que " la position hiérarchique du CIL " (le " C.P.D.C.P. ") doit être caractérisée par la possibilité de communiquer directement avec la direction de l'organisme, l'interdiction pour le responsable de traitement d'interférer dans l'accomplissement des missions du " C.P.D.C.P. " et l'absence de conflits d'intérêt avec les fonctions exercées en même temps qui sont de nature à apporter les garanties d'indépendance. Ainsi, à l'évidence, les dirigeants de l'entreprise ne devraient pas pouvoir être désignés comme correspondant[13].

La loi précise que le correspondant doit remplir ses missions " d'une manière indépendante " : il ne peut faire l'objet d'aucune sanction de la part de son employeur du fait de l'accomplissement de sa tâche. Cette dimension peut s'avérer délicate à gérer par l'organisme en cas de conflit ou de litige avec le " C.P.D.C.P. ". Le statut du correspondant ainsi posé soulève quelques réserves. D'une part, l'indépendance du correspondant salarié est perçue comme très relative compte tenu du lien de subordination entre le correspondant et son employeur. La loi ne met pas en place un statut de salarié protégé, réservé aux représentants du personnel et, dans ce cas, le " C.P.D.C.P. " devra servir les intérêts de son entreprise tout en veillant au respect des dispositions légales et réglementaires. Par exemple, en cas de non respect des obligations légales, le correspondant devra en informer la CNIL... Ménager ces deux intérêts pourra donner lieu à quelques difficultés pour le " C.P.D.C.P. ".

UN ROLE A GEOMETRIE VARIABLE ET DES RESPONSABILITES QUI RESTENT ENCORE A DETERMINER

Les missions du correspondant devaient être clairement définies par le décret du 20 octobre 2005. Par comparaison avec les pays dans lesquels ont déjà été mis en place des " C.P.D.C.P. " (comme l'Allemagne, la Suède ou les Pays Bas), la mission du " C.P.D.C.P. " consiste notamment à :

- sensibiliser, réaliser ou faire faire des formations, diffuser des informations relatives à la loi

Informatique et Libertés ; " superviser les traitements mis en œuvre, " établir une liste des traitements dont les éléments à mentionner sont fixés par le décret ; " détecter les problèmes éventuels liés à la mise en œuvre des traitements ; " alerter les autorités de tutelle en cas de problème identifié ou de soupçon sur la conformité d'un traitement.

L'article 47 du décret établit les traitements qui doivent figurer sur la liste, ainsi que les éléments à mentionner pour chacun desdits traitements (art. 48). En outre, la liste doit être mise à jour et elle doit être mise à la disposition de toute personne qui en fait la demande. Certains verront dans cet allègement une simple dispense de la mise sous pli et de l'affranchissement des déclarations à la CNIL, étant donné qu'il y a peu de différence de travail entre la tenue de la liste des traitements soumis à déclaration et l'établissement de la déclaration en tant que telle. A méditer...

Plus généralement, le " C.P.D.C.P. " est investi d'une mission de contrôle des traitements effectués par son entreprise (ou organisme public) et à ce titre, il est chargé d'assurer le respect des obligations légales existantes. Il doit tenir un registre desdits traitements et répertorier les informations nécessaires à toute déclaration préalable à la CNIL.

De fait, il pourra donc être chargé des déclarations auprès de la CNIL pour les données sensibles, soumises à autorisation ou pour les transferts en dehors de l'Union européenne et il devra assurer le suivi des traitements. A quel titre interviendra-t-il ? En tant que " C.P.D.C.P. " ou en tant que délégué du responsable des traitements ? Ce changement du périmètre de responsabilité du " C.P.D.C.P." devra être soigneusement analysé et transcrit dans les documents contractuels applicables au salarié. Si le " C.P.D.C.P. " est un tiers/externe, c'est le contrat de prestation de services qui devra être négocié avec soin.

D'autre part, les contours de la responsabilité du " C.P.D.C.P. " restent flous : il n'est pas responsable au nom de l'entreprise. Toutefois, en cas de fautes ou manquements qui restent à préciser, la CNIL pourra le décharger de ses fonctions. Dès lors, le responsable des traitements devra effectuer les déclarations auprès de la CNIL (ou remplacer le correspondant). De plus, la question reste ouverte d'une éventuelle responsabilité pénale du correspondant. Le responsable du traitement encourt de lourdes responsabilités au regard de l'article 34 de la loi Informatique et Libertés^[14] ou des articles 226-16 à 226-24 du Code pénal. De son côté, le " C.P.C.D.P. " pourrait être soumis à certaines obligations et sa responsabilité pourrait être engagée. Par exemple, s'il n'a pas signalé les précautions nécessaires à prendre en terme de sécurité au responsable^[15]. Mais les réponses restent incertaines et les risques juridiques malaisés à maîtriser.

Lorsque le responsable du traitement envisage de mettre fin aux fonctions de correspondant, soit en cas de manquement aux devoirs et obligations qui lui sont imposés, soit en cas de démission (art. 52 à 55), la saisine de la CNIL est prévue et détaillée (art. 51). Cette fin de fonction " C.P.D.C.P. " sera, selon l'hypothèse retenue, distincte ou non de la cessation du contrat de travail.

DANS LES GRANDES ENTREPRISES LE C.P.D.C.P. S'IMPOSE, DANS LES PETITES CELA SE DISCUTE

La décision de l'entreprise ou de l'organisme correspond à un véritable choix stratégique et organisationnel dont chaque élément doit être pesé. Les risques juridiques ne sont pas négligeables. La démarche pour faire un choix est essentielle, elle s'opère en trois phases :

1°) Analyse/Audit : Il s'agit de faire un inventaire complet des fichiers déclarés et des autres fichiers et d'établir les outils de l'audit (grilles d'audit,...).

2°) Diagnostic : Les différents traitements doivent être qualifiés juridiquement. De la sorte, on pourra déterminer la quantité des fichiers qui relèvent de la compétence du " C.P.D.C.P. " par rapport à ceux qui relèvent de la responsabilité du responsable des traitements.

L'examen portera également sur l'organisation des pouvoirs et des délégations au sein de l'organisation en cause.

En principe, c'est à ce stade que la décision doit se prendre : Désignation auprès de la CNIL ou non ? De quel profil et de quel niveau de responsabilité a-t-on besoin ?

Dans les grandes entreprises, on peut penser que le " C.P.D.C.P. " est une fonction qui doit être exercée par une personne indépendante, chargée d'une mission transversale, par exemple le responsable de la conformité, le responsable de la déontologie, de l'audit interne. Le rattachement devra sans doute être auprès du secrétaire général ou de la direction générale. La fonction ne doit pas être rattachée à une direction qui crée des fichiers et qui fixe leurs finalités.

Dans les plus petites entreprises, il n'y a pas de réponse unique.

3°) Prescriptions : Des modifications contractuelles devront être apportées aux contrats de travail du C.P.D.C.P. et du responsable des traitements. La conformité de leurs délégations devra être vérifiée. La charte informatique nécessitera sans doute des remaniements. Un plan d'actions relatives à la fonction devra être établi : sensibilisation, formation/labellisation, procédures internes, formalités relatives aux traitements, tenue de la liste et/ou des fichiers, bilan " CNIL ", etc.

Les missions peuvent être exercées en interne, sans désignation officielle à la CNIL – une fonction de responsable de la vie privée (" chief privacy officer ") – et partant, non soumise au présent décret. A tout le moins, il reste que les traitements de l'entreprise ou de l'organisme doivent être conformes aux obligations légales et qu'au minimum la fonction de " Responsable Vie privée et Données personnelles" (non assujetti au décret du 20 octobre 2005) doit être assurée au même titre que l'obligation de tenir une comptabilité.

La fonction de responsable des données à caractère personnel qu'il soit " C.P.D.C.P. " désigné auprès de la CNIL ou non, est incontournable ; elle contribue à la protection et à la valorisation des données des personnes, élément essentiel du patrimoine informationnel des entreprises et des organisations publiques.

Pour plus d'information, voir nos articles sur le Correspondant à la protection des données : J.C.P. éd. E, Cahiers de droit de l'entreprise :

Notes

[1] JO. 7 août 2004, p. 14063 et s. Voir la rubrique protection des données personnelles sur le site www.caprioli-avocats.com.

[2] Bull. civ. 2004, V, n°103, p.93 ; décision disponible sur le site : legifrance.gouv.fr.

[3] Ces données doivent faire l'objet d'une demande d'autorisation auprès conformément à ses recommandations.

[4] Eric A. Caprioli, Loi du 6 août 2004 : commerce à distance sur Internet et protection des données à caractère personnel, disponible sur le site : www.caprioli-avocats.com.

[5] Cass. crim. 14 mars 2006, n° pourvoi : 05-83423, publié au bulletin, disponible sur le site www.legifrance.gouv.fr.

[6] Eric A. Caprioli, Commentaire de la décision, Les Echos du 2 novembre 2005.

[7] Art. 22-III de la loi Informatique, Fichiers et Libertés.

[8] Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004-801 du 6 août 2004, JO. 22 octobre 2005, p. 16769. V. Isabelle Cantéro, Décret du 20 octobre 2005 pris en application de la loi " Informatique et Libertés ", Com. Comm. Electr., février 2006, n° 6.

[9] Il est important de souligner que le décret du 20 octobre 2005 comporte un article 56 qui est spécifique aux organismes de presse écrite et audiovisuelle

[10] Eric A. Caprioli, Commentaire de l'arrêté du 31 mars 2005 modifiant le règlement du comité de la réglementation bancaire et financière n°97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement, Comm. Com. Electr., octobre 2005, n°167, p. 49 et s.

[11] V. Eric A. Caprioli, Isabelle Cantéro, Protection des données, Les nouveaux pouvoirs de contrôle de la CNIL dans les collectivités territoriales, voir : www.caprioli-avocats.com.

[12] Pierre Leclercq, Le contrat international sur les données personnelles, in Les deuxième journées internationales du droit du commerce électronique, sous la direction scientifique de Eric A. Caprioli, Litec, Act. Dr. de l'entrep., mars 2005, p. 243 et s.

[13] V. sur le site de la CNIL, disponible à l'adresse : www.cnil.fr.

[14] Le I. de cet article dispose : " Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès ".

[15] On peut penser qu'il s'agit du responsable des traitements qui désigne le CPDCP au vu de la rédaction de l'article 22-III de la loi Informatique et Libertés.