

Droit de l'immatériel

INFORMATIQUE | MÉDIAS | COMMUNICATION

Collection
LAMY
DROIT DE
L'IMMATÉRIEL

*Copyright et innovation technologique :
de Sony à Grokster, avancées et faux
pas de la Cour suprême*

Par Olivier HUGOT

*Contrat sur l'image et jeu de la garantie
d'éviction*

Par Zaïna AZZABI

*Le Real Madrid perd son match devant
les juridictions françaises*

Par Philippe BELLOIR

*Le public et la définition
de la communication audiovisuelle*

Par Marcel MORITZ

ENTRETIEN

*L'ordonnance du 6 juin 2005
relative aux données publiques*

Par Jean-Michel BRUGUIÈRE

DOSSIER SPÉCIAL

*La loi « Informatique et libertés »
et l'entreprise*

*Par Jean FRAYSSINET
Christophe PALLEZ
Gilles VERCKEN
Michel VIVANT*

Lamy

Par Gilles
VERCKEN

Avocat
au Barreau de Paris
Denton Wilde Sapte

Co-auteur du Lamy
droit de l'informatique
et des réseaux



et

Gwendoline
VAN OSSEL

Juriste

Céline
SERPAGLI

Juriste

Le « correspondant à la protection des données » : une création inachevée ?

Article 22 de la loi du 6 janvier 1978 relative aux fichiers, à l'informatique et aux libertés, modifiée par la loi du 6 août 2004

INTRODUCTION

La loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, a modifié la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Le correspondant à la protection des données à caractère personnel constitue, parmi les innovations de la loi du 6 août 2004, l'une des plus visibles et des plus souvent mises en avant.

Ce nouveau dispositif a suscité d'abondants commentaires malgré le laconisme de la loi. Dans l'attente du décret d'application, initialement prévu pour le mois de juin 2005, mais non encore paru à ce jour, il nous semble opportun de revenir sur les principales interrogations auxquelles devrait répondre ce dernier (*). Le dispositif mis en place par la loi française transpose celui créé par la directive 1995/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel et à la libre circulation de ces données. Le législateur communautaire s'est inspiré des expériences étrangères en la matière et en particulier du modèle allemand, pour permettre aux États de créer la fonction de correspondant à la protection des données à caractère personnel, appelé « détaché à la protection des données » dans la directive.

Il s'agit plus précisément de la transposition de l'article 18 de la directive n° 1995/46/CE qui dispose que les États membres peuvent prévoir une simplification ou une dérogation à l'obligation de notification à l'autorité de contrôle, lorsque le responsable désigne un « détaché à la protection des données à caractère personnel ». Le détaché est

« chargé notamment d'assurer, d'une manière indépendante, l'application interne des dispositions nationales prises en application de la présente directive, de tenir un registre des traitements effectués par le responsable du traitement (...), et garantissant de la sorte que les traitements ne sont susceptibles de porter atteinte aux droits et libertés des personnes concernées ».

La directive a été transposée et la fonction de détaché à la protection des données créée en Allemagne, aux Pays-Bas, au Luxembourg et en Suède.

En France, l'article 22 nouveau de loi du 6 janvier 1978 prévoit qu'une société ayant nommé en son sein un correspondant indépendant à la protection des données à caractère personnel sera dispensée des formalités de déclaration auprès de l'autorité de contrôle française, la Commission nationale de l'informatique et des libertés (CNIL).

Le Conseil constitutionnel a validé l'institution du correspondant à la protection des données à caractère personnel, en considérant que cette nouvelle fonction était entourée d'un « ensemble de précautions » concernant leur qualification, leur rôle et leur indépendance.

Le « correspondant à la protection des données à caractère personnel » (désigné par la CNIL par les lettres « CL » pour « Correspondant informatique et libertés ») est défini comme étant la personne « chargée d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente

loi » (art. 22, III, al. 1^{er}). Il doit être distingué du « responsable du traitement », qui est « la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens » (L. 6 janv. 1978, art. 3, 1).

Le correspondant doit agir de manière indépendante. À ce sujet, le Conseil constitutionnel a été saisi par des requérants qui ont notamment mis en cause cet aspect de l'article 22 nouveau, en soutenant que « ce correspondant ne bénéficie pas, à la lettre, des garanties d'indépendance indispensables » dès lors qu'« en prévoyant, au titre d'une simplification toujours souhaitable, un amoindrissement des mécanismes de contrôle, le législateur a privé de garantie légale le droit à la vie privée et à la liberté individuelle ». Le Conseil constitutionnel a cependant validé l'institution du correspondant à la protection des données à caractère personnel, en considérant que cette nouvelle fonction était entourée d'un « ensemble de précautions » concernant leur qualification, leur rôle et leur indépendance.

La dispense de formalités visée à l'article 22 nouveau se limite aux seuls traitements soumis à déclaration, c'est-à-dire aux traitements de données « peu sensibles ». Les traitements relevant des articles 25, 26, 27 (traitements soumis à autorisation préalable) ou du deuxième alinéa de l'article 36 (traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives) de la loi du 6 janvier 1978 ne peuvent profiter d'une dispense de formalités.

La dispense de formalités est, de plus, exclue dans l'hypothèse où un transfert de données à destination d'un État non membre de l'Union européenne est envisagé.

Il existe aujourd'hui en France des millions de traitements créés et utilisés par les entreprises, alors que seuls quelque 800 000 fichiers sont déclarés auprès de la CNIL.

(*) Note des auteurs : Les opinions et avis de la CNIL cités dans le présent article sont tirés des différents commentaires publiés sur son site : <www.cnil.fr>.

La méconnaissance de la loi par les entreprises explique probablement le défaut de déclaration des fichiers courants que traitent nécessairement les entreprises dans leur activité quotidienne, tels que les fichiers de paie, les fichiers inhérents à l'utilisation de standards téléphoniques, ceux relatifs à la cantine, au parking, aux clients et fournisseurs, aux prospects, etc.

Pour éviter de devoir déclarer le moindre de ces traitements de données à caractère personnel, l'entreprise peut donc, en application de l'article 22 nouveau de la loi du 6 janvier 1978, nommer une personne responsable du respect de la loi. Du point de vue de l'entreprise, l'avantage immédiat de la désignation d'un correspondant est la diminution des contraintes administratives (avantage qui ne sera toutefois pas ressenti par l'entreprise qui n'effectuait aucune déclaration auprès de la CNIL, alors même qu'elle était soumise à cette obligation). De plus, de l'avis de la CNIL, le correspondant informatique apporte à l'entreprise une aide précieuse : il a un rôle de conseil et de suivi dans la légalité de déploiement des projets informatiques et, plus largement, de la gestion des données à caractère personnel. Il propose à l'entreprise des solutions permettant de concilier protection des libertés individuelles et intérêt légitime.

Du point de vue de la CNIL, cette désignation aura également ses avantages. Le premier est qu'elle aura pour effet de renforcer la pédagogie en interne et la diffusion de la « culture liberté et informatique » – ce à quoi la CNIL tient tout particulièrement. Pour la CNIL, le correspondant « a vocation à être un interlocuteur spécialisé en matière de protection des données à caractère personnel, tant pour le responsable du traitement, que dans les rapports de ce dernier avec la CNIL. Il occupe ainsi une place centrale dans le développement maîtrisé des nouvelles technologies de l'information et de la communication ». D'après Alex Türk, président de la CNIL, il s'agit « d'opérer un diagnostic permanent quant au respect de la déontologie "informatique et libertés", ce qui devrait rassurer les dirigeants, et non pas être ressenti comme une charge » (Türk A., Loi du 6 août 2004. Présentation générale de la loi, Comm. com. électr., févr. 2005, p. 12). Le correspondant à la protection des données à caractère personnel sera ainsi un véritable relais de la CNIL, dans les entreprises et les collectivités locales.

Le deuxième avantage affiché par la réforme est la simplification des procédures et dès lors la suppression de la « paperasserie » pour la CNIL.

Enfin, la réforme devrait permettre la limitation des fichiers clandestins (dont le nombre est estimé à plusieurs millions) grâce à la tenue d'un registre par le correspondant. La CNIL espère ainsi voir réapparaître dans le registre, des fichiers qui n'auraient pas été déclarés autrement.

La mise en place de ce nouveau dispositif est une solution pragmatique : il est plus simple d'instaurer un système qui exonère des millions de fichiers non déclarés que de parvenir à ce que les entreprises procèdent aux déclarations. Ce système permet par conséquent à l'entreprise de légaliser sa situation.

La nouvelle fonction de correspondant à la protection des données à caractère

La nouvelle fonction de correspondant à la protection des données à caractère personnel suscite de nombreuses interrogations.

personnel suscite cependant de nombreuses interrogations. La présente étude – non exhaustive – a pour objet de soulever quelques-unes des principales difficultés que peut poser la mise en œuvre de cette nouvelle fonction.

Tout d'abord, lorsque l'entreprise souhaitera désigner un correspondant, se posera la question de la qualité et du statut que cette personne devra avoir (I). Ensuite, une fois le correspondant désigné, celui-ci sera confronté à plusieurs difficultés dans la détermination et l'exécution de ses missions (II).

I. – UN STATUT INDÉFINI

La loi du 6 janvier 1978 modifiée par celle du 6 août 2004 prévoit que le correspondant à la protection des données à caractère personnel est « une personne bénéficiant des qualifications requises pour exercer ses missions » (art. 22, III, al. 3). Elle n'explicite pas davantage la teneur de ces qualifications.

La CNIL a cependant précisé que le correspondant devra justifier de connaissances juridiques, de compétences en informatique, en conseil et en management, ainsi qu'en médiation et pédagogie (ce qui peut faire beaucoup !).

La loi dispose par ailleurs que la désignation du correspondant à la protection des données à caractère personnel incombe au responsable du traitement et

non à la CNIL (art. 22, III al. 1). Cette dernière se verra notifier la désignation du correspondant mais elle ne devra ni ne pourra en aucun cas l'agréer (art. 22, III, al. 2).

La désignation du correspondant devra également être portée à la connaissance des instances représentatives du personnel (art. 22, III, al. 2).

Ceci étant rappelé, on constate que plusieurs interrogations demeurent, auxquelles seule la pratique pourra répondre. On se demande d'abord s'il faudra exiger une formation initiale ou prescrire une formation continue et s'il faudra exiger en outre la connaissance des notions de sécurité informatique (aura-t-on besoin d'un organisme pour valider l'expertise du correspondant à la protection des données à caractère personnel et dispenser des formations ?).

La question majeure sera ensuite de déterminer quelle personne peut être désignée : personne morale ou personne physique ? Personne interne à l'entreprise (salarié, cadre...) ou personne extérieure ? Cette dernière question soulève particulièrement notre intérêt et nous souhaitons nous y attarder dans les lignes qui suivent.

Le législateur a volontairement refusé de faire obligatoirement du correspondant un salarié protégé, car dans ce cas, il aurait fallu rendre leur institution obligatoire pour éviter que des dirigeants refusent de s'en doter. Toutefois l'article 22, III, alinéa 3 de la loi du 6 janvier 1978 précise que le correspondant à la protection des données à caractère personnel « ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions ». Cette disposition laisse entendre que le correspondant devra ou pourra être un employé de la société. Cependant, ni la doctrine ni la CNIL n'exclut que le correspondant soit une personne extérieure à l'entreprise.

D'après la CNIL, le correspondant pourra donc être désigné au sein de l'entreprise ou à l'extérieur, dès lors qu'il justifie des garanties d'indépendance et de qualification. La CNIL conseille toutefois de privilégier un correspondant interne, notamment pour les grandes entreprises (le seuil restant à définir). Elle estime par ailleurs que le directeur de l'organisme ne pourra pas être désigné comme correspondant, pour éviter d'être juge et partie. Ce dernier devra cependant être, selon la CNIL, en rapport direct avec la direction.

Il est effectivement à craindre que la désignation d'un prestataire extérieur à la fonction de correspondant n'apporte pas de garanties suffisantes à son indépendance (I.1) et que, dès lors, la désigna-

tion d'une personne interne à l'entreprise à la fonction de correspondant à la protection des données à caractère personnel devrait être privilégiée (I.2).

I.1 L'absence de garantie d'indépendance d'un correspondant prestataire extérieur

La désignation d'un prestataire extérieur aux fonctions de correspondant peut ne pas répondre à l'exigence d'indépendance qui va de pair avec cette nouvelle fonction au sein de l'entreprise. La personne extérieure désignée comme correspondant ne dispose en effet que d'une indépendance juridique théorique, mais d'aucune indépendance économique pratique, la seconde risquant de l'emporter sur la première dans les faits.

En effet, on peut s'interroger légitimement sur la capacité du correspondant-prestataire extérieur à prévenir la CNIL soit d'une difficulté qu'il rencontrerait avec l'entreprise dans l'exercice de sa mission, soit du non respect de la loi par cette même entreprise. Dans ces deux hypothèses, la sanction que doit prendre la CNIL conformément à l'article 22 nouveau est d'obliger le responsable du traitement à effectuer les déclarations – pour lesquelles il avait obtenu une dérogation grâce à la désignation d'un correspondant. Ceci amène l'entreprise à mettre fin au contrat avec le prestataire extérieur, puisque l'intérêt du contrat avec celui-ci est justement de ne pas effectuer de déclaration. Le prestataire extérieur est ainsi chargé de saisir la CNIL, saisine qui entraînera vraisemblablement la fin de son contrat de prestation... Est-ce le meilleur moyen de le motiver ? (Le parallèle peut être fait avec la fonction de commissaire aux comptes, qui rencontrera le même dilemme : dénoncer son client au tribunal de commerce et risquer de le perdre. Ne pas le dénoncer, et ne pas exécuter la mission pour laquelle il a été engagé).

De plus, si l'entreprise choisit de confier la mission de correspondant à un prestataire extérieur, la question se pose de savoir qui elle pourra désigner.

Pourra-t-il s'agir d'un expert-comptable ou d'un commissaire aux comptes ? A priori la réponse nous semble négative, car ces personnes ne peuvent pas statutairement s'immiscer dans la gestion de l'entreprise.

Pourra-t-il s'agir d'un avocat ? L'avocat présente certes les garanties d'indépendance et de compétence, mais le secret professionnel semble incompatible avec le fait de dénoncer à la CNIL un client qui ne se conformerait pas à la loi. La réponse devrait donc également être négative.

Il semble alors préférable de privilégier la désignation d'une personne interne à l'entreprise.

I.2 La désignation d'un correspondant interne à l'entreprise

La désignation d'une personne interne à la fonction de correspondant à la protection des données à caractère personnel est incontestablement une des solutions les plus adéquates pour garantir

L'indépendance requise du correspondant interne à l'entreprise suppose que sa fonction au sein de l'entreprise n'entre pas en conflit avec sa mission de correspondant.

l'indépendance exigée par la loi (I.2.1). Toutefois, ce choix peut entraîner aussi des difficultés, qui devront être résolues par la pratique (I.2.2).

I.2.1 Désignation d'une personne interne à l'entreprise à la fonction de correspondant

Contrairement à ce que l'on pourrait penser de prime abord, l'indépendance du correspondant exigée par la loi du 6 janvier 1978 peut être garantie par la désignation d'une personne interne à l'entreprise, par le fait que l'article 22 de cette même loi dispose que l'employeur ne peut pas sanctionner le correspondant lorsque ce dernier accomplit sa mission. En outre, le législateur a donné au correspondant la faculté de saisir la CNIL des difficultés rencontrées.

La CNIL précise « *qu'au-delà de ces dispositions, c'est la position hiérarchique du correspondant, 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 correspondant et l'absence de conflit d'intérêt avec les fonctions exercées en même temps qui sont de nature à apporter les garanties de l'indépendance* ».

Elle ajoute que « *directement rattaché au responsable du traitement, [le correspondant] ne pourra être influencé dans les conseils, les recommandations ou alertes qu'il sera conduit à formuler lors de la mise en œuvre des traitements ou dans l'instruction des plaintes et requêtes adressées par les personnes concernées* ».

La personne interne à l'entreprise désignée à la fonction de correspondant peut toutefois rencontrer des difficultés.

I.2.2 Difficultés rencontrées par le correspondant interne à l'entreprise

Deux questions doivent être posées : comment la personne désignée en interne par l'entreprise en application de l'article 22 nouveau de la loi du 6 janvier 1978, va-t-elle parvenir à gérer sa fonction de salarié et sa mission de correspondant (a) ? Quelle est sa responsabilité en sa qualité de correspondant (b) ?

a) Difficile gestion des deux attributions

L'indépendance requise du correspondant interne à l'entreprise suppose que sa fonction au sein de l'entreprise n'entre pas en conflit avec sa mission de correspondant.

Dès lors, on peut légitimement se poser la question de savoir comment l'indépendance du correspondant peut se concilier avec le rapport de subordination du salarié.

Si cette mission de correspondant est indépendante des fonctions définies par le contrat de travail, le salarié sera-t-il rémunéré ? Si non, s'agit-il d'un louage de services sans contrepartie ?

Si l'entreprise désigne un salarié, faudra-t-il rédiger un avenant à son contrat de travail ?

Si le salarié s'occupe principalement de sa fonction initiale au sein de l'entreprise, comment peut-il gérer en même temps sa mission de correspondant ? S'il décide au contraire de se concentrer sur sa mission de correspondant, au détriment de sa fonction initiale, ne prend-il pas un risque ? Que se passe-t-il s'il remplit parfaitement sa mission de correspondant mais que des reproches lui sont adressés au sujet des prestations accomplies dans l'exercice de sa fonction initiale par son responsable ?

Pourrait-il trouver une solution en déterminant à l'avance le nombre d'heures qu'il doit consacrer à l'une et l'autre par semaine ? Mais qu'en est-il des imprévus ? Qui pourrait fixer les temps impartis ?

Toutes ces questions demeurent à ce jour non résolues. La pratique devra pourtant y répondre. Nous serions toutefois enclin à privilégier les réflexions sur le contrat de travail ou l'avenant au contrat de travail, qui doit être signé entre les parties.

La question de la responsabilité encourue par cette personne interne en sa qualité de correspondant n'est pas non plus résolue.

b) Responsabilités en cause

Les règles de responsabilité applicables au responsable du traitement peuvent-elles l'être dans certaines hypothèses au correspondant ?

L'article 22 nouveau de la loi est muet à ce sujet.

Il nous semble qu'il faut envisager un double régime de responsabilité.

D'une part, le correspondant encourt une responsabilité vis-à-vis de la CNIL, en cas de défaillance ou de manquement aux obligations qui lui incombent en cette qualité. Le correspondant ne peut en effet faire l'objet d'aucune sanction de la part de son employeur mais la CNIL pourra le décharger de ses fonctions. La question se pose toutefois de savoir sur quels critères le correspondant sera jugé avoir mal rempli ses fonctions de correspondant.

D'autre part, il faut se demander si le correspondant pourrait être responsable vis-à-vis des personnes concernées par le traitement.

On vise tout d'abord l'article 45 nouveau de la loi du 6 janvier 1978, applicable au responsable des traitements, ou les articles 226-16 à 226-24 nouveaux du Code pénal, qui prévoient de lourdes peines d'emprisonnement et d'amende en cas de méconnaissance des obligations imparties. La loi ne précise pas expressément leur application au correspondant. Si on imagine l'hypothèse où le correspondant découvre que l'entreprise ne respecte pas la loi du 6 janvier 1978, et qu'il n'en avise pas l'entreprise (de manière officielle) ni ne dénonce cette dernière à la CNIL, en opposition aux dispositions de l'article 22 nouveau, on peut s'interroger sur les conséquences de cette abstention. En effet, se poserait dans ce cas la question d'un éventuel « *transfert* » (ou cumul) de la responsabilité de l'entreprise vers le correspondant : le correspondant pourrait-il être tenu responsable vis-à-vis des personnes, des manquements de l'entreprise faute d'avoir dénoncé ceux-ci ? Il nous semble que l'élément intentionnel serait toutefois difficile à établir. On vise ensuite la responsabilité civile du correspondant vis-à-vis des personnes concernées par le traitement. La difficulté rencontrée ici se situe au niveau de l'appréciation de la faute et du lien de causalité pour établir cette responsabilité éventuelle. De plus, si une telle responsabilité peut être mise en cause, il faut également analyser la nécessité et l'utilité pour le correspondant de prendre une assurance RC.

On peut d'ores et déjà affirmer que la responsabilité du correspondant doit être en tout état de cause cantonnée aux trai-

tements pour lesquels il est nommé, au regard de la délimitation qui est faite de sa mission par l'article 22 nouveau de la loi du 6 janvier 1978, qui ne concerne que les traitements soumis à déclaration. En cas de rupture du contrat par la CNIL, la loi ne prévoit pas non plus d'indemnités à payer. Faut-il l'envisager ?

De nombreuses questions restent donc en suspens quant à la qualité, au statut et au régime de responsabilité applicable au correspondant. Reste à déterminer les missions qui lui sont attribuées.

II. – DES MISSIONS IMPRÉCISES

La loi ne dresse pas une liste exhaustive des différentes missions du correspondant à la protection des données à caractère personnel. Elle se contente de préciser qu'il est chargé d'assurer le respect des dispositions de la loi du 6 janvier 1978 modifiée par celle du 6 août 2004, obligation générale (II.1) et qu'à ce titre, il doit tenir un registre des traitements effectués par l'entreprise, immédiatement accessible à toute personne en faisant la demande, obligation spéciale (II.2).

II.1 Le respect des dispositions de la loi : quels contours ?

L'obligation générale d'assurer le respect des dispositions de la loi du 6 janvier 1978 (art. 22, III, al. 1^{er}) implique, aux termes de l'article 6 de la même loi, que les traitements créés par l'entreprise portent sur des données qui :

- doivent être collectées de manière loyale et licite ;
- pour des finalités déterminées, explicites et légitimes ;
- ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités ;
- doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;
- doivent être exactes, complètes et, si nécessaire, mises à jour ;
- doivent être conservées sous une forme permettant l'identification des per-

sonnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Le correspondant à la protection des données devra vérifier que l'entreprise a recueilli le consentement des personnes concernées (art. 7).

Pour s'assurer que ces obligations sont respectées, le correspondant à la protection des données à caractère personnel devra, lors de sa prise de fonction, réaliser un important travail d'audit sur les traitements de données existants (II.1.1). Il faut ensuite se demander quelle devra être l'attitude du correspondant face aux non-respects constatés lors de cet audit (II.1.2).

II.1.1 Correspondant auditeur

Dans le cadre de sa mission d'audit, le correspondant devra notamment identifier les finalités des traitements, vérifier et valider les conditions dans lesquelles ils ont été mis en œuvre. Il devra vérifier la loyauté de ces traitements, leur proportionnalité aux finalités, les durées de conservation des données. Il lui faudra également structurer tous les traitements de données et les bases de données et détecter les problèmes éventuels liés à la mise en œuvre des traitements. Des difficultés d'application de cet audit se font d'ores et déjà pressentir.

En effet, si le fichier n'a pas été constitué dans le respect des obligations de la loi, il sera plus difficile – voir impossible, sauf à le détruire – de le régulariser *a posteriori*. Tout dépendra en définitive de la manière dont les données ont été structurées.

On envisage par exemple l'hypothèse où le fichier tel que structuré et paramétré ne permet pas de savoir depuis combien de temps la donnée est conservée ; ni si la donnée a été recueillie directement auprès de la personne concernée ou auprès d'un tiers ; ni si la personne a été informée de la possibilité de communiquer à un tiers le fichier ; ni non plus s'il existe une preuve que la personne concernée a donné son consentement (le correspondant devrait prendre le cas échéant à nouveau contact avec les personnes concernées par les traitements, ce qui ne sera probablement pas toujours possible). Dès lors, on réalise que si le traitement des données n'a pas été documenté à l'origine sur la base de ces critères, le correspondant ne pourra apporter de réponses à ces questions.

Concrètement, le seul moyen d'avoir une vue exhaustive des traitements de données dans une entreprise, sera d'élaborer un questionnaire complet à adresser à tous les chefs de service, afin de re-

De nombreuses questions restent en suspens quant à la qualité, au statut et au régime de responsabilité applicable au correspondant.

censer les fichiers existants. Notre expérience des audits nous permet d'affirmer que le correspondant sera alors probablement surpris par la multiplicité des traitements, l'absence de respect de la loi et l'impossibilité de documenter utilement les fichiers *a posteriori*.

Que se passe-t-il si, au cours de cet audit, le correspondant est confronté à des traitements qui n'ont pas été créés en conformité avec les dispositions de la loi ?

II.1.2 Correspondant préconisateur, régulateur ou seulement dénonciateur ?

La question se pose de savoir jusqu'où s'étend la mission du correspondant de veiller au respect de la loi et comment doit réagir le correspondant face à un éventuel non-respect de celle-ci.

On imagine l'hypothèse où l'entreprise n'a pas respecté les dispositions de la loi dans l'établissement de ses traitements, ou celle où l'entreprise et le correspondant ont un avis divergent quant à l'appréciation, l'interprétation, le respect et l'application de la loi, ou encore celle où l'entreprise refuse de donner accès à toutes les données personnelles. Comment le correspondant doit-il réagir face à ces situations ?

On peut se demander s'il doit faire des préconisations à l'entreprise, qui impliqueront nécessairement des interprétations juridiques sur les traitements créés par elle ; s'il doit demander à l'entreprise la modification des fichiers existants et non-conformes ; s'il a l'obligation de veiller à ce que l'entreprise régularise les situations non conformes à la loi et si l'entreprise a l'obligation de respecter les préconisations et injonctions faites par le correspondant.

Et que faire si, quels que soient les efforts que l'entreprise est prête à fournir suite au constat du non-respect par le correspondant, il apparaît qu'un fichier ne peut pas être rendu conforme (par exemple parce qu'il y a impossibilité de prendre contact avec les personnes concernées par le fichier, pour s'assurer qu'elles ont donné leur consentement exprès et préalable dans les cas où la loi le réclame ? Ou encore parce que la durée de conservation a été dépassée ?). L'entreprise a-t-elle l'obligation de détruire le fichier et le correspondant doit-il y veiller ?

La loi nous dit qu'en cas de manquement à ses dispositions et d'absence de mise en conformité, le responsable du traitement est enjoint d'effectuer les formalités, c'est-à-dire les déclarations. Suffit-il alors à l'entreprise d'effectuer ces déclarations pour être exonérée de sa responsabilité ? Le texte le suggère, mais cela ne couvrira pas les irrégularités des

fichiers, non plus vis-à-vis de la CNIL, mais tout simplement vis-à-vis des personnes concernées, la CNIL n'étant au final que le gardien des intérêts de ces derniers.

On peut dès lors se demander si l'entreprise ne doit pas encourir des sanctions pénales. L'article 45 de la loi et les articles 226-16 à 226-24 du Code pénal pourraient être applicables à l'entreprise, lorsque celle-ci a désigné un correspondant. Si les articles du Code pénal sont applicables à cette hypothèse, il faudra encore se demander ce qu'il en est de l'élément intentionnel requis par ces articles : l'élément intentionnel risque de faire justement défaut, l'entreprise ayant désigné un correspondant et ayant par là démontré sa volonté d'appliquer et de respecter la loi.

En définitive, si la seule conséquence de la découverte par la CNIL de ces agissements, à la suite des révélations du correspondant, est pour l'entreprise de se

La question se pose de savoir jusqu'où s'étend la mission du correspondant de veiller au respect de la loi et comment doit réagir le correspondant face à un éventuel non-respect de celle-ci.

voir enjoindre de procéder aux formalités de déclaration, il suffirait également à l'entreprise de nommer un correspondant pour dissimuler des agissements. L'entreprise trouverait donc un avantage indirect dans l'exonération de sa qu'en entraîne la désignation d'un correspondant. Lorsque l'audit a été réalisé, le correspondant doit accomplir une nouvelle mission : inscrire l'ensemble des traitements de l'entreprise dans un registre créé à cet effet.

II.2 La tenue du registre des traitements : et la confidentialité ?

Après avoir audité les traitements créés par l'entreprise, le correspondant à la protection des données à caractère personnel doit « tenir une liste des traitements effectués, immédiatement accessible à toute personne en faisant la demande » (art. 22, III, al. 3).

L'obligation spéciale de tenir un registre des traitements effectués par l'entreprise (art. 22, III, al. 3) n'est pas explicitée par la loi française. En effet, celle-ci ne précise pas les informations que doit contenir le re-

gistre, contrairement à la directive qui vise expressément :

- le nom et l'adresse du responsable du traitement et, le cas échéant, son représentant ;
- la ou les finalités du traitement ;
- une description de la ou des catégories de personnes concernées et des données ou catégories de données s'y rapportant (on constate que seule la nature des données y est indiquée et non les données elles-mêmes) ;
- les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées.

La loi précise que le registre est public : toute personne peut y avoir accès et peut par conséquent, notamment, avoir connaissance de l'existence de fichiers normalement couverts par le secret des affaires. Le problème de la confidentialité se pose dès l'investigation sur les fichiers existants, et jusqu'à l'inscription de ceux-ci dans le registre. Les fichiers étant des éléments stratégiques de l'entreprise, beaucoup sont confidentiels, et non partagés entre les différents services de l'entreprise. Le correspondant dispose lui-même d'un fort pouvoir d'immixtion dans l'activité des services, mais il se trouvera confronté, lors de ses investigations tout d'abord, à la résistance (légitime ?) de certains services de lui dévoiler l'existence de fichiers créés par eux. Ensuite, une fois leur existence révélée au correspondant, celui-ci rencontrera leur opposition à ce que ces fichiers soient repris dans le registre et donc susceptibles d'être découverts par toute personne qui en ferait la demande.

Pour les fichiers n'impliquant que le personnel de l'entreprise, l'exigence légale a un sens et peut se comprendre. Mais que penser des autres fichiers ? Le service « *Prospectives* », ou « *Recherche et développements* », voudra-t-il nécessairement informer l'ensemble de l'entreprise sur les fichiers qu'ils détiennent ? Le service « *Marketing* » devra-t-il fournir la liste de ses contacts presse ? La direction « *Communication* » était-elle d'ailleurs au courant de l'existence du fichier contacts presse de la direction « *Marketing* » ? Et qu'en est-il des fichiers clients et des fichiers fournisseurs ? Chaque direction commerciale doit-elle savoir quels sont les fichiers constitués par les autres ? Il est évident qu'à travers le simple établissement du registre des traitements existants, il risque d'y avoir des révélations internes sur les pratiques de chaque service, sans que cela soit nécessairement approprié par rapport aux objectifs poursuivis par la loi. Il n'est pas de notre propos de nous prononcer sur la nécessité ou non de la transparence

dans l'entreprise d'un service à un autre. Mais il est aussi légitime, certainement pour les fichiers autres que ceux relatifs au personnel, de poser la question de la nécessité de communiquer tous les fichiers à l'ensemble du personnel par l'inscription de ceux-ci dans le registre.

Et que dire si ce registre doit être tenu par le tiers qu'est le correspondant-prestataire extérieur ? À quelle obligation de confidentialité est tenu ce tiers ? Il conviendra ici de décrire en détail, dans le contrat d'entreprise, les obligations de secret et de confidentialité qui s'imposeront à ce correspondant-prestataire extérieur.

La mission du correspondant n'est donc pas simple. Elle implique une grande transparence dans l'entreprise, ce qui n'est pas nécessairement de l'intérêt de celle-ci, et alors même que le secret peut être justifié par des motifs légitimes et ne pas porter atteinte aux droits des personnes protégées par la loi du 6 janvier 1978.

En conclusion, on soulignera le rôle intéressant et nouveau du correspondant à la protection des données à caractère personnel. On attend avec intérêt la mise en place de cette nouvelle fonction clé au sein de l'entreprise, afin de répondre aux incertitudes face auxquelles on se

trouve aujourd'hui. Il convient d'ores et déjà d'insister sur la nécessité d'un audit précis de la situation par l'entreprise elle-même, avant même le choix de faire appel ou non à un correspondant, et sur l'importance d'un cadre contractuel clair. En définitive, n'est-il pas à craindre que la désignation d'un correspondant ne suscite plus de problèmes qu'elle n'en résolve, notamment au regard de l'immixtion dans la marche de l'entreprise et des coûts supplémentaires ? L'entrepreneur pourra alors être tenté de reprendre à son compte l'adage populaire « *pour vivre heureux, vivons cachés* ». ♦