



International Chamber of Commerce

The world business organization

Department of Policy and Business Practices

Commission on E-Business, IT and Telecoms

**Groupe de Travail Vie Privée et Protection des
Données Personnelles**

Contribution informelle à destination de la CNIL sur les lignes éthiques

Introduction

ICC est l'organisation mondiale des entreprises. Elle est l'unique porte-parole représentatif du secteur privé à s'exprimer au nom des entreprises de tous les secteurs dans le monde entier.

ICC a pour objectif d'encourager la liberté des échanges et des investissements internationaux et de défendre l'économie de marché. Dirigeants et experts des entreprises membres d'ICC travaillent à formuler le point de vue des milieux d'affaires mondiaux, tant sur de grands problèmes touchant au commerce et à l'investissement que sur des sujets techniques et sectoriels essentiels, dans le domaine, entre autres, des services financiers, des technologies de l'information, des télécommunications, de l'éthique du marketing, de l'environnement, des transports, du droit de la concurrence et de la propriété intellectuelle.

Au sein de la CCI, un groupe de travail Vie Privée et Protection des Données Personnelles analyse l'impact du contexte réglementaire dans le domaine de la vie privée et de la protection des données personnelles et exprime la position des entreprises sur ce sujet.

La CCI apprécie l'opportunité de répondre au projet de lignes directrices de la Commission Nationale de l'Informatique et des Libertés (CNIL) pour la mise en oeuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004 relative à l'informatique, aux fichiers et aux libertés.

Cependant, en raison de la brièveté des délais qui ont été accordés à la CCI pour revenir vers la CNIL, cette contribution informelle sera finalisée ultérieurement par une position officielle sur les lignes éthiques, après consultation de l'ensemble des membres de la CCI.

International Chamber of Commerce

38, Cours Albert 1er, 75008 – Paris, France
Telephone +33 1 49 53 28 28 Fax +33 1 49 53 28 59
Web site www.iccwbo.org E-mail icc@iccwbo.org

31 October 2005 MvdL/dfc



A titre liminaire, il serait utile de clarifier la portée géographique de ces lignes directrices, en particulier pour éviter les risques de conflits de lois qui pourraient résulter de différentes approches nationales sur ce sujet.

1. Portée du dispositif d'alerte : un caractère subsidiaire, un champ restreint, un usage facultatif

Les premier et second paragraphes semblent impliquer qu'un employé ne peut utiliser un dispositif d'alerte qu'en option de second ordre, éventuellement après avoir épuisé tout autre moyen d'alerte disponible (tel qu'une information de sa hiérarchie). Les entreprises sont d'avis que différents moyens d'alerte devraient être mis à la disposition des employés sans distinction de degré, afin qu'ils puissent choisir l'option avec laquelle ils sont le plus à l'aise, selon les circonstances. En effet, les employés peuvent craindre des représailles en contactant leur hiérarchie. Même dans les hypothèses où ce n'est pas le cas, les responsables hiérarchiques directs ne sont pas toujours les personnes les plus disponibles pour assister l'employé sur une problématique, ni les plus qualifiées car ils risquent de ne pas toujours avoir la meilleure connaissance des questions juridiques concernées ou de ne pas les traiter avec les précautions nécessaires (risque de divulgations inappropriées). Les personnes en charge de la mise en œuvre de systèmes d'alerte étant en nombre plus limité que les responsables hiérarchiques, il est possible de leur imposer de suivre des instructions pour garantir un traitement approprié de la problématique. C'est pourquoi nous pensons qu'il y a de grands avantages à mettre à la disposition des employés, en parallèle, tous les moyens d'alerte sans privilégier l'un plutôt que l'autre.

Le champ d'application des lignes directrices (cad les systèmes d'alerte) mériterait d'être clarifié. En effet, il serait utile pour les entreprises de comprendre si les conditions qu'elles imposent s'appliquent uniquement aux systèmes d'alerte employant des lignes dédiées de téléphone, télécopie ou courrier électronique ou si elles s'appliquent (en tout ou en partie) aux mécanismes de « compliance » habituellement mis en œuvre dans les grandes entreprises où les employés ont la possibilité (ou sont tenus) de faire part des manquements auprès d'organisations du groupe autres que leur responsable hiérarchique (responsables « éthique », départements juridiques, médiateurs, responsables ressources humaines ...). Les entreprises souhaitent en effet comprendre si les lignes directrices les restreignent d'une façon ou d'une autre dans l'organisation de leurs propres « voies hiérarchiques ».

Par ailleurs les entreprises ne comprennent pas pourquoi le champ des systèmes d'alerte devrait être restreint aux seuls domaines financiers et comptables. En effet, les entreprises ont besoin de mécanismes de « compliance » pour assurer le respect des règles, qu'elles aient trait au domaine financier ou à d'autres domaines juridiques tels que le droit de l'environnement, le travail des enfants, le harcèlement, la protection des données personnelles, les règles d'hygiène et de sécurité, les restrictions aux exportations, etc. Les employés travaillent dans un environnement juridique complexe. C'est pourquoi les entreprises s'efforcent de rendre cet environnement accessible en le synthétisant dans des règles internes (codes éthiques). Elles ont par conséquent besoin



de mettre en œuvre des systèmes d'alerte qui recouvrent tout manquement à des règles internes conformes à l'environnement juridique dans lequel les employés travaillent.

Nous nous permettons d'attirer votre attention sur le fait qu'il est contradictoire d'indiquer que Sarbanes Oxley (SOX) ne peut pas justifier en soi une système d'alerte (Section 1, 4ème par.) tout en autorisant ces système pour des questions entrant dans le champ de cette loi. En outre, il convient de souligner que SOX va au-delà des questions financières et comptables et qu'elle impose aux entreprises de traiter tout type de risque pouvant avoir un impact financier (Section 806).

Nous pensons que les principes de protection des données personnelles sont les mêmes quelque soit l'objet de l'alerte et que, par conséquent, les systèmes d'alerte devraient être autorisés avec un champ d'application plus large, dès lors qu'ils respectent les principes de protection des données personnelles. En outre, il paraît difficile de limiter des systèmes d'alerte aux questions financières et comptables, ces notions étant larges et pouvant concerner toute sorte de situations, seulement la falsification de comptes mais aussi la corruption, la fraude sur les dépenses professionnelles ...

Par ailleurs, l'avant dernier paragraphe indique que les entreprises devraient s'interdire d'exploiter des alertes remontées par le système d'alerte qui sont hors du champ du système. Cette interdiction peut mettre les sociétés en situation de risque car une inaction pourrait leur être reprochée ultérieurement, par exemple pour ne pas avoir assisté un employé en situation difficile. De même, il ne serait pas raisonnable d'exiger d'une entreprise de ne pas donner suite à une réclamation liée à une question non comptable ou financière mais qui pourrait causer un préjudice important à l'entreprise, à un employé ou à un tiers (par ex : un problème de sécurité).

La CCI souhaite rappeler qu'il est de la responsabilité de chaque employé, à son niveau, de respecter les lois, dès lors qu'elles leur ont été expliquées clairement par leur employeur. Les entreprises, de nos jours, sont exposées à des risques importants (faillite, atteinte à la réputation ...) du fait de manquements de certains de leurs employés et leurs conséquences peuvent affecter non seulement l'entreprise même mais aussi ses fournisseurs et la société dans son ensemble. De tels risques ne peuvent pas être toujours évités par de simples audits et contrôles ponctuels. Il paraît donc plus proportionné d'impliquer les employés dans le respect des règles au quotidien (dès lors que cela est fait de façon raisonnable et proportionnée) plutôt que de créer des contrôles plus pesants sur leurs activités journalières.

2. Des catégories limitativement définies de personnes concernées par le dispositif d'alerte

De telles limitations ne paraissent pas appropriées. Des employés qui n'ont pas de responsabilité directe dans la comptabilité et les finances de l'entreprise peuvent néanmoins être impliqués dans des manquements comptables et financiers. Par exemple, une fraude sur des feuilles de paie peut être effectuée par un employé falsifiant



les données du système de paie, alors qu'il ne fait pas partie des départements Finance et Comptabilité de l'entreprise.

De même, toute catégorie d'employé peut se trouver dans une situation où il aura besoin d'utiliser le système d'alerte. Par exemple, un ouvrier qui est témoin du fait que le chef d'usine ou un de ses collègues subtilise régulièrement des équipements fabriqués par l'entreprise pour les revendre au marché noir doit avoir les moyens d'alerter de cette situation.

En outre, les employés, sans distinction, peuvent être témoins de manquements de tous types autres que des manquements financiers et comptables (hygiène et sécurité, travail des enfants, harcèlement ...) et devraient bénéficier de moyens pour faire part de leurs inquiétudes.

3. Un traitement restrictif des dénonciations anonymes

Nous comprenons que ce paragraphe n'interdit pas aux entreprises de faire suite à une alerte anonyme dès lors que les entreprises ne les encouragent pas. La dernière phrase mériterait d'être clarifiée cependant: "Cela implique de ne pas faciliter la dénonciation anonyme, et notamment de ne pas ouvrir une ligne téléphonique qui ne prévoirait pas l'identification de l'émetteur de l'alerte au début de l'entretien ». Cela implique, d'après ce que nous comprenons, que dans le cadre d'une alerte par téléphone il faut demander le nom de l'appelant, mais qu'en cas de refus la personne en charge de l'alerte peut néanmoins poursuivre l'entretien si cela lui paraît approprié. Si tel est le cas, nous proposons la rédaction suivante: "Cela implique de ne pas faciliter la dénonciation anonyme, et notamment de demander l'identification de l'émetteur de l'alerte au début de l'entretien. Toutefois, si celui-ci refuse de s'identifier, l'entreprise peut décider de poursuivre l'entretien ».

4. La diffusion d'une information claire et complète sur le dispositif d'alerte

La dernière phrase impose aux entreprises d'indiquer clairement que l'utilisation abusive du dispositif expose son auteur à des sanctions disciplinaires et à des poursuites judiciaires.

Cette approche semble sévère à l'égard des employés, en particulier dans la mesure où en définitive c'est à l'entreprise qu'il appartient d'apprécier le bien fondé d'une alerte et de décider des suites à lui donner. Par ailleurs la notion d'"abus" est délicate à définir; or les entreprises, pour pouvoir prendre des sanctions disciplinaires doivent définir cette notion dans leur règlement intérieur. Néanmoins, comme le code pénal français réprime les dénonciations calomnieuses, les entreprises pourraient rappeler à leurs employés que ce type de dénonciation peut les exposer à des poursuites pénales. Ceci devrait dissuader les abus du système.



6 Des données d'alerte pertinentes, adéquates et non excessives

Le terme “objectives” devrait être supprimé. En effet, toute alerte comporte nécessairement un jugement personnel. Dans certains cas, les alertes sont reproduites telles que reçues, sans modification aucune. Toutefois, les commentaires faits par l'organisation en charge de l'alerte pourraient être rédigés de façon à indiquer qu'il s'agit d'allégations en cours de vérification, comme le suggère la seconde phrase de la Section 6.

7 Une gestion interne des alertes réservée à des spécialistes, dans un cadre confidentiel

L'exigence du traitement des alertes par une organisation spécifique ne soulève pas de question. Nous souhaiterions que le terme “organisation” soit utilisé par préférence à celui d' « entité » et le terme “spécifique” par préférence à celui de “dédiée”, qui pourraient autrement être interprétés comme se référant à une entité juridique ou à un département unique au sein d'une entité juridique unique. En effet, dans certaines entreprises il peut y avoir des fonctions dédiées au traitement des alertes mais dans d'autres, les alertes peuvent être traitées par un groupe spécifique de personnes (directeurs juridiques, responsables “compliance”, etc.) qui appartiennent à différents départements internes et qui ont d'autres fonctions que la seule gestion des alertes.

Le second paragraphe exige la confidentialité, ce qui est bien entendu une protection essentielle. Cependant, ce doit être une confidentialité à portée restreinte qui ne doit pas interdire à l'organisation d'informer les dirigeants de l'entreprise ou les autorités judiciaires ou de police en temps requis.

Nous comprenons et approuvons que le partage des données doive être strictement limité à ce qui est nécessaire pour le traitement de l'alerte. Nous craignons cependant que les deuxième et troisièmes paragraphes puissent être interprétés dans un sens qui ne tiendrait pas compte des modes de fonctionnement habituels des groupes d'entreprises, en limitant le partage des données entre entités juridiques du groupe à des cas exceptionnels (soupçon portant sur un haut dirigeant). Dans certains groupes internationaux, les organisations en charge du traitement des alertes peuvent ne pas comprendre uniquement des individus travaillant pour la seule filiale française. Par exemple, il n'est pas inhabituel pour des groupes dont le siège européen est hors de France d'avoir une organisation “compliance” située dans le pays européen où se trouve ce siège. En outre, les groupes créent des réseaux d'individus en charge de répondre aux questions et de traiter les alertes dans différents pays. Il ne serait pas dans l'intérêt des employés de leur imposer de contacter uniquement le représentant français d'un tel réseau. Les employés doivent pouvoir contacter quiconque au sein du réseau restreint (pour des raisons de langue, mais aussi parce qu'ils peuvent vouloir que leur question soit traitée par quelqu'un qui n'a pas potentiellement de relations personnelles avec la personne incriminée). Par conséquent, dans ces contextes, il peut y avoir partage de données entre des membres de l'organisation spécifique qui sont employés par



différentes entités juridiques du groupe. Cependant, comme ils appartiennent à l'organisation spécifiquement constituée, la protection adéquate sera assurée.

Aussi, par exemple dans le cadre de SOX, les alertes doivent être centralisées au sein d'une organisation de la société cotée aux Etats Unis. Cette société peut être la société mère d'une filiale française. Par conséquent, dans ce cadre, le partage des données avec la société mère est nécessaire.

En ce qui concerne le dernier paragraphe relatif au recours à un prestataire extérieur, il est clair que le prestataire doit respecter les règles de protection des données personnelles et être tenu contractuellement de le faire. Cependant, s'agissant de l'obligation d'« informer les personnes identifiées dans le dispositif de traitement des alertes », nous pensons qu'il conviendrait d'ajouter « à moins que l'entreprise ne décide de conserver cette obligation à sa charge ». En effet, dans certains cas il peut être préférable que l'information de la personne intéressée soit effectuée par son employeur plutôt que par un prestataire.

8 La diffusion de rapports d'activité anonymes

Dès lors que les statistiques sont anonymes, nous ne voyons pas ce qui peut justifier que leur distribution soit restreinte aux organisations en charge des alertes. En effet, si les individus ne peuvent être identifiés, il n'y a pas de risque de préjudice à leur rencontre et l'entreprise peut avoir intérêt à communiquer à ses employés les statistiques de « compliance ». Des exemples anonymes peuvent être utilisés pour illustrer des exemples de conduite inappropriée et pour éviter de nouveaux cas. Les données qui ne concernent pas des personnes identifiables sont en effet hors du champ de la protection des données personnelles.

9 Une conservation limitée des données

Les durées de conservation indiquées dans cette section ne sont pas suffisamment flexibles et exposent les entreprises au risque de ne pas respecter des durées de conservation légales. Les lignes directrices devraient reconnaître que le respect d'obligations légales est une raison légitime pour conserver les alertes au delà des durées indiquées.

En outre, il est important pour une entreprise, même en cas d'alerte infondée, de conserver les informations afin de pouvoir faire la preuve ultérieurement des démarches entreprises pour traiter et conclure la question. L'employé incriminé, ou celui à l'origine de l'alerte, peut par exemple décider de poursuivre l'entreprise, qui doit pouvoir démontrer les actions qu'elle a menées. Bien entendu, les informations ne doivent pas être disponibles de façon active sur les systèmes, mais elles pourraient être archivées de façon sécurisée et leur retrait pourrait n'être effectué que par des personnes spécifiquement identifiées dans des cas très restreints.



Par ailleurs, l'entreprise doit pouvoir conserver des données anonymes.

10 Une information précise de la personne mise en cause

Il faudrait indiquer clairement que les entreprises, dans des cas exceptionnels, peuvent à des fins d'enquête reporter l'information due à la personne incriminée, dès lors qu'elles justifient d'un intérêt légitime prépondérant.

* * * * *