LES ALERTES PROFESSIONNELLES

Par Christophe Pichard,
Avocat

Lignes directrices pour la mise en place d'un tel dispositif

Un dispositif d'alerte professionnelle a pour objet de permettre aux employés d'une entreprise de signaler des faits et comportements illicites ou susceptibles de nuire à la société et d'engager sa responsabilité, voire de les inciter à dénoncer de tels faits. Ce dispositif d'alerte professionnelle spécifique n'a pas vocation à se substituer aux autres mécanismes qui pourraient exister au sein de l'entreprise ou en vertu d'une disposition légale ou réglementaire.

Autorisation Unique

Considérant que la mise en place de tels dispositifs conduisait nécessairement à des traitements automatisés portant sur des données à caractère personnel (à savoir collecte, enregistrement, utilisation et conservation de ces données), la CNIL s'est tout naturellement saisie de la légalité de tels dispositifs. A ce titre, une délibération du 8 décembre 2005 a été publiée portant « Autorisation Unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle ». Cette décision est d'une importance capitale pour les entreprises : dès lors qu'elles respectent les conditions fixées dans cette décision pour la mise en place de tels systèmes, il leur suffit de déclarer qu'elles s'y conforment pour valider leurs dispositifs. En revanche, si l'entreprise ne se conforme pas au contenu de cette décision, il faudra alors déposer un dossier de **déclaration préalable** de son dispositif qui fera l'objet d'une étude spécifique de la CNIL. Dans ces conditions, nous rappelons ci-après les principales dispositions à respecter pour bénéficier de cette Autorisation Unique.

I – La finalité du traitement

Sont concernés par cette Autorisation Unique les traitements résultant d'une obligation législative ou réglementaire de droit français. Toutefois, la CNIL a admis que les traitements mis en œuvre dans les domaines comptable et d'audit par les entreprises concernées par la loi Sarbanes-Oxley de juillet 2002 pouvaient rentrer dans le champ d'application de cette autorisation.

II – Les domaines d'application du dispositif d'alerte

La CNIL distingue trois catégories d'alerte :
- La première catégorie concerne les risques sérieux pour l'entreprise dans les domaines comptable, d'audit financier, bancaire ou de lutte contre la corruption.
- La deuxième catégorie comprend les faits qui ne relèvent pas des « risques sérieux » mais qui doivent être considérés comme des faits particulièrement graves, c'est à dire mettant en jeu l'intérêt vital de l'entreprise ou l'intégrité physique ou morale de ses employés.
On peut regretter la formulation retenue pour distinguer ces deux premières catégories dans la mesure où des faits « mettant en jeu l'intérêt vital » ou « l'intégrité physique » semblent également sérieux. Il aurait sans doute été plus opportun que la première catégorie, pleinement concernée par l'Autorisation Unique, s'intitule « risques comptables et financiers » à distinguer d'une deuxième catégorie « risque graves autres que comptables et financiers ».
- La troisième catégorie est constituée de tous les autres actes et faits au sein de l'entreprise qui ne rentrent pas dans la définition des deux autres catégories.

Seuls les risques sérieux, relevant donc de la première catégorie, rentrent pleinement dans le champ d'application de l'Autorisation Unique. Ils peuvent donc être recueillis, enregistrés et traités par l'organisme chargé de la gestion des alertes.

Les faits et comportements relevant de la deuxième catégorie, même s'ils ne relèvent pas du champ d'application de l'Autorisation Unique, pourront néanmoins être recueillis par l'organisme chargé du traitement des alertes, compte tenu de leur gravité. Toutefois, de telles alertes doivent alors être simplement réorientées par cet organisme vers les personnes compétentes au sein de l'entreprise, sans que cet organisme ne puisse conserver de traces de cette alerte : l'alerte est alors soit détruite, soit archivée sans délai. Précisons dès maintenant que l'archivage au sens de l'Autorisation Unique doit être mis en place selon des modalités particulières.

Pour les autres faits qui ne constituent ni des risques sérieux ni des faits graves, l'organisme chargé du traitement ne peut recueillir l'alerte : il doit purement et simplement la détruire ou l'archiver sans la transmettre au service compétent pour un tel fait et informer l'émetteur en conséquence.

III - Destinataires et transferts des données

Sachant que les alertes professionnelles comprennent nécessairement des données à caractère personnel, il convient donc de s'attacher à la qualité du destinataire de ces informations. Plusieurs possibilités sont a priori envisageables : il peut s'agir soit d'une organisation au sein même de l'entreprise concernée, soit d'une autre société du groupe auquel appartient l'entreprise concernée, ou encore d'un prestataire extérieur. Outre le fait que l'organisme chargé du transfert, qu'il soit interne ou externe, doit nécessairement se conformer

aux règles applicables au traitement des données recueillies, la CNIL conditionne la validité du dispositif au respect des règles applicables aux transferts de données, notamment lorsqu'il s'agit de transferts transfrontaliers.

La transmission des données à un organisme appartenant à l'entreprise concernée ne pose pas de difficulté particulière, à partir du moment où cet organisme est destinataire de données uniquement nécessaires à l'accomplissement de la mission d'alerte. En revanche, la question peut s'avérer plus délicate si l'alerte est transmise à une autre société du groupe ou à un prestataire extérieur.

A - Prestataire extérieur

Même si elle n'y est pas favorable, la CNIL n'est pas opposée à la transmission de ces données à un prestataire extérieur dès lors que :

- l'organisme extérieur prend un certain nombre d'engagements ;
- la communication s'opère conformément aux dispositions de la loi du 6 janvier 1978 modifiée relative aux transferts internationaux de données.

En particulier, la CNIL entend que les pays où les destinataires de l'alerte sont situés assurent un niveau de protection suffisante de ces données au sens de la loi française.

Plus précisément, conformément à la délibération du 8 décembre 2005 précitée, le prestataire de services doit s'engager, notamment dans le cadre du contrat qui le lie à la société concernée, à ne pas utiliser les données à des fins détournées, à assurer leur confidentialité, à respecter la durée de conservation limitée de ces données et à procéder à la destruction ou à la restitution de tous les supports au terme de sa prestation. Ce prestataire doit également veiller à ce que les personnes chargées du traitement de l'alerte n'accèdent qu'aux données nécessaires dans la limite de leurs attributions respectives.

Dans tous les cas, la CNIL exige que les personnes ayant accès à ces données soient en nombre limité et aient été spécialement formées.

Lorsque les données sont transmises dans un autre pays, il convient de distinguer les pays appartenant à l'Union Européenne des autres. Les pays appartenant à l'Union Européenne sont supposés accorder une protection suffisante au sens de la loi du 6 janvier 1978, et le transfert de données à un prestataire établi dans ces pays ne pose pas de difficulté. En revanche, tel n'est pas le cas lorsqu'il s'agit d'un pays non membre de l'Union Européenne. Dans cette hypothèse, il faut alors s'interroger sur les dispositions prises par chacun des pays concernés en terme de protection des données. Soulignons le cas particulier des Etats-Unis : les entreprises américaines qui adhèrent au« Safe Harbor » (« Sphère de Sécurité » qui impose des principes de protection des données à respecter) sont considérées comme assurant un niveau de protection adéquate ; le transfert de données vers de telles entreprises ne nécessite alors pas de formalités spécifiques. La CNIL considère également que le niveau de protection est suffisant lorsque le prestataire, destinataire des données, a conclu un contrat de transfert basé sur les clauses contractuelles type émises par la Commission Européenne.

B - Société du groupe

La CNIL s'est également interrogée sur la possibilité de communiquer les données à une autre société du groupe auquel appartient l'entreprise concernée par l'alerte. Dans ce cas, la CNIL est assez ouverte à retenir une telle possibilité, à condition qu'elle soit justifiée par un intérêt légitime comme par exemple l'organisation du groupe et/ou la nature et la gravité des faits rapportés. Toutefois, la CNIL insiste à nouveau sur le respect des règles en matière de transfert des données transfrontalières. Ainsi le pays dans lequel est située l'autre société du groupe doit assurer un niveau de protection suffisant des données collectées, au sens de la loi française. A cet égard, les règles exposées ci-dessus en cas de transmission de données à un prestataire extérieur situé à l'étranger s'applique de la même façon.

IV - Traitement des alertes

En fonction de la qualification de l'alerte qui sera recueillie, le traitement apporté diffèrera. En d'autres termes, l'organisme chargé du traitement des alertes devra classer l'alerte reçue selon qu'elle relève de l'une des trois catégories décrites ci-dessus, à savoir risques sérieux, comportements graves ou faits sans gravité au sens de l'Autorisation Unique.

Lorsque l'alerte recueillie relève d'un risque sérieux - et qu'elle rentre donc pleinement dans le cadre du dispositif -, la CNIL considère que la personne visée par cette alerte doit tout d'abord être informée par le responsable du dispositif dès l'enregistrement, informatisé ou non, des données la concernant afin de lui permettre d'exercer ses droits d'accès et de rectification et d'opposition à ce traitement. Toutefois, la CNIL admet, lorsque des mesures conservatoires sont nécessaires, que l'information de la personne visée puisse être reportée jusqu'à ce que ces mesures aient été prises, à condition bien sûr que cette information ne soit pas retardée abusivement. En parallèle de cette information, l'organisme chargé du traitement y donne la suite appropriée et diligente les enquêtes qui lui paraissent nécessaires. L'organisme dispose alors d'un délai de deux mois pour communiquer ses conclusions.

Comme cela a été évoqué ci-dessus, une alerte qui ne rentre pas dans le champ d'application des risques sérieux mais qui revêt une certaine gravité doit être transmise au service compétent pour être soit détruite, soit archivée sans délai. L'organisme ne doit donc pas y donner suite.

Dans les autres cas, à savoir faits sans gravité, l'organisme informe l'émetteur de l'alerte qu'il n'est pas compétent pour y donner suite. Il réoriente alors l'émetteur vers le service compétent, les données recueillies à cette occasion étant alors soit détruites, soit archivées sans délai comme dans le cas des faits graves.

La seule différence entre ces deux dernières catégories résulte en fait de la réorientation qui, pour les faits graves, relève de l'organisme saisi alors que, pour les faits sans gravité, il appartiendra à l'émetteur de l'alerte de saisir directement le service compétent.

V - Alerte anonyme

La CNIL et plus généralement les européens ne sont pas favorables à des alertes anonymes. La CNIL considère en effet que l'anonymat n'est pas une bonne approche et génère de nombreuses dérives possibles. La CNIL d'ailleurs a pris soin d'apporter de nombreux arguments pour justifier sa position. On pourra retenir notamment les éléments suivants : l'anonymat n'est pas forcément une protection, puisque la personne visée pourra sans doute reconnaître l'émetteur de l'alerte ; une telle pratique risque de créer un climat social délétère ; et enfin si l'auteur de l'alerte anonyme se sent réellement menacé, il sera plus facile d'assurer sa protection s'il est connu...

Toutefois, le recours à ce procédé n'est pas exclu par la CNIL dans le cadre d'un dispositif d'alerte professionnelle dès lors que certaines conditions sont remplies. Ainsi, tout d'abord, le dispositif doit être conçu de manière à ne pas encourager un tel anonymat. Ensuite, le traitement d'une telle alerte doit s'entourer de précautions particulières, par exemple :

- lors de toute transmission d'informations relatives à cette alerte, le caractère anonyme devra apparaître très clairement ;
- le traitement de la plainte devra toujours s'attacher à se concentrer sur les faits plutôt que sur la personne mise en cause ;
- une analyse de l'opportunité de diffuser l'alerte doit également être effectuée.

VI - Durée de conservation des données

Si l'alerte ne rentre pas dans le champ d'application du dispositif (faits graves ou mineurs), la destruction ou l'archivage des données s'y rapportant doivent être réalisés sans délai.
Si l'alerte rentre dans le champ d'application du dispositif (risques sérieux), l'organisme chargé du traitement des données dispose d'un délai de deux mois pour communiquer ses conclusions. A l'issue de cette période de deux mois, en fonction de la suite qui sera donnée, les données personnelles seront conservées jusqu'au terme de la procédure qui sera éventuellement engagée ou, à l'inverse, elles seront détruites ou archivées sans délai.

Précisons que d'une façon générale, au sens de l'Autorisation Unique, en cas d'archivage, les données peuvent être conservées pendant une durée maximale de trente ans, sachant que seul un accès restreint doit être permis dans le cadre de cet archivage.

VII - Information des utilisateurs / Représentant du personnel

La CNIL insiste plus particulièrement sur le fait qu'une information claire et complète doit être donnée aux utilisateurs potentiels du dispositif d'alerte.

En outre, comme tout dispositif visant à mettre en place des moyens de contrôle au sein de l'entreprise, l'employeur doit respecter la procédure prévue par le Code du travail en la matière, en particulier les représentants du personnel, devront être consultés préalablement à la mise en place de ce système.

VIII – Droit d'accès et de rectification

La CNIL insiste particulièrement sur les droits d'accès, de rectification et d'opposition des personnes concernées par ces dispositifs d'alerte, ces droits étant essentiels au regard de la loi du 6 janvier 1978 modifiée. Le responsable du dispositif d'alerte, conformément à l'article 10 de la délibération du 8 décembre 2005, devra donc garantir ce droit d'accès aux données aux personnes concernées ainsi que la possibilité de rectifier les données si elles sont inexactes, incomplètes, équivoques ou périmées, voire même d'en demander la suppression. Toutefois, la CNIL considère que ce droit d'accès ne peut pas porter sur les documents préparatoires à une décision, par exemple une décision de poursuivre ou non la personne mise en cause. En revanche, ces documents deviendront accessibles une fois la décision prise. Par ailleurs, la CNIL admet, comme pour l'information de la personne mise en cause lors du traitement d'une alerte, que le droit d'accès puisse être différé de façon à ne pas porter atteinte à une enquête en cours.

En tout état de cause, la personne concernée par l'alerte ne peut en aucun cas obtenir le nom de l'émetteur de l'alerte, même dans le cadre de l'exercice de son droit d'accès ; cette restriction semble effectivement nécessaire pour s'assurer d'une certaine efficacité du dispositif.

Christophe Pichard,
Avocat,
Ancien Elève de l'Ecole Polytechnique,
Ancien Elève de l'ENSAE,
Pichard & Associés