AJ Pénal - mensuel - juin 2010 - pages 257 à 304 - n° 6

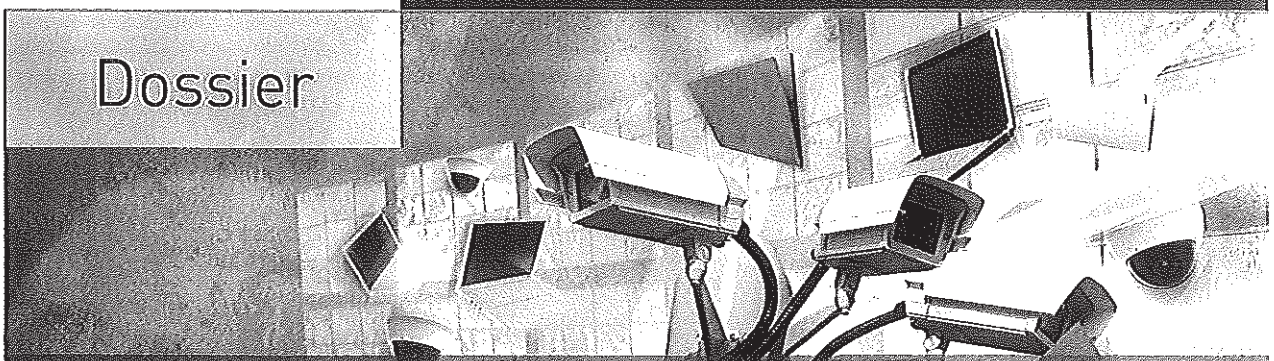
ref : 671006

9 782996 710064

AJ Pénal

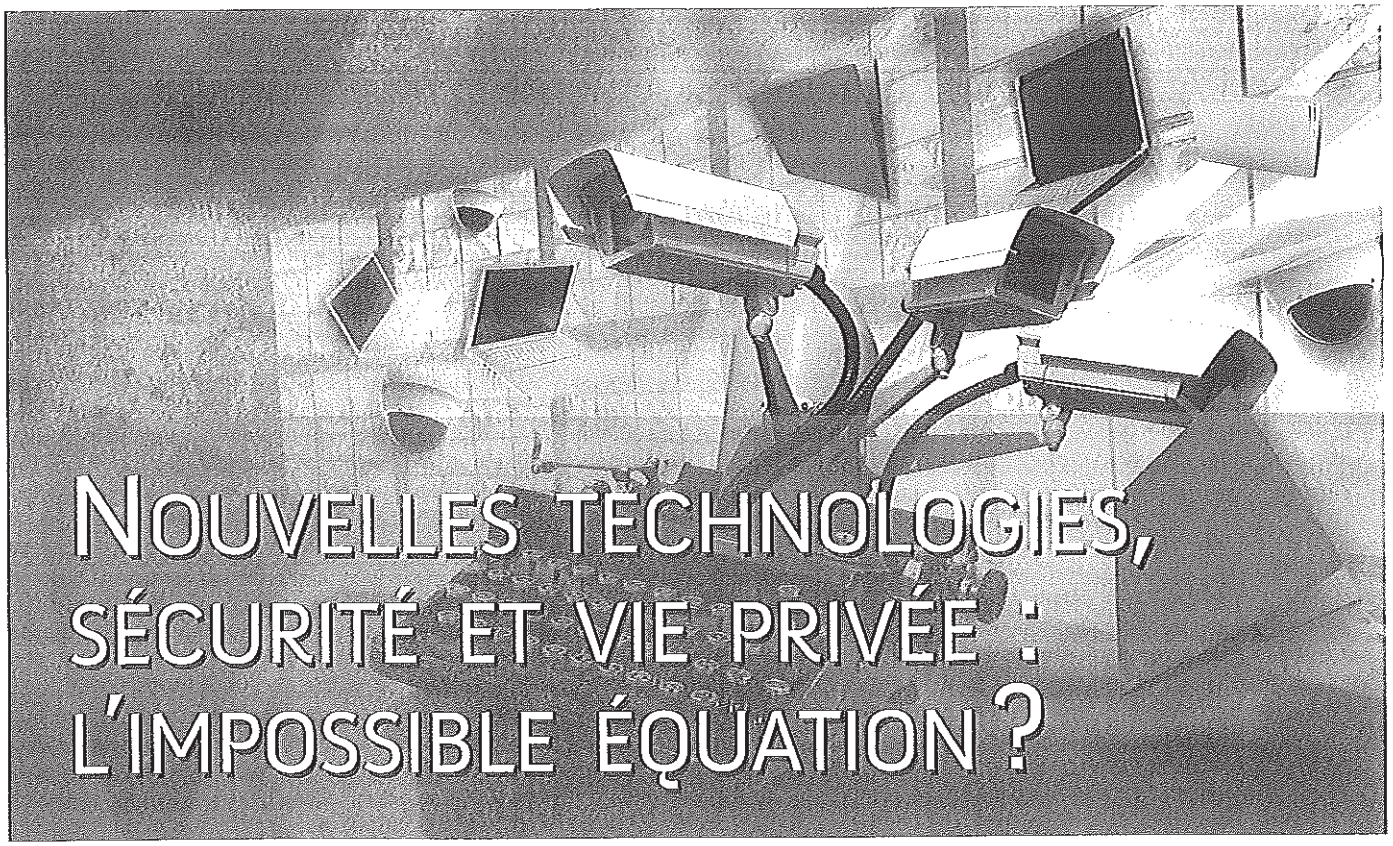
ACTUALITÉ JURIDIQUE PÉNAL

Dossier



NOUVELLES TECHNOLOGIES, SÉCURITÉ ET VIE PRIVÉE

DALLOZ



Nouvelles technologies, sécurité et vie privée : l'impossible équation ?

Vidéo-protection ou vidéosurveillance : deux termes recouvrant une même réalité mais avec deux approches radicalement différentes. Cette divergence de terminologie illustre bien le propos de ce dossier qui pose la question des risques d'atteintes à la vie privée via *l'exploitation des nouvelles technologies au nom de la sécurité.*

Ainsi, du côté des pouvoirs publics, il apparaît que si les fichiers de police se multiplient, leur contrôle est de moins en moins effectif au détriment des intéressés. Du côté de la société civile, sous la pression américaine, la pratique du whistleblowing *tend à se développer en Europe; mais, s'agissant d'une pratique totalement étrangère à notre culture, elle est encadrée strictement. Enfin, les garanties liées à l'usage de la vidéo, dont l'efficacité ne semble pas à la hauteur de ce qu'en attend le public, pâtit de la coexistence de deux systèmes parallèles... mais des textes plus protecteurs des droits des citoyens sont attendus prochainement.*

adoptée en première lecture par l'Assemblée Nationale en décembre 2009 valide la création de la plupart des fichiers de police par simple arrêté. Le procureur de la République serait par ailleurs autorisé à faire état d'informations visées dans les fichiers d'antécédents à l'occasion d'une comparution immédiate. Si cette réforme aurait le mérite d'encadrer des pratiques officieuses constatées dans quelques juridictions, et de porter à la connaissance de la défense l'utilisation de telles informations dans le processus pénal, elle aurait pour effet de légitimer des pratiques attentatoires à la présomption d'innocence. Une nouvelle fois, la preuve serait faite que le droit à la sécurité, pourtant présenté comme une déclinaison du droit à la sûreté, se déploie au détriment de la protection des citoyens contre l'arbitraire de l'État.

LE *WHISTLEBLOWING* ET LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL : LE COMPROMIS AMÉRICANO-EUROPÉEN

par Emilie Bailly et Emmanuel Daoud
Avocats au Barreau de Paris, Cabinet Vigo associés

La protection des données à caractère personnel n'est pas une notion abstraite, mais traduit la nécessité d'accorder des garanties concrètes aux personnes physiques : il s'agit de protéger un droit à ne pas être fiché, surveillé, contrôlé de manière abusive.

Sont considérées comme des données à caractère personnel toutes les informations qui permettent d'identifier directement ou indirectement une personne (nom, prénom, adresse électronique, numéro de téléphone, etc.).

En Europe, la collecte, le traitement et la conservation de telles données sont strictement encadrés par la directive 95/46/CE : elles doivent être collectées et traitées loyalement et licitement, en respectant, comme règle générale, le pouvoir de décision de la personne concernée; les personnes doivent être informées de l'identité du responsable du traitement et des finalités du traitement; le traitement des données doit être proportionnel aux finalités pour lesquelles elles sont collectées; les catégories particulières de données qui par leur plus grande sensibilité exigent une protection renforcée doivent être identifiées; la confidentialité et la sécurité des traitements doivent être garanties; enfin toute personne concernée doit avoir un droit d'accès au traitement, ainsi qu'un droit à la rectification, à l'effacement ou au verrouillage de ses données.

La protection des données ne peut être une réalité que si elle est effective. Ainsi, le non-respect de ces dispositions est sanctionné dans chaque pays européen selon leurs traditions juridiques, le législateur national ayant le choix entre des sanctions pécuniaires, pénales, administratives...

Depuis plusieurs années, les autorités européennes de protection des données doivent faire face à de nouveaux défis. En effet, les technologies et mécanismes de surveillance se sont développés à une vitesse époustouflante, au nom de la lutte contre le terrorisme et le crime organisé, mais aussi de la lutte contre la corruption et les autres formes de fraudes économique et financière.

En ce dernier domaine, les entreprises ont recours à leur personnel comme source d'information potentielle afin de prévenir les formes de délinquance précitées. Elles ont ainsi développé des mécanismes de *whistleblowing* (traduit en français par « procédure d'alerte » ou « alerte éthique »), par lesquels les salariés sont invités à dénoncer des pratiques illicites dont ils auraient eu connaissance dans le cadre de leur activité professionnelle à des personnes ou organismes en mesure d'y mettre un terme.

Pratique courante dans les pays de tradition de *common law*, tels que l'Australie, le Canada, le Royaume-Uni ou les États-Unis, le *whistleblowing* était, il y a encore peu, méconnu des systèmes de droit romano-germanique.

C'est la loi américaine *Sarbanes-Oxley Act* du 30 juillet 2002 (dite loi « SOX »), adoptée à la suite des scandales financiers Enron et WorldCom, qui est venue imposer aux sociétés internationales (et donc européennes) détenues en partie par des entreprises américaines ou cotées en bourse aux États-Unis, la mise en place d'un mécanisme de *whistleblowing*.

Dans la mesure où cette exigence américaine était assortie de sévères sanctions [1], les entreprises européennes concernées ont généralisé ce mécanisme d'alerte. Toutefois, le *whistleblowing* a suscité une réaction de franche hostilité en Europe, comme en témoigne la décision récente de la Cour de cassation française qui a annulé le mécanisme de *whistleblowing* de la société Dassault Systèmes [2]. Outre le fait que dans la plupart des pays européens, les normes politiques et administratives ne valorisent pas la délation [3], de nombreuses voix se sont élevées pour dénoncer le fait que ces mécanismes de *whistleblowing* pouvaient entrer en conflit avec la législation européenne en matière de respect de la vie privée et de protection des données à caractère personnel.

(1) Les sociétés qui ne se conforment pas à ces obligations en matière de dénonciation des dysfonctionnements sont passibles de lourdes sanctions et peines infligées par le Nasdaq, la bourse de New York ou la *Securities and Exchange Commission* (Organisme fédéral américain de réglementation et de contrôle des marchés financiers).

(2) Soc. 8 déc. 2009, n° 08-17.191, publié au Bulletin.

(3) Selon le Rapport de M. Pieter Omtzigt pour la Commission des questions juridiques et des droits de l'homme, *La protection des « donneurs d'alerte »*, du 14 septembre 2009, ces attitudes culturelles sont « profondément ancrées depuis les régimes sociopolitiques de dictature et/ou de domination étrangère sous lesquels il était tout à fait normal de se méfier des "informateurs" des autorités méprisées. C'est probablement parce que les États-Unis et le Royaume-Uni ont été longtemps épargnés qu'ils ont pu développer un climat bien plus favorable aux "donneurs d'alerte" que la plupart des pays d'Europe ».

En effet, une telle procédure, qui implique pour un salarié de dénoncer des faits précis concernant d'autres personnes, est particulièrement intrusive. La dénonciation peut porter atteinte au droit à la vie privée du salarié objet de la dénonciation et avoir des conséquences considérables sur son avenir professionnel parfaitement injustifiées si elle s'avérait infondée.
Par ailleurs, le mécanisme de *whistleblowing* tel que prévu par la SOX porte atteinte aux dispositions européennes de protection des données personnelles et notamment au droit d'information et d'opposition des personnes concernées, à la proportionnalité du traitement des données, ainsi qu'aux règles en matière de transfert de données.
Or, l'obligation imposée par une loi étrangère exigeant l'établissement du mécanisme de *whistleblowing* ne saurait permettre de contourner la réglementation européenne en matière de protection des données à caractère personnel, qui – faut-il le rappeler – est plus stricte qu'elle ne l'est outre-Atlantique.
Pour dépasser ces clivages et permettre l'instauration du mécanisme de *whistleblowing* dans les entreprises européennes dans le respect du droit communautaire et des dispositions nationales applicables, des négociations entre les autorités américaines et européennes ont été menées.
Après une présentation générale des mécanismes de *whistleblowing*, nous reviendrons sur leur difficile instauration dans les pays européens avant de proposer un rapide tour d'horizon des réglementations adoptées par nos voisins en la matière.

Les mécanismes de *whistleblowing*

Les États-Unis ont été les premiers à instaurer de tels systèmes de dénonciation et ce dès la fin du XIX[e] siècle [4].
Toutefois, ce n'est qu'en 2002, que la SOX a institutionnalisé le *whistleblowing* dans toutes les entreprises. On a vu, en effet, que la SOX impose aux sociétés américaines, à leurs filiales implantées à l'étranger, ainsi qu'aux sociétés étrangères cotées aux bourses américaines, de mettre en place un mécanisme d'alerte interne, habilité à recevoir et à traiter les dénonciations de salariés concernant des fraudes ou des malversations financières ou comptables, dont ils auraient eu connaissance dans le cadre de leurs fonctions [5].
Les sociétés qui ne se conforment pas à ces obligations en matière de dénonciation des dysfonctionnements sont passibles de lourdes sanctions et peines infligées par le Nasdaq, la bourse de New York ou la Securities and Exchange Commission [6].
Le *whistleblowing*, tel qu'instauré par le droit américain, a pour but de favoriser la responsabilisation des collaborateurs de l'entreprise et de ses dirigeants, et ainsi de lutter efficacement contre la corruption, les malversations et les abus en tous genres, dans le secteur public comme dans le privé [7]. Le mécanisme de *whistleblowing* peut se concrétiser sous la forme d'un numéro de téléphone « ligne éthique » ou une adresse électronique particulière mis à disposition des salariés.
Bien que centrée sur les questions financières et de comptabilité, la SOX n'interdit pas les dénonciations relatives à d'autres comportements répréhensibles (tels que le harcèlement sexuel, la violation des chartes éthiques...), et les entreprises américaines n'ont pas hésité à étendre le champ des faits susceptibles d'être dénoncés. Ce développement s'explique par le fait que l'approche américaine est fondée sur un contrat individuel entre le citoyen et l'État, qui l'incite à protéger et contrôler les agissements contraires à l'intérêt collectif. Aux États-Unis, la dénonciation des abus est considérée comme un devoir et les donneurs d'alerte comme des héros publics [8].
La conception européenne est radicalement différente. Certes les pays européens reconnaissent que les mécanismes de *whistleblowing* peuvent être utiles pour permettre à une société ou à une organisation de contrôler le respect des règles et des dispositions qu'elle a instaurées en matière de gouvernement d'entreprise, en particulier dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière et du droit pénal. Il n'en demeure pas moins que ces systèmes doivent être encadrés, et le droit fondamental à la protection des données à caractère personnel consacré par l'Union européenne, respecté d'un bout à l'autre du processus de *whistleblowing*, au bénéfice du dénonciateur, comme de la personne mise en cause.

La difficile instauration du *whistleblowing* dans les sociétés européennes

Outre les divergences culturelles et historiques qui expliquent en partie le décalage entre les États-Unis et les pays européens dans la mise en œuvre de tel mécanisme, les pays ont dû faire face à un conflit relatif à la protection des données à caractère personnel.
Aux États-Unis, la protection de la vie privée et des données à caractère personnel est assurée par un ensemble complexe de réglementations sectorielles, tant au niveau fédéral que des États, auxquelles vient s'ajouter l'autorégulation observée par l'industrie [9]. Il n'existe toutefois aucune législation globale à vocation universelle, et aucun contrôle par un organisme indépendant (du type CNIL) n'est prévu.
Ainsi, pour satisfaire à l'obligation d'implanter une procédure de réception et de traitement des dénonciations des employés relatives aux infractions dont ils seraient témoins, certaines entreprises américaines n'hésitent pas à mettre en place un système de réception, de traitement et d'archivage automatique de toutes sortes de dénonciations qui peuvent souvent porter sur des sujets très éloignés des infractions comptables et financières, et qui sont

(4) La législation sur le *whistleblowing* remonte au XIX[e] siècle avec l'introduction, durant la guerre civile, du *False Claims Act* à la suite de la découverte de la vente, par certaines entreprises, de fournitures défectueuses à l'armée.
Le *Whistleblower Protection Act* (WPA) constitue le principal texte législatif de protection des donneurs d'alerte aux États-Unis. Toutefois, cette loi ne s'appliquait qu'aux employés du secteur public, et uniquement aux personnes travaillant dans les organes fédéraux.
(5) L'article 301 (4) de la SOX dispose que « chaque comité de vérification doit établir des procédés pour : (1) consigner, conserver et traiter les plaintes reçues par la société au sujet de questions de comptabilité, de contrôles comptables internes ou de vérification; (2) et la soumission anonyme et confidentielle, par les employés, de leurs inquiétudes au sujet de questions douteuses en matière de comptabilité ou de contrôle ».
(6) Le *Listing Manual* de la Bourse de New York (art. 303A.10) et le *Listing Manual* du Nasdaq (art. 4350) disposent que les sociétés cotées doivent adopter un code d'éthique pour les administrateurs, cadres et employés. Dans le commentaire, il est souligné que tout code d'éthique doit contenir des normes et des procédures de mise en conformité destinées à faciliter son application effective et, entre autres, des procédures d'alerte éthiques et une protection des lanceurs d'alerte.
(7) V. le Rapport de M. Pieter Omtzigt pour la Commission des questions juridiques et des droits de l'homme, *La protection des « donneurs d'alerte »*, 14 sept. 2009.
(8) Rapport de M. Pieter Omtzigt, préc.
(9) Avis n° 1/99 concernant le niveau de protection des données à caractère personnel aux États-Unis et les discussions en cours entre la Commission européenne et le gouvernement américain, adopté par le Groupe 29 le 26 janv. 1999.

conservées pour une durée indéterminée.
À la suite de l'adoption de la SOX, plusieurs affaires emblématiques ont révélé les réticences des pays européens à adopter de tels mécanismes jugés contraires à la protection des données personnelles.
En effet, au sein de l'Union européenne, la protection des données à caractère personnel a une vocation universelle et a été érigée au rang de liberté fondamentale par l'article 8 de la Charte des droits fondamentaux de l'Union européenne [10].
La directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, a fixé des normes de protection des données personnelles parmi les plus élevées au monde et prévoit des sanctions en cas de violation de ces règles [11].
En outre, les libertés et droits fondamentaux relatifs aux principes régissant la protection des données à caractère personnel dans l'Union européenne ne peuvent être restreints que dans les cas où cela est nécessaire au sein d'une société démocratique ou pour les besoins de la protection des intérêts publics.

Ainsi, en France, la CNIL a, dans un premier temps, refusé d'autoriser les dispositifs d'alerte professionnelle qu'elle qualifiait de « systèmes organisés de délation professionnelle » [12]. Elle estimait que « les dispositifs présentés étaient disproportionnés au regard des objectifs poursuivis et des risques de dénonciations calomnieuses et de stigmatisation des employés objets d'une alerte éthique ». En Allemagne, le code d'éthique d'une société de grande distribution, qui prévoyait la mise en place d'une « ligne éthique », a été annulé au motif que la direction n'avait pas sollicité l'accord préalable du comité d'entreprise [13].
Toutefois, ces positions radicalement « anti-*whistleblowing* » mettaient les sociétés européennes en porte-à-faux par rapport à la réglementation américaine [14] et étaient donc source d'insécurité juridique.
Ainsi, afin de permettre aux entreprises françaises concernées de se conformer à la SOX et après des consultations avec ses homologues européens et les autorités américaines, la CNIL a admis, dès 2006, le principe du *whistleblowing*, tout en restreignant son champ à des domaines précis (comptabilité, contrôle des comptes, domaine bancaire, corruption) et en précisant les conditions que doivent remplir les mécanismes de *whistleblowing* pour être conformes à la loi du 6 janvier 1978 (dite « Informatique et libertés ») et à la directive 95/46/CE [15].

> La directive 95/46/CE a fixé des normes de protection des données personnelles parmi les plus élevées au monde et prévoit des sanctions en cas de violation de ces règles.

Dans la foulée, le Groupe 29, organe consultatif européen indépendant sur la protection des données et de la vie privée [16], a rendu un avis [17], dans lequel il a confirmé la position de la CNIL, estimant que « loin d'empêcher » les mécanismes de *whistleblowing*, la directive 95/46/CE contribue à leur bon fonctionnement en les encadrant et en en réduisant les risques.
Cet avis, a servi de ligne directrice pour la mise en œuvre par les sociétés européennes de mécanismes de *whistleblowing* dans le respect des règles de protection des données instaurées par l'Union européenne. Selon le Groupe 29, la légalité du mécanisme de *whistleblowing* dépend, entre autres choses, des points suivants :
- le traitement doit être légitime, c'est-à-dire que l'établissement du mécanisme de *whistleblowing* est nécessaire au respect d'une obligation légale ou à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ;
- en application du principe de proportionnalité, le groupe de travail recommande la limitation du nombre de personnes autorisées à signaler des irrégularités ou fautes présumées, ainsi que le nombre de personnes susceptibles d'être mises en cause par le biais d'un mécanisme de *whistleblowing* ;
- le groupe de travail recommande de privilégier les signalements confidentiels dont l'auteur est identifié par rapport aux signalements anonymes ;
- les données collectées et traitées par le biais d'un mécanisme de *whistleblowing* doivent se limiter aux données strictement et objectivement nécessaires pour vérifier les allégations faites ; celles-ci étant, elles-mêmes, limitées aux domaines de la comptabilité, des contrôles comptables internes, de l'audit ou de la criminalité bancaire et financière et de la lutte contre la corruption ;
- la durée de conservation des données à caractère personnel ne saurait excéder un délai de deux mois à compter de l'aboutissement de l'enquête sur les faits signalés ;
- le responsable du traitement doit informer les personnes concernées de l'existence, la finalité et le fonctionnement du mécanisme de *whistleblowing*, ainsi que de leurs droits d'accès, de rectification et de suppression.

Sur la base de cet avis, la majorité des autorités de protection des

(10) L'article 8 dispose :
« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »
La charte est intégrée dans le traité de Lisbonne et juridiquement contraignante pour l'Union européenne et ses États membres lorsqu'ils mettent en œuvre le droit de l'Union.

(11) L'article 24 de la directive dispose « les États membres prennent les mesures appropriées pour assurer la pleine application des dispositions de la présente directive et déterminent notamment les sanctions à appliquer en cas de violation des dispositions prises en application de la présente directive ». Bien entendu, les sanctions varient en fonction des États membres et de leurs traditions juridiques, le législateur national ayant le choix entre des sanctions pécuniaires, pénales, administratives.

(12) Délibération n° 2005-110 du 26 mai 2005 relative à une demande d'autorisation de McDonald's France pour la mise en œuvre d'un dispositif d'intégrité professionnelle.
Délibération n° 2005-111 du 26 mai 2005 relative à une demande d'autorisation de la Compagnie européenne d'accumulateurs pour la mise en œuvre d'un dispositif de « ligne éthique ».

(13) Décision de l'Arbeitsgericht (conseil de prud'hommes) de Wuppertal, en date du 15 juin 2005, confirmée par le Landesarbeitsgericht (conseil de prud'hommes national) de Düsseldorf, le 14 nov. 2005.

(14) Les entreprises françaises et les filiales françaises de sociétés américaines cotées sur les marchés américains, directement ou indirectement concernées par la SOX, étaient franchement pénalisées.

(15) Document d'orientation adopté par la Commission le 10 nov. 2005 pour la mise en œuvre 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.
La CNIL a également adopté, le 8 décembre 2005, une décision d'autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle, conformes aux orientations retenues par elle (Délibération n° 2005-305 du 8 décembre 2005 « portant autorisation unique de traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle »).

(16) La directive 95/46/CE a instauré, en son article 29, un groupe de travail baptisé « Groupe de protection des personnes à l'égard du traitement des données à caractère personnel » (également appelé « Groupe de travail article 29 » ou « Groupe 29 » ou « G29 »), ayant pour mission notamment de conseiller la Commission européenne, et lui donner un avis autorisé, sur toute mesure communautaire ayant une incidence sur les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel et de la protection de la vie privée.

(17) Avis préc. note 9.

données des pays européens ont adopté des recommandations qui, bien qu'elles ne soient pas juridiquement contraignantes, constituent des normes de référence pour les sociétés européennes soucieuses d'instaurer un mécanisme de *whistleblowing* tout en respectant les dispositions nationales et communautaires en matière de protection des données.

Tour d'horizon des réglementations européennes en matière de mécanisme de *whistleblowing*

À l'exception du Royaume-Uni, les pays européens n'ont pas de législation propre au mécanisme de *whistleblowing*. En revanche, en application de la directive 95/46/CE, chaque pays membre s'est doté d'une autorité de protection des données à caractère personnel, qui ont pour la plupart édicté des recommandations en la matière.

Pour la mise en place des mécanismes de *whistleblowing*, la majorité des autorités de protection des données des pays européens ont adopté des recommandations qui bien qu'elles ne soient pas juridiquement contraignantes, constituent des normes de référence.

Ces recommandations n'ont pas valeur de loi, mais constituent des lignes directrices expliquant comment les responsables du traitement des données peuvent concilier les exigences de la procédure américaine de *whistleblowing* avec les règles protectrices des données à caractère personnel de la directive 95/46/CE transposée en droit national interne.

On a vu qu'en France, la CNIL a adopté le 10 novembre 2005 un document d'orientation pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004 [18], relative à l'informatique, aux fichiers et aux libertés.

Le *whistleblowing* est considéré comme un mécanisme supplémentaire complétant les procédures d'information et de notification classiques, tels que les représentants du personnel, la voie hiérarchique...

Le domaine d'application du *whistleblowing* est strictement défini : les dénonciations ne peuvent concerner que « les domaines financier, comptable, bancaire et de la lutte contre la corruption ». La chambre sociale de la Cour de cassation a récemment jugé qu'un dispositif d'alerte professionnelle ne peut en aucune manière concerner d'autres domaines que les domaines financier, comptable, bancaire et de lutte contre la corruption, à moins d'avoir fait l'objet d'une autorisation préalable individuelle par la CNIL [19].

Les dénonciations anonymes ne sont autorisées que dans des cas strictement limités.

Les données doivent être détruites dans les deux mois qui suivent la conclusion de l'enquête sur les faits signalés. Les dénonciations non fondées doivent être supprimées immédiatement.

Le traitement local des données est exigé pour préserver la confidentialité.

En Belgique, la Commission de la protection de la vie privée a émis une recommandation, le 29 novembre 2006 [20] concernant la compatibilité des programmes de *whistleblowing* avec la loi belge de protection des données.

Cette recommandation suit de manière générale l'avis du Groupe 29 et la décision de la CNIL.

Toutefois, elle étend le champ des dénonciations au-delà des matières financière et comptable.

Elle encourage la confidentialité et n'accepte les dénonciations anonymes que de manière exceptionnelle.

Elle considère le *whistleblowing* comme un mécanisme supplémentaire par rapport aux voies traditionnelles de dénonciation.

Le transfert de données à un pays tiers de l'Union européenne n'est possible que si les faits dénoncés impliquent des problèmes graves nécessitant un traitement au-delà du niveau européen ou peuvent avoir des répercussions au-delà de la compagnie située en Belgique ou dans l'Union européenne.

Les données ne peuvent être conservées plus longtemps que pour les besoins de l'enquête sur les faits signalés.

En Espagne, l'Agencia Española de Protección de Datos (AEPD) n'a pas publié de recommandation sur le *whistleblowing*. En revanche, en 2007, l'AEPD a rendu une décision à la suite d'une demande d'une société pharmaceutique japonaise, qui fait « précédent ». Cette décision suit de manière générale l'avis du Groupe 29 et la décision de la CNIL.

Comme en Belgique, le champ des dénonciations est plus largement défini : des dénonciations peuvent être faites dans des domaines autres que les finances et la comptabilité.

L'AEPD n'accepte pas des dénonciations anonymes, là ou le Groupe 29 se contente de les déconseiller.

Les dispositions applicables au transfert de données vers des États tiers suivent les règles posées par l'Union européenne, et plus particulièrement par la directive 95/46/CE.

L'AEPD exige la suppression des données dès lors que celles-ci cessent d'être nécessaires.

En Allemagne, le groupe de travail *ad hoc* sur la « protection des données des employés » du Düsseldorfer Kreis [21] reprend, également, de manière générale l'avis du Groupe 29 et la décision de la CNIL.

Selon lui, les systèmes de *whistleblowing* doivent être considérés comme un mécanisme additionnel venant en supplément des canaux traditionnels de dénonciation.

Le champ des dénonciations peut inclure les questions d'éthique au-delà des domaines financier et comptable.

Les dénonciations anonymes ne sont pas encouragées, sauf cas exceptionnels. En revanche, la confidentialité doit être assurée.

Le transfert des données personnelles du dénonciateur ou de la personne incriminée à un tiers est interdit, exception faite des éventuelles autorités chargées d'enquêter sur les faits dénoncés.

Enfin, les données doivent être supprimées dans un délai de deux mois après la fin des investigations sur les faits dénoncés.

Conclusion

Dans ces périodes de crise où l'opinion publique mondiale exige davantage de transparence et de moralité dans le monde des affaires, la tentation de céder à la « facilité » de la dénonciation est grande.

(18) Loi n° 2004-801 du 6 août 2004.

(19) Soc. 8 déc. 2009, n° 08-17.191, préc.

(20) Recommandation n° 01/2006 du 29 novembre 2006 relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

(21) Groupe réunissant toutes les autorités de protection des données allemandes.

En ne précisant pas les modalités de mise en œuvre de tels systèmes (périmètre des faits susceptibles d'être dénoncés, information du mis en cause, conservation, transfert des données, etc.), la loi américaine a indiscutablement fait primer les impératifs économiques sur la protection des données personnelles. En effet, sous prétexte de plus de transparence, tous les salariés d'une entreprise pouvaient faire l'objet d'une dénonciation et être ainsi « fichés ».
Cette régression des libertés publiques des citoyens, (qui plus est dictée par les lois du marché financier... américain) a suscité de vives réactions dans les pays européens. Des négociations inévitables ont été engagées et ont permis de déboucher sur un compromis relatif aux modalités de mise en œuvre de ces mécanismes de *whistleblowing*.
Les avis et recommandations émis par le Groupe 29 et la majorité des autorités de protection des données européennes démontrent, s'il en était besoin, qu'il est toujours possible d'atteindre un juste équilibre entre la protection de la vie privée et des données personnelles, et les impératifs de lutte contre la fraude.

VIDÉOSURVEILLANCE, RISQUES D'ATTEINTES AUX LIBERTÉS : UNE DUALITÉ DE RÉGIME INSATISFAISANTE

Interview d'Alex Türk
Président de la CNIL (Commission nationale de l'informatique et des libertés), sénateur du Nord

AJ Pénal : *Quels sont les risques d'une vidéosurveillance qui se généralise de plus en plus ?*
Alex Türk : C'est un sujet sur lequel la CNIL est très vigilante sans toutefois condamner la vidéosurveillance. En effet, son propos n'est pas de rejeter *a priori* cette technologie qui peut rendre des services dans certaines hypothèses.
Une réflexion préalable doit être rappelée : un sondage a été effectué il y a deux ans dont il est ressorti que 71 % des Français sont favorables à la vidéosurveillance puisqu'ils considèrent que cela peut augmenter le niveau de sécurité collective. 79 % d'entre eux considèrent qu'on ne peut pas développer la vidéosurveillance sans mettre en place les dispositifs nécessaires pour garantir le respect des libertés individuelles.
Deuxième idée force, la vidéosurveillance aujourd'hui s'inscrit dans un ensemble qui génère un débat d'une plus grande ampleur : l'évolution exponentielle de la vidéo, de la biométrie et de la géolocalisation des personnes et des biens. Toutes ces technologies se développent fortement et créent des synergies entre elles. Cela entraîne de plus en plus de couplages, comme par exemple entre la vidéosurveillance et la biométrie (qui relève d'un régime d'autorisation préalable). Toutes ces technologies différentes convergent pour aboutir à une société de traçage : l'individu aujourd'hui est tracé physiquement dans l'espace par la vidéosurveillance, la biométrie ou la géolocalisation (y compris par des technologies d'usage quotidien comme le téléphone portable, la carte bancaire, les passes de transport en commun). À cela s'ajoute le développement du suivi des personnes sur les réseaux sociaux et les moteurs de recherche qui conduit à un traçage dans le temps puisque les informations demeurent parfois indéfiniment sur internet.
On prend alors conscience de l'ensemble de la problématique et l'on constate que l'on est en train de changer de mode de civilisation : nous entrons dans la civilisation de la société de surveillance liée aux technologies numériques. Ceci amène à reconsidérer toute la problématique de la vidéosurveillance car elle doit être vue comme un élément dans un ensemble.

AJ Pénal : *Les propositions d'installations de systèmes de vidéosurveillance sont très nombreuses : la CNIL intervient-elle en amont auprès de ces entreprises pour vérifier qu'elles respectent bien la réglementation dans ce domaine ?*
A. Türk : Nous le faisons mais les sociétés qui développent la vidéo ont avant tout un objectif commercial et n'informent pas systématiquement leurs clients de leurs obligations. Le constat est le même, voire pire, en matière de biométrie. Il existe des sociétés qui commercialisent des systèmes biométriques sans préciser à leurs clients qu'ils doivent obtenir une autorisation préalable de la CNIL. C'est pour cette raison que des dizaines de proviseurs qui ont installé des bornes biométriques à l'entrée des réfectoires découvrent après coup qu'ils sont dans l'illégalité la plus totale. Certaines sociétés leur indiquent même que leur système biométrique est homologué par la CNIL. Or, nous n'avons jamais homologué aucun système biométrique.

AJ Pénal : *Le nombre de déclarations à la CNIL est-il croissant ? Le régime des demandes d'autorisation (à la CNIL ou à la préfecture) est-il clarifié (pour les cas qui posaient problème : comme l'installation dans un lieu mixte avec conservation des données) ?*
A. Türk : Il faut distinguer les deux régimes juridiques existant en matière de vidéosurveillance :
Pour les zones auxquelles le public a accès : un régime d'autorisations (le cas le plus général) données par les commissions départementales placées auprès des préfets (commission présidée par un magistrat, qui donne un avis au préfet qui accorde ou non l'autorisation). La commission départementale fait ensuite des contrôles sur le terrain (v. la circulaire du 12 mars 2009 relative aux conditions de travail de déploiement des systèmes de vidéoprotection).
Pour les zones d'accès privé : un régime de déclarations à la CNIL