

Organisation, technologies de l'information et vie privée.

Henri Isaac, Maître de conférences en sciences de gestion

Michel Kalika, Professeur en sciences de gestion

CREPA, Université Paris Dauphine, 75775 Paris Cedex

isaac@dauphine.fr

michel.kalika@cip.dauphine.fr

Introduction.

La question du respect de la vie privée dans l'entreprise et dans les relations commerciales a suscité un intérêt particulier au cours de ces derniers mois. Licenciement pour usage personnel de l'Internet dans l'entreprise, courrier électronique « ouvert » par l'employeur (Kovach & alii, 2000), il n'est pas une semaine sans que les médias, les forums sur Internet ne débattent de ces questions. Comment comprendre l'émergence de cette problématique dont la véritable nature n'est pas simplement managériale ou économique mais aussi sociologique ? Qui peut encore soutenir que cette question n'a pas sa place en management tant la rationalisation des méthodes de gestion a conduit à évacuer les aspects de la vie privée dans l'entreprise ?

La question de la relation entre technologies de l'information et vie privée se pose en France avec une acuité particulière. En effet, la réforme récente du temps de travail a été l'occasion d'un vif débat sur la frontière entre vie professionnelle et vie privée.

Le développement des technologies de l'information, qu'il s'agisse du téléphone mobile ou de l'Internet, est certainement en partie responsable de l'émergence de ce débat, car ces outils permettent aisément le suivi de l'activité du salarié ou l'identification des clients et l'exploitation des données dans une relation salariale ou commerciale. Plus généralement, les technologies de l'information, par la puissance de traitement qu'elles permettent et par leur usage, inquiètent. Elles troublent à la fois le salarié qui utilise son courrier électronique et le client qui remplit un formulaire en ligne. Les technologies de l'information rendent possible une double *traçabilité* des comportements (tant interne qu'externe) génératrice de méfiance.

Cette inquiétude partagée est à notre sens le point crucial. En effet, la disparition de l'anonymat ne concerne pas seulement les relations marchandes mais aussi les relations salariales. Une des caractéristiques essentielles des mutations organisationnelles actuelles est précisément la fin de l'anonymat et la nécessité d'identifier les acteurs économiques qu'ils soient clients ou salariés.

[1] Deux facteurs expliquent la disparition de l'anonymat : l'évolution des formes organisationnelles du travail et le progrès des technologies de l'information. La fin des relations anonymes n'est pas sans poser de sérieuses interrogations quant à l'utilisation des données personnelles. [2] La réflexion et les pratiques actuelles pèchent lourdement et risquent d'entraîner une forte défiance de la part des salariés. Ceci remet directement en cause la politique de transparence des données privées et risque à terme de d'affaiblir tous les dispositifs déployés par les entreprises en la matière. [3] Il nous semble dès lors nécessaire, de mettre en place une véritable politique de gestion des données privées, qu'il s'agisse de données internes ou de données externes.

[1] L'évolution des formes organisationnelles du travail

Alors même que le développement du capitalisme occidental s'est appuyé sur l'usage de l'anonymat dans les relations économiques, il semble désormais que sa croissance appelle une remise en cause de cette caractéristique essentielle de l'extension du domaine marchand.

La croissance des économies occidentales s'est appuyée sur la transformation de relations sociales en relations économiques et notamment la transformation du travail en marchandise (Polanyi, 1983). Ce développement s'est systématisé par la mise en place d'appareils productifs de masse dès le début du XX^e siècle et trouve son accomplissement dans ce que l'on appelle le fordisme. Dans ce système productif, les entreprises fournissent des produits standardisés en masse. Les produits sont peu ou pas différenciés. Leur production s'appuie sur une organisation du travail très spécialisée dans laquelle l'identité des opérateurs importe peu puisque ce sont les méthodes et le contrôle de leur mise en œuvre qui sont censés en assurer l'efficacité. Les salariés ne sont que des *inputs* substituables sur un « poste de travail ». La fonction commerciale écoule des marchandises sur des marchés de masse où la connaissance *individuelle* du consommateur n'a que peu d'incidence sur l'efficacité des ventes.

Ce système n'est plus de mise aujourd'hui. Les raisons en sont multiples et certaines d'entre elles sont directement à l'origine de la modification des pratiques concernant l'identité des acteurs dans l'entreprise.

En premier lieu, les mutations radicales de l'environnement ont conduit les entreprises à se réinventer. Dans un contexte économique décrit comme un univers d'hyper-compétition, les entreprises ont procédé à des reconfigurations complètes de leur outil de production et de leur organisation, pour survivre (Boyer, Freyssenet, 2000). Dans cette perspective, les nouvelles formes d'organisation du travail recherchent une plus grande transversalité dans les processus opérationnels, une flexibilité accrue (Mayère, 1999), et une plus forte implication des employés dans l'obtention des gains de productivité (Coriat, 1990, 1995, Pochet, 1998). Cette recherche d'implication passe par une sélection plus forte des salariés. Les critères de sélection dépassent de plus en plus souvent les simples caractéristiques nécessaires à l'obtention du poste, particulièrement aux Etats-Unis où l'employeur peut légalement s'enquérir de très nombreux aspects de la vie privée d'un futur employé (Masters & Brown, 1994). L'employé s'apparente non plus à un *input* interchangeable mais à une ressource dont les caractéristiques importent dans l'univers concurrentiel. Dès lors, l'entreprise s'intéresse de plus en plus aux caractéristiques privées du salarié afin de s'assurer la collaboration d'une ressource à même de remplir non seulement des tâches définies par les processus, mais également des tâches non programmées, sources de comportements d'innovation et d'apprentissage.

En second lieu, les frontières de l'entreprise sont devenues beaucoup plus floues et changeantes dans le but de s'adapter et se reconfigurer en permanence au gré des évolutions de la demande. Cette évolution organisationnelle s'étend à la notion même de travail (passage de contrat de long terme à des contrats de court terme renouvelables ou non). Alors même que le travail a été longtemps conçu sur la base d'un triptyque (unité de lieu, unité de temps, unité d'action), celui-ci se définit désormais en dehors des heures officielles de l'activité, en dehors du lieu de travail

et requiert souvent un esprit d'initiative qui dépasse les procédures existantes (Alter, 2000, Akerloff, 1976, Lallé, 1999). La frontière entre vie privée et vie professionnelle devient donc très floue pour certaines catégories de salariés. Cette évolution est elle-même rendue possible par les nouveaux outils de communication.

Les mutations organisationnelles se sont appuyées sur des évolutions fondamentales des technologies de l'information entraînant de profonds changements des systèmes d'information des entreprises (Isaac, 2000). Une des caractéristiques majeures de ces systèmes réside dans leur capacité de *traçabilité* totale des échanges d'informations¹. Par exemple, les technologies de l'Intranet comportent par nature des fonctions de collecte d'informations sur l'activité des différents salariés l'utilisant. Il est désormais possible de suivre très précisément l'activité sur un poste de travail informatisé (nombre et types de touches enfoncées sur un clavier, durée d'utilisation d'une application, données saisies). Il devient donc aisé d'effectuer un contrôle très précis de la productivité individuelle, qu'il s'agisse du travail sur ordinateur, sur caisse enregistreuse ou sur machine à commandes numériques, sans que l'employé en ait conscience.

Dans cette perspective, nombreuses sont les entreprises qui filtrent l'accès Internet afin de limiter la flânerie supposée (chère à Taylor) de leurs salariés. De plus, le coût du contrôle de la productivité du travail a fortement diminué, notamment par la suppression de certains échelons hiérarchiques traditionnellement en charge de ce type de contrôle.

Par ailleurs, les nouveaux outils de communication obligent pour des raisons de sécurité, et au-delà des fonctions de traçage inhérentes aux outils, à vérifier les communications entrantes et sortantes de l'entreprise (téléphone, courrier électronique, données numériques). Ceci conduit à traiter tous les courriers électroniques comme des courriers professionnels. Il y a là une nouveauté dans la façon dont les entreprises appréhendent ce vecteur de communication. En effet, elles n'ont jamais filtré *l'ensemble* des communications téléphoniques de leurs employés. Elles en ont fortement limité l'utilisation – volontairement ou involontairement - à des fins privées en réorganisant l'espace de travail sous forme de plateaux ouverts. La promiscuité agit dans cet espace comme un frein à la sphère privée. A cet égard, le courrier électronique permet aux salariés d'échapper à cette contrainte car il est silencieux et non détectable par les collègues. Dès lors, il devient nécessaire de filtrer l'ensemble des courriers électroniques.

Enfin, les outils de la communication mobile (*pager*, téléphone mobile, assistant numérique personnel, ordinateur portable), permettent d'étendre l'activité en dehors du lieu et du temps de travail. Ils rendent possible la mobilisation du personnel où qu'il se situe. Non seulement ils permettent à l'entreprise de contacter un salarié en permanence (extension de l'astreinte dans le temps et l'espace), mais ils incitent ou contraignent le salarié à utiliser une partie de son temps personnel pour son travail.

[2] Les risques des technologies de l'information

Intrinsèquement, les technologies de l'information ne sont pas porteuses d'atteinte à la vie privée. C'est leur utilisation abusive et non concertée qui est à l'origine d'une méfiance accrue de la part des salariés. Le risque majeur est un accroissement de la

¹ Pour un panorama détaillé et didactique de la traçabilité des outils informatiques, cf. Bouchet H., 2001.

défiance des utilisateurs vis-à-vis de telles pratiques aboutissant à l'inefficacité de ces nouvelles méthodes. Alors même que ces systèmes de contrôle panoptique apparaissent très efficaces et peu coûteux, quels sont donc précisément ces risques dans l'entreprise et leur impact sur le fonctionnement de l'organisation ?

Le développement des technologies de l'information dans l'entreprise conduit à l'émergence de systèmes de contrôle des salariés que l'on peut qualifier à la suite de Foucault, de panoptique (Foucault, 1975). La particularité de ces dispositifs est liée à leur capacité d'observer l'ensemble des comportements sans être vu. Permanents dans ses effets sur les comportements individuels, ces systèmes de contrôle s'avèrent discontinus dans leur exercice. L'efficacité d'un système panoptique est atteinte lorsque l'exercice du pouvoir est inutile et que le système a réussi à créer un état de conscience des individus tel qu'il assure la conformité des comportements (Stanton & Weiss, 2000. Est-ce là une vision exagérée du contrôle électronique ? Nous ne le pensons pas, car au-delà de l'existence des outils spécifiques de contrôle centraux, les outils de travail collaboratif (*groupware*) multiplient les occasions de contrôle indirect entre salariés. Cette forme de contrôle porte notamment sur l'emploi du temps d'un salarié au travers du partage de son agenda en ligne existant dans de nombreuses applications de *groupware* (Lotus Notes, Microsoft Exchange par exemple). De fait, le contrôle est potentiellement présent en permanence mais ne s'exerce pas pour autant de façon continue. Dans ce contexte, n'y a-t-il pas un risque de rejet de la part des salariés et donc d'inefficacité d'un tel système ?

Pour répondre à cette interrogation, plusieurs éléments sont à considérer.

En premier lieu, il faut noter, qu'à notre connaissance, aucune étude exhaustive n'existe à ce jour sur l'utilisation *effective* des données issues de tels systèmes. Quelques informations très globales sur l'équipement des entreprises américaines (Corbin, 2000 ; Boehle 2000) sont disponibles. Seuls des cas dispersés de licenciements, de mises à pied, de rappels à l'ordre (Brown, 2000) sont relatés.

En second lieu, les *a priori* sur un tel système de contrôle dans l'entreprise conduisent à penser que ces dispositifs s'avèrent contre-productifs dans la mesure où ils réduisent la satisfaction liée au travail, augmentent le stress, et conduisent à développer un climat de défiance. Mais, plusieurs études récentes apportent des arguments nuancés à cet égard : une étude exploratoire sur un faible échantillon de salariés suggère que certains salariés ne perçoivent pas de tels systèmes comme une intrusion dans leur vie privée (Stanton & Weiss, 2000). Ceci est en partie confirmé par une autre recherche sur un échantillon plus vaste (Oz & alii, 1999. Un nombre non négligeable de personnes interrogées perçoit ces systèmes comme beaucoup plus justes dans l'évaluation de leur productivité individuelle que l'évaluation subjective par un contrôleur. Ces systèmes de contrôle seraient donc, par leur transparence, des facteurs d'amélioration de la perception de la justice procédurale. Il existe cependant des différences notables parmi les salariés en fonction de leur situation dans le système (observés, observateurs).

Il semble se dégager des recherches, que le déploiement et l'usage d'un tel dispositif doit faire l'objet d'une notification systématique aux employés pour que le système soit accepté (Vaught, Taylor, Vaught, 2000. Ces résultats conduisent à souligner la nécessité d'une véritable politique de gestion des données privées.

[3] Pour une véritable politique de gestion des données privées

Il apparaît donc de plus en plus nécessaire pour les entreprises d'intégrer dans les méthodes de management la question du respect de la vie privée de leurs salariés. Quelles pistes se dégagent actuellement pour cette nouvelle dimension du management de l'entreprise ? Les pratiques actuelles sont-elles suffisantes ?

Le management des données privées des salariés impose à l'évidence, à l'entreprise, le respect des législations existantes. Malheureusement, cette application n'est pas simple. En effet, de nombreux groupes opèrent dans différentes zones géographiques et juridiques dans lesquelles les lois en la matière divergent fortement. Dès lors, la multiplicité des règlements et leur mise en cohérence constituent parfois un obstacle difficile à surmonter. En outre, le rôle désormais central du système d'information de l'entreprise dans cette problématique empêche d'envisager cette question managériale uniquement sous l'angle juridique, tant les aspects techniques sont complexes.

Pour pallier l'insuffisance des législations, nombre d'entreprises ont mis en place des codes de bonne conduite (Isaac, Mercier 2001) ou des chartes d'utilisation de leur intranet et messagerie électronique (Cigref, 1999, 2000). A cet égard, les grandes entreprises françaises semblent avoir orienté leur réflexion plutôt sur l'utilisation du courrier électronique que sur l'utilisation d'Internet par le biais d'un intranet d'entreprise. Deux études récentes sur cette question (Cigref, 1999, 2000) mettent tout d'abord en évidence que le courrier électronique est désormais un outil banal et que les messages privés ne représentent en moyenne que 6% des volumes échangés. 84% des entreprises diffusent désormais des règles d'utilisation de la messagerie électronique, mais seulement 26% ont mis en place un comité d'éthique sur la question de son usage. Elles ne sont que 22% seulement à formaliser leurs règles d'observation des usages de la messagerie.

Il y a là un véritable défi pour l'entreprise. Elle ne peut plus longtemps continuer l'observation de ses salariés sans les en avertir ; ceci est illégal dans le cadre français (cf. Bouchet, 2001). En outre, l'entreprise doit mettre en place un accès du salarié aux données qu'elles stockent sur lui afin de se conformer à la loi « Informatiques et libertés. Combien d'entreprises offrent-elles ouvertement cette possibilité à leur salarié ? En la matière, il semble que tout reste à faire pour parvenir à un minimum de transparence tant les pratiques anciennes du secret demeurent présentes.

Autant la conformité à la législation, la formalisation des règles et leur large diffusion apparaissent souhaitables, autant ces mesures semblent encore insuffisantes.

Pour marquer l'importance de l'attention que l'entreprise apporte à cette question sensible dans la relation commerciale, les entreprises anglo-saxonnes ont créé une direction spécifique incarnée par le Chief Privacy Officer². Ce dernier est en charge de la gestion des données que l'entreprise utilise dans la relation commerciale. IL est envisageable d'étendre les prérogatives de cette direction à l'ensemble des données privées qu'elles soient internes ou externes. On s'orienterait donc vers un poste proche de celui d'*ombudsman* comme certaines entreprises anglo-saxonnes l'ont créé lors de la mise en place de leur politique éthique. Cette direction investie de prérogatives juridiques et techniques serait en charge du respect des procédures par l'entreprise tant pour les données concernant les salariés que pour les données issues des relations commerciales. A cet égard, c'est une véritable politique de

² A titre d'exemple, IBM a un CPO tout comme AOL, ou encore Doubleclick.

gestion de ces données que l'entreprise doit mettre en place (Henderson & Snyder, 1999). Elle aurait pour vocation de définir des règles de transparence des procédures d'accès aux données personnelles stockées par l'entreprise. Outre l'application des règles de transparence, la direction de la protection de la vie privée aurait également pour mission de créer un climat de confiance dans l'entreprise par tous les moyens appropriés. L'existence et la place dans l'organigramme d'une telle *direction des données privées* traduit l'importance que l'entreprise accorde à cette question sensible (Kalika, 1995).

[conclusion]

De nouveaux champs de recherche émergent et le besoin d'investigations empiriques apparaît. Quelles sont les pratiques des entreprises en matière de gestion de la relation TIC et vie privée ? Quelle est la perception des salariés quant à la mise en place et à l'utilisation de ces systèmes de contrôle ? Quelle est l'efficacité de ces nouveaux systèmes de contrôle numérique ? La diffusion rapide des technologies de l'information dans l'entreprise permet en effet à celle-ci de déployer de nouveaux dispositifs de surveillance de ses salariés. Qualifiés de « cybersurveillance » (Bouchet, 2001), ces systèmes de contrôle électronique soulèvent de nombreux problèmes liés au respect de la vie privée dans l'entreprise. Alors que la France et les pays européens se sont dotés de législations fournissant un minimum de garanties aux salariés, les Etats-Unis ne possèdent actuellement pas de législation pour les entreprises privées. La mondialisation des économies conduit à l'affrontement de deux modèles sur cette question. Là où l'Europe préfère légiférer, les Etats-Unis préfèrent l'auto-régulation. La création d'une direction en charge du respect de la vie privée mais uniquement sur les données clients en fournit un exemple. Au-delà des réglementations, ce sont les pratiques managériales qui doivent se modifier et intégrer cette nouvelle dimension du management ou plutôt du e-management !

Bibliographie.

- Alter N., (2000), « La gestion du désordre dans l'entreprise », Nouvelle édition, L'Harmattan, 207 p., Paris
- Akerloff G., (1976), « The economics of caste and of the rat race and other woeful tales », *Quarterly Journal of Economics*, Vol. 90, November, pp. 599-617.
- Boehle S., (2000), « They're watching you », *Training*, Vol. 37, n°8, pp. 68-72.
- Bouchet H., & alii, (2001), « La cybersurveillance des salariés dans l'entreprise », Rapport d'étude et de consultation publique, Mars, 51 p., disponible sur le site www.cnil.fr
- Boyer R., Freyssenet, (2000), « Les modèles productifs », La Découverte, Paris.
- Brown S., (2000), « Ontological security, existential anxiety and workplace privacy », *Journal of Business Ethics*, Vol. 23, n°1, pp. 61-65.
- Corbin D.A., (2000), « Keeping a virtual eye on employees », *Occupational Health and Safety*, Vol. 69, n° 11, pp. 24-28.
- CIGREF, (1999), « Maîtrise d'internet », Septembre, 70 p., Paris, disponible sur le site www.cigref.fr
- CIGREF, (2000), « Impacts et usage de la messagerie électronique », Octobre, 59 p., Paris, disponible sur le site www.cigref.fr.
- Coriat B., (1990), « L'atelier et le robot. Essai sur le fordisme et la production de masse à l'âge de l'électronique », Ed. Bourgois, Paris.

- Coriat B., (1995), « Les métamorphoses de la division du travail dans la crise contemporaine : l'implication et ses modèles », in J. Bidet, J. Texier (dir.), La crise du travail, Paris, P.U.F., p.51-69.
- Foucault M., (1975), « Surveiller et punir », Gallimard, Paris.
- Henderson S.C., Snyder C.A., (1999), « Personal information privacy : implications for MIS managers », Information & Management, Vol. 36, pp. 213-220.
- Isaac H., (2000), « L'entreprise numérique enjeux et conséquences des nouveaux systèmes d'information », Revue Française de Gestion, n°129, Juillet.
- Isaac H., Mercier S., (2001), « Ethique ou déontologie : quelles différences pour quelles conséquences managériales ? L'analyse comparative de 30 codes d'éthique et de déontologie », in « Perspectives en Management stratégique », à paraître.
- Kalika M., (1995), « Structures d'entreprises », Economica.
- Kalika M., (2000), « le management est mort, vive le e-management », Revue Française de Gestion, n°129, Juillet
- Kovach A.K., Conner S.L., Livneh T., Scallan M.K., Schwartz R.L., (2000), « L'e-mail et le droit à la vie privée », in L'Expansion Management Review, n°99, décembre, pp. 72-77.
- Lallé B., (1999), « Nouvelles technologies et évolution de la problématique (contrôle/autonomie) dans le secteur des services : application au cas bancaire », Revue de Gestion des ressources Humaines, n° 32, pp.97-107, Juillet-Août.
- Laval F., (2000), « GRH et NTIC : enjeux et perspectives », Revue Française de Gestion, n°129, Juillet
- Masters M.F., Brown W.S., (1994), « Manager's workplace privacy rights : a survey of current practice », Journal of Individual Employment Rights, Vol. 2, n°2, pp. 133-151.
- Mayère A., (1999), « Les effets de l'introduction d'outils d'information et de communication mobile dans l'entreprise. », Revue Française de Gestion, Mars-Avril, pp.88-99.
- Oz E., Glass R., Behling R., (1999), « Electronic workplace monitoring : what employees think », Omega The International Journal of Management Science, Vol. 27, pp. 167-177.
- Pochet C., (1998), « A la recherche de la nouvelle productivité », Revue Française de gestion, n°, pp. 4-16.
- Polanyi K., (1983), « La grande transformation », Gallimard, 419 p., Paris.
- Rapport « Impacts et usages de la messagerie électronique », CIGREF, Octobre 2000, disponible sur le site www.cigref.fr
- Rapport « Maîtrise d'internet », CIGREF, Septembre 1999, disponible sur le site www.cigref.fr
- Marciniak R., Rowe F., « Systèmes d'Information, Dynamique et Organisations », Economica, 1997.
- Stanton J.M., E.M. Weiss, (2000), « Electronic monitoring in their own words : an exploratory study of employee's experiences with new types of surveillance », in Computers in Human Behavior, Vol. 16, pp. 423-440.
- Vaught B.C., Taylor, E.T., Vaught S.F., (2000), « The attitudes of managers regarding the electronic monitoring of employee behavior : procedural and ethical considerations », in American Business Review, January, pp. 107-114.

- 1- La fin de l'anonymat dans l'organisation et les relations marchandes.
 - a. Mutations de l'environnement et des organisations.
 - i. Transversalité et nouvelles formes de productivité
 - ii. Frontière floue, vie privée/vie professionnelle.
 - b. L'expansion des technologies de l'information dans l'organisation.
 - i. Traçabilité des actions et mesure de la performance
 - ii. Outils de mobilité et astreinte.
- 2- Les dérives potentielles des technologies de l'information et leurs conséquences.
 - a. Technologies de l'information et contrôle dans l'organisation : le panoptisme ?
 - b. La défiance dans les relations et ses conséquences.
- 3- Pour une gestion des données privées par l'entreprise.
 - a. Gestion des données relatives aux salariés.
 - b. Pour une politique de la vie privée dans l'entreprise.