Existe-t-il un droit à une vie privée dans l'entreprise à l'heure de la guerre économique ?

Frédéric Ocqueteau

EXISTE-T-IL UN DROIT À UNE VIE PRIVÉE DANS L'ENTREPRISE À L'HEURE DE LA GUERRE ÉCONOMIQUE ?

Frédéric OCQUETEAU*

* Directeur de recherche au CNRS, Centre de recherches sociologiques sur le droit et les Institutions pénales.

Avant de tenter de répondre à la question du titre, quelques préalables de cadrage sont nécessaires à qui ne serait pas nécessairement familiarisé avec les normes et les institutions françaises.

Par qui la « liberté publique » du « droit à la vie privée » à l'heure de l'invasion des technologies de sécurité dans la vie de la cité est-elle garantie ? Que signifient de tels principes dans la vie interne de l'entreprise confrontée aux mêmes défis ?

Si l'on ne veut pas en rester à la déréalisation de ces questions dont les solutions se résoudraient dans le ciel des idées, force est de repartir d'une donnée de base simple : le pouvoir de direction et de gestion du chef d'entreprise a toujours été justifié par le fait qu'il devait pouvoir s'assurer de la présence des salariés, de leurs comportements et de leur productivité dans l'unité de travail. Mais ce qui ressortait jadis de l'observation directe, visuelle ou auditive du salarié par son supérieur hiérarchique (ou de ses « agents de contrôle interne »), se pose aujourd'hui de manière beaucoup plus subtile quand l'utilisation des technologies de l'information et de la communication accompagnent le travail quotidien des salariés des entreprises industrielles et de services. Face à l'apparition de nouvelles technologies de contrôle et de protection apparemment moins oppressives dans un contexte de guerre économique entre les entreprises où l'Intelligence Économique (IE) et la veille économique deviennent des enjeux de survie, quel sens doit-on accorder aux possibles mises à mal des libertés quand circulent intensivement de l'information jusqu'à présent ouverte au sein des entreprises et dans leur environnement (concurrents, clients, salariés, etc.) ? Quels sont les nouveaux usages de « l'information » quand l'entreprise elle-même tend à se méfier de ses salariés et de ses collaborateurs, parce qu'ils ne seraient pas assez conscients des risques pris, face aux vulnérabilités de son propre patrimoine ? Comment est-elle amenée à contrôler les différents foyers de ses vulnérabilités ? Quelles implications concrètes cela a-t-il pour la vie des salariés au sein même de l'entreprise ?

Répondre à ces questions exige tout d'abord de rappeler quelques grands principes normatifs régissant la tension inhérente aux libertés octroyées aux salariés et aux impératifs des règlements intérieurs. À la suite de quoi, doit être réexaminé à nouveaux frais cet enjeu dans un

contexte de « guerre économique » entre entreprises vitales. La nécessité pour les entreprises de prévenir la survenue de nouvelles menaces et vulnérabilités liées à l'espionnage industriel, et en même temps de faire preuve de bonne conduite sous la pression d'organismes tiers ou dédiés tels que la CNIL, conduisent à renouveler de fond en comble l'examen des usages problématiques de la reconnaissance de la « vie privée » des salariés dans l'entreprise.

I. Rappel de quelques principes fondateurs des droits et devoirs dans l'entreprise

Comme nous en informe un avocat spécialisé (Forest, 2011)[1], avant d'être un travailleur salarié, l'individu est un citoyen reconnu comme doté d'une « vie privée ». Dès 1950, la Convention européenne des droits de l'Homme énonce deux principes intangibles. L'article 8-1 affirme que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». Et l'article 8-2 ajoute :

> Il ne peut y avoir d'ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

De son côté, le code civil français réaffirme solennellement dans son article 9 : « chacun a droit au respect de sa vie privée ». Et ajoute plus récemment, un alinéa 1 à ce principe : « chacun a droit au respect de la présomption d'innocence ».

Quand il est salarié dans une entreprise, le citoyen est gouverné par d'autres normes qui restreignent le principe général du droit à la vie privée ; c'est ainsi que le code du travail français affirme en son article 1121-1 :

---

1 Nombre d'éclairages suivants sont largement redevables à la science de ce spécialiste, David Forest, avocat et conseiller à la CNIL et excellent pédagogue (Forest, 2009). Voir également Ocqueteau et Ventre, 2011, p. 32-33.

> Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions *qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.*

Quant à l'alinéa 4 de l'article 1222 du même code, il ajoute ceci : « Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été préalablement porté à sa connaissance ».

Comment se présentent les arguments de la Commission nationale de l'informatique et des libertés (CNIL) au sujet de cet équilibre instable et toujours difficile à trouver, relatif à la tension réelle existant entre exigences de sécurité dans l'entreprise et respect des libertés liées à la vie privée des salariés ? Et singulièrement, au sujet des dispositifs de contrôle numériques dans l'entreprise, surveillance à distance et usages de l'Internet ?

De fait, la CNIL défend l'idée que l'Internet peut être utilisé à des fins professionnelles et à des fins personnelles sur le lieu de travail, et que tout sera affaire d'interprétations s'agissant du point d'équilibre à trouver dans un usage raisonnable de cet outil. La CNIL estime, par exemple, que si l'employeur a fixé des règles d'utilisation claires et précises, plus précises sont ces règles, plus les litiges sont aisés à solutionner en cas de non-respect des recommandations. S'agissant de la mise en œuvre de dispositifs de surveillance, elle fait prévaloir deux grands principes, en vertu de son mandat de 1978 : la proportionnalité des moyens de contrôle, d'une part, la loyauté et la transparence de l'autre.

S'agissant du principe de proportionnalité, elle estime qu'une surveillance générale et permanente des employés est contraire au principe de proportionnalité. Serait ainsi fautive une entreprise dont le système de vidéosurveillance (CCTV) placerait les salariés sous surveillance constante et permanente sous prétexte de lutter contre le vol par exemple. La CNIL a même ordonné l'interruption d'un tel dispositif qui retraçait tous les déplacements de salariés, lorsqu'ils s'absentaient de leur lieu de travail. Notons que dans sa défense du principe de proportionnalité, la CNIL estime que si les conditions dans lesquelles la mise en place de dispositifs de contrôle est acceptable dans l'ensemble le sont beaucoup moins en pratique les contrôles a posteriori de l'employeur effectués à

propos des usages de l'Internet par les employés. La CNIL aligne en général sa justification du contrôle sur la jurisprudence de la chambre sociale de la Cour de cassation. Celle-ci pose le principe selon lequel les utilisations de l'Internet dans l'entreprise sont présumées professionnelles dans un arrêt rendu le 9 février 2010 :

> mais attendu que les connexions établies par un salarié sur des sites Internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel, [...] l'employeur peut les rechercher aux fins de les identifier, hors de sa présence ; [...] que l'inscription d'un site sur la liste des favoris de l'ordinateur ne lui confère aucun caractère personnel.

Des fichiers qui auraient été créés grâce à l'outil informatique de l'employeur doivent pouvoir être consultés par le salarié, mais leur cryptage visant à rendre inopérante cette consultation constituerait une faute grave (Cass, soc., 18/10/2006).

En pratique, se pose fréquemment la question de la *nature juridique des courriels* émis sur le lieu de travail. À ce sujet, il convient d'en référer au principe de la protection du « caractère secret des correspondances » par voie de télécommunications régi par la loi du 10 juillet 1991. La position de la CNIL est la suivante : le courriel constitue une correspondance privée adressée de personne à personne (TGI, Paris, 2/11/2000) ou à des personnes liées par une communauté d'intérêt (Cass, crim, 28/4/2009). Le principe du secret des correspondances est régi par un droit pénal relativement protecteur (articles 226-15 et 432-9 du CP) qui en punit toute atteinte ou entrave comme un délit. Transposée dans l'entreprise, se pose fréquemment la question de savoir comment s'assurer qu'on ait bien affaire à une correspondance de caractère privé. De fait, la solution retenue est la suivante : l'employé doit avoir expressément protégé son courrier personnel volontairement et explicitement, faute de quoi l'employeur qui en prendrait connaissance serait présumé de bonne foi : les initiales du salarié sur le document ne suffisent pas à justifier du caractère privé de la correspondance (Cass, soc, 21/10/2009), des mentions trop peu explicites du genre « essais divers, essais divers B, essais divers restaurés » (Cass., soc, 15/12/2009), pas plus que ne le seraient une « inscription d'un site pornographique sur le liste des 'favoris' du logiciel

de navigation » de l'employé (Cass, soc. 9/2/2010). Si les courriels et les fichiers sont réputés personnels, l'employeur peut néanmoins les consulter ou se faire ouvrir le disque dur du salarié, dans au moins deux cas (Cass., soc, 17/5/2005) : quand l'employé a été convoqué en bonne et due forme, ce que doit prouver l'employeur quand bien même la convocation serait restée sans réponse ; en cas de « risque ou d'événement particulier caractérisé » (des circonstances exceptionnelles, par exemple, du même ordre que celles qui justifieraient la fouille de sac lors d'une alerte à la bombe).

S'agissant de la loyauté et de la transparence, la loyauté exige qu'ait eu lieu une consultation préalable du Comité d'entreprise sur le principe du contrôle des salariés, et qu'il en ait été clairement informé (article L. 1222-4 du C T). Une bonne illustration de ce principe s'observe dans cette jurisprudence : la loyauté a été respectée si un courriel individuel a été adressé aux salariés les alertant qu'une technique de contrôle et d'évaluation de leur activité allait être mise en place. À défaut, les preuves obtenues seraient inopposables. Quant à l'information et à la consultation préalable du Comité d'entreprise (articles L 2347 et L 2323-32 du C.T.), la nécessité s'en impose à l'employeur, car à défaut, il pourrait se voir reprocher un délit d'entrave. Ce devoir d'informer les salariés ne saurait être pris à la légère ni ressortir d'une simple formalité ; la CNIL a estimé qu'apporter un autocollant comportant le dessin d'une caméra et le mot vidéo était notoirement insuffisant pour signaler l'existence de ce type de dispositif. Voici en revanche des illustrations de décisions favorables aux employeurs : un employeur a eu raison de sanctionner un salarié pour un usage de l'outil Internet à des fins personnelles, estimant le caractère abusif de 41 heures de connexions personnelles en un mois (Cass, soc, 18/3/2009). Il a par ailleurs été jugé qu'un employeur était fondé à mettre en place des logiciels de surveillance des connections, à condition de les avoir déclarés préalablement à la CNIL, dans le droit fil d'une position de principe adoptée en 2002[2]. Elle estima en effet qu'un employeur pouvait toujours mettre en place un logiciel d'analyse poste par poste, à condition que les salariés en aient été informés, et notamment sur le point précis de la durée de conservation des données enregistrées.

---

2 Cf. CNIL, *Rapport sur la cybersurveillance dans les lieux de travail*, 5 février 2002.

* * *

Face à l'introduction des nouvelles technologies de géolocalisation et d'identification biométrique des salariés, il importe d'observer comment la CNIL a été amenée à faire évoluer sa doctrine. Elle s'est récemment efforcée d'établir quelques lignes directrices pour en encadrer la mise en œuvre. En dehors de l'adoption d'autorisations uniques portant sur des dispositifs de biométrie (par exemple l'identification des salariés par le moyen du réseau veineux à l'intérieur d'un doigt ou à l'intérieur de la paume qui ne laissent pas de trace dans une opération de contrôle d'accès aux locaux sur les lieux de travail), elle estime que toutes les autres techniques sensibles qui laissent des traces individuelles permettant des identifications nominatives exigent son autorisation sur leurs finalités réelles.

Pour la ***biométrie***, en effet, le principe de différentiation majeur établi par la CNIL est bien de savoir si la nouvelle technologie laisse ou non des traces. Elle prend des autorisations uniques (AU) quand, à ses yeux, il n'y a pas de risques de récupération et de réutilisation des données. C'est le cas dans les systèmes de reconnaissance palmaire, d'analyse d'iris ou de rétine, ou de contour de la main, ou bien encore dans le cas de technologies comportementales, par exemple la manière de signer en fonction de la pression et de la vitesse, de la frappe sur le clavier, des caractéristiques vocales, etc.). Dans les cas où il y aurait, de son point de vue, risque de traces ou de traçage (empreintes digitales générant des risques de récupération et de réutilisation), la CNIL ne les rejette pas catégoriquement, mais conformément à son mandat, elle estime qu'avant de donner son autorisation, elle a à se prononcer sur la finalité de leurs usages, les limitant au strict périmètre de la sécurisation des biens, des personnes ou de l'information de l'entreprise.

Concrètement, la CNIL a considéré que la « gestion du temps de travail » des employés n'était pas de nature à justifier le recours à la biométrie (meilleure gestion du personnel d'une mairie, délibération 2002 ; ou contrôle d'un « temps de présence »). Cette position a été confirmée par le TGI de Paris, (1e Ch. Soc., 19 avril 2005) :

> est disproportionné un dispositif de pointage du personnel par empreinte digitale du pouce contenue dans un badge, car l'amélioration

de l'établissement du temps de présence du salariés dans l'entreprise, alors qu'il existe des solutions plus communes comme le contrôle par les badges classiques, n'a pas de finalités strictement sécuritaires. (*Syndicat Sud Rail* c. *Effia Services*).

La CNIL recommande surtout que les données biométriques soient stockées sur un support individuel (badge, puce, clé USB) et non centralisées au sein d'une base de données car, à ses yeux, la centralisation présente toujours un risque de détournement accru, ce qui ne serait pas le cas des procédés sans traces.

En dépit de ces quelques garde-fous normatifs, la CNIL ne serait pas parvenue à faire entrer dans les principes juridiques légaux, un «droit à la déconnexion» des salariés à l'égard de ces technologies, ce que déplore à juste titre le juriste D. Forest dans une prise de position plus radicale en la matière (Forest, 2011).

En matière de ***géolocalisation*** (i.e. les systèmes GSM/GPS censés reconnaître à un instant *t* la position géographique satellitaire d'une personne), la protection de la vie privée du salarié et son «droit d'aller et de venir anonymement», peuvent être mis à mal. Les dérives possibles de cette nouvelle technologie n'ont pas manqué d'être considérées comme susceptibles de porter atteinte à l'exercice des droits collectifs, droit syndical ou droit de grève des salariés. La cour d'appel de Dijon (14 septembre 2010) a cependant estimé qu'un système de géolocalisation incrusté dans le véhicule professionnel d'un salarié préalablement informé, et dûment déclaré à la CNIL, valait preuve suffisante de son introduction.

Sur le plan des principes plus généraux, la doctrine de la CNIL consiste à défendre les principes suivants : un système de géolocalisation ne doit pas conduire à un contrôle permanent du salarié, car ses finalités ne doivent ressortir que d'un impératif de sécurité-sûreté ou dans un but de meilleur suivi pour la facturation d'une prestation.

La simple information préalable du personnel – qui reste finalement le seul devoir de l'employeur – au sujet de la mobilisation de ces nouvelles technologies de contrôle dans les entreprises, a pu paraître à certains une avancée d'adaptation. Dans la grande majorité des cas, elles sont plutôt considérées par les sciences humaines comme de nouvelles

atteintes aux droits fondamentaux de la personne humaine, et notamment à sa vie privée (Strugala, 2011). Non pas tant parce que les salariés seraient obligés de les subir contre leur gré, mais parce que, fondamentalement, la recherche de leur adhésion ou consentement préalables resterait une obligation très relative. Dans un contexte de bluff technologique, les nouvelles technologies prennent une apparence libératoire et progressiste, bien plus souvent qu'une allure potentiellement liberticide. Il reste assez difficile d'y résister.

Car en dépit des idéologies technologistes de prétendue libération et facilitation de la vie, l'instrumentalisation professionnelle de l'humain apparaît de plus en plus insidieuse en prenant des chemins de justifications de plus en plus raffinés (Deharo, 2011). Alors que les usages réels demeurent le plus souvent opaques aux salariés, nombreuses restent les exploitations clandestines des informations personnelles virtuellement collectées à leur insu. Et ces phénomènes tendent à s'accentuer dans un contexte plus général de « guerre économique » entre les entreprises.

II. Les grands principes face au réalisme de la « guerre économique »

La protection des « informations sensibles » dans l'entreprise justifierait-elle d'attenter un peu plus à la vie privée des employés et salariés ? C'est poser l'ancienne question de la nature des « échanges d'informations » entre privé et public (Ocqueteau, 2005), et leur composante normative, sombre ou claire, légitime ou illégitime, celle du passage très ténu de la frontière entre « espionnage industriel » et « intelligence économique ». L'acuité de cet enjeu exige de repenser la maîtrise du secret et de l'information dans un contexte de « guerre économique » très à la mode aujourd'hui (Vuillerme, 2011), voire de la « cyberguerre » au sein desquelles nos sociétés surdéveloppées seraient plongées (Ocqueteau, Ventre, 2011).

Après avoir rappelé quelques généralités contextuelles (1), nous expliquerons les efforts de certains *think tanks* français pour démarquer symboliquement la démarche de « l'intelligence économique », concept vertueux, de celle de « l'espionnage industriel » ayant de tout temps prédisposé l'entreprise à traquer des ennemis hostiles parmi ses salariés

mêmes (2). Nous diagnostiquerons enfin les modalités par lesquelles l'ordre de « l'entreprise sensible », dans le nouveau cadre d'une problématique dite de la « sécurité globale », tend progressivement à se militariser aujourd'hui (3), ce qui redessine l'enjeu de la défense de quelle vie privée des salariés.

(1) Au tournant des années 1990, la chute du mur de Berlin et l'effondrement de l'empire soviétique semblaient ouvrir de nouvelles perspectives à l'humanité. Les deux grands blocs autour desquels l'histoire du monde s'était organisée depuis la fin de la Seconde Guerre mondiale cédaient leur place à un environnement global, à la mondialisation de l'économie et des échanges. Cette mondialisation et les rêves de croissance qu'elle portait en elle s'appuyaient sur les nouvelles autoroutes de l'information, gages d'un monde ouvert, sans contraintes. Mais la mondialisation était aussi le lieu de la course à la domination, qu'il s'agisse de la conquérir ou de la préserver. Le cyberespace portait donc en lui les germes du conflit : dominer grâce au cyberespace signifiait aussi chercher à écarter les adversaires de cette course à la domination.

Le cyberespace est ainsi devenu un nouvel espace d'affrontements. De fait, la masse de données produites dans le monde est devenue une source de renseignements inépuisable que savent exploiter les États mais aussi les acteurs non étatiques. S'observer, s'espionner est la règle.

Mais si un État tire profit de ces ressources nouvelles, il est aussi l'objet d'attaques de la part d'autres États et acteurs non étatiques, adversaires et alliés. Les cyberattaques, à l'image de celles qui ont touché le ministère des Finances français au début de l'année 2011, sont symptomatiques de ce nouveau contexte qui voit se multiplier les intrusions à des fins d'espionnage dans les systèmes d'information des États et des entreprises vitales et sensibles. Les États se voient contraints à prendre des mesures strictes de sécurisation de leurs propres systèmes d'information. Mais l'approche est nécessairement plus large qu'elle ne l'était naguère : il leur faut veiller à la défense des intérêts économiques, du patrimoine scientifique, des échanges diplomatiques, de la culture même. En France, une récente agence l'ANSSI (Agence nationale de la sécurité des systèmes d'information) fut créée en 2009, dans le prolongement des

recommandations du Livre Blanc de 2008[3]. L'une de ses missions essentielles est de protéger la France contre les cyberattaques qui pourraient mettre en péril les « intérêts de la Nation » et du « patrimoine industriel national ». S'ensuivent des efforts rhétoriques quasi pathétiques pour distinguer la symbolique des nouvelles frontières de « l'espionnage industriel » du champ de « l'intelligence économique ».

(2) Les efforts pour distinguer le vice de l'espionnage industriel de la vertu de l'intelligence économique sont évidemment liés à l'image calamiteuse laissée par l'histoire des ravages de l'espionnage industriel inhérent à l'apparition des polices privées à la solde des magnats de l'entreprise industrielle (Kalifa, 2000 ; Ocqueteau, 1997). Cette pratique est aujourd'hui le repoussoir des actions sur lesquelles raisonnent les défenseurs de l'intelligence économique qui entendent prendre leurs distances avec des procédés scabreux à proscrire avec la dernière énergie : ce que l'on fait quand on entre dans l'illégalité, par exemple, en procédant à des écoutes téléphoniques sauvages, quand on cherche à corrompre, à établir des faux et usage de faux ou quand on cherche à bénéficier de l'information fermée, alors qu'il serait si aisé de rester parfaitement dans les clous de la légalité en recherchant de l'information ouverte, axée sur les interrogations de la presse, en fouillant dans les innombrables banques de données disponibles, dans les interviews et les contacts professionnels (Rouach, 2010).

Les méthodes d'espionnage offensives immorales et illégales pour épier les adversaires ou les concurrents ont pourtant toujours été légions et sont connues de très longue date : acheter des poubelles, infiltrer des taupes, soudoyer des salariés, s'introduire discrètement dans les locaux, placer des micros ou des écoutes téléphoniques, des capteurs de vibrations, etc., ont-elles vraiment disparu du paysage ?

L'intelligence économique prétend s'en distancier, en conciliant protection de l'entreprise par le biais de comportements légaux et moraux, et exercice d'une veille ou vigilance constantes pour prévenir de possibles hémorragies de matière grise au sein d'entreprises de plus en plus sou-

---

3 *Défense et sécurité nationale. Le Livre blanc*, préface de Nicolas Sarkozy, vol. 1 et 2, Paris, Odile Jacob/La Documentation française, 2008.

vent dématérialisées. Il s'agit de prévenir toute occasion d'un vol de documents, d'un vol informatique, de pratiques cybercriminelles, telles les transmissions de virus par des hackers extérieurs, de suspecter l'espionnage possible de stagiaires étrangers, de contrer intrusions sous formes diverses, écoutes téléphoniques et interceptions de fax, faux partenariats et systèmes de cheval de Troie (infiltrations avec alibi), faux recrutements, débauchages chez les concurrents, mais par-dessus tout, la négligence coupable des employés. L'imaginaire de la conjuration des « nouvelles menaces » attentant au « patrimoine informationnel » de l'entreprise, à sa marque et à sa réputation est débridé (Juillet, Vuillerme, 2011).

On voit par là comment une conception hautement victimaire de la vulnérabilité de l'entreprise justifie sa mise en protection tous azimuts contre des menaces extérieures (Ocqueteau, 2011) et internes, quand bien même cela ne dit rien des stratégies offensives destinées à garder un avantage concurrentiel sur des compétiteurs d'importance analogue. Au fond, les puissants lobbies de l'IE se donnent pour mission de convertir les pouvoirs publics à l'idée de n'avoir rien de commun avec les pratiques d'espionnage ancestrales des concurrents dont ils seraient les victimes désarmées, vu qu'ils ne pratiqueraient de leur côté que de la capture d'informations licites, quitte à la prélever chez leurs meilleurs ennemis, c'est-à-dire leurs concurrents directs[4].

Pour ce qui est de la stratégie d'anoblissement de l'image de l'IE et de la veille technologique, un petit retour en arrière au sujet de ce nouveau référentiel d'action dans le contexte franco-français est sans doute nécessaire, car il est intraduisible (et peut-être intransposable) dans le monde anglo-saxon. De quoi s'agit-il au juste ? L'IE peut être définie comme l'ensemble des actions de recherche, de traitement, de diffusion

4 Il serait sans doute fort utile de méditer ce passage toujours d'actualité dans le monde de l'entreprise d'aujourd'hui issu du roman d'Umberto Eco : « Certains grognent contre la fusion de l'espionnage et du contre-espionnage, mais les deux activités sont strictement liées. Il faut savoir ce qui arrive à l'ambassade d'Allemagne, parce que c'est un territoire étranger et ça, c'est de l'espionnage, mais c'est là qu'on recueille des informations sur nous, et le savoir c'est du contre-espionnage » (Eco, 2011, p. 450)

et de protection de l'information utile aux différents acteurs économiques. Ces actions sont pensées comme :

> un système global destiné à inspirer la stratégie de la direction générale de l'entreprise à informer en continu, et innerver ses différents niveaux d'exécution, afin de créer une gestion offensive et collective de l'information, qui devient une richesse principale. (Martre et al, 1994)

De la sorte conçue, l'IE justifie une veille technologique sans relâche, elle-même définie comme :

> l'ensemble des techniques visant à organiser de façon systématique la collecte, l'analyse, la diffusion de l'exploitation des informations techniques utiles à la sauvegarde et à la croissance de l'entreprise. (Rouach, 2010)

L'information relève des différents services de l'entreprise, finance, production, vente, marketing et s'exerce selon deux modalités principales : un recueil plutôt passif de l'information (veille par scanning, monitoring) et un recueil plutôt actif (renseignement, reconnaissance). La veille active est nécessairement incarnée par des veilleurs, des guetteurs ou des chasseurs, (les dormeurs étant généralement exclus du panorama, vu qu'ils jugent la veille inutile et ne craignent pas la concurrence).

Le spécialiste D. Rouach distingue les veilleurs réactifs, les veilleurs actifs, les veilleurs offensifs et les guerriers. Il estime qu'une veille offensive très active aurait lieu dans les domaines très concurrentiels, où se concentreraient de nombreux spécialistes du renseignement militaire se reconvertissant comme des veilleurs professionnels dans le civil, (*id.*, p. 30). Cette activité, décrite comme noble et parfaitement légale, se résumerait en sept missions principales : élaboration et suivi des réseaux ; repérage des sources d'information ; élaboration de fiches de renseignements, de Q/R adaptées à des demandes précises ; suivi de la qualité des informations ; contrôle des infos stratégiques ; diffusion des informations, et gestion d'un budget veille. Elle exigerait trois qualités : communication/optimisme ; vigilance et non quiétude ; esprit critique et perfectionnisme.

Mais comment expliquer que pareilles compétences aillent très souvent de pair en France avec le recrutement d'agents aux éthos professionnels militaires ?

(3) Le recours bien compris aux compétences militaires dans le domaine de « l'intelligence économique » ne va pas de soi. D'autres facteurs, pas nécessairement liés à l'apparition de « nouvelles menaces », expliquent la militarisation progressive de l'ordre dans les entreprises sensibles et vulnérables. Qu'en est-il d'abord du champ concrètement couvert ? Une enquête récente de l'ASIS-France estime à 70 % le nombre des militaires reconvertis dans les directions de sécurité des grandes entreprises françaises[5]. Parmi les interrogés de ses adhérents, 67 % des cadres exerceraient dans une entreprise prestataire de services et 27 % dans une direction de sécurité d'entreprise. Par ailleurs, 77 % appartiendraient à des forces armées (anciens militaires, gendarmes, sapeurs-pompiers à statut militaire) ; 9 % des directeurs seraient d'anciens fonctionnaires de police et 14 % seraient issus du monde civil. Semblable constat n'a pas manqué de nous étonner dans une étude personnelle dédiée aux managers de la sécurité-sûreté dans 25 grandes entreprises françaises à rayonnement international (Ocqueteau, 2011). Nous y avons pareillement constaté que la présence d'anciens cadres de la police ou de hauts fonctionnaires du ministère de l'Intérieur dans les entreprises réputées « non vitales » constituait un cas de figure rare. En revanche, nous avons observé dans le « staff » de la direction de sûreté de l'entreprise ou de l'établissement public, la présence quasi automatique d'un numéro 2, bras droit militaire ou gendarme accompagnant le titulaire du poste, cadre civil ou policier détaché temporaire. Pourquoi donc les directions des grandes entreprises ont-elles ce réflexe si facile, au moins en France, de recourir aux militaires dans leurs directions de sûreté, alors qu'ils sont, à tort ou à raison, du point de vue des salariés, réputés les moins souples dans la gestion des risques polymorphes vécus dans l'entreprise ? Trois éléments de réponses cumulatifs peuvent être apportés à cette question.

---

5 *Source* : AISG.org, 20/09/2011 – Baromètre d'ASIS France sur les fonctions de sécurité et de sûreté privée.

Deux d'entre eux résident dans un mécanisme d'offre de reconversion en phase avec une demande incertaine. Ce n'est pas tant la présence caricaturale des généraux «cinq étoiles», pantouflards de jadis, qui emporte désormais l'explication, que le besoin de mobiliser des personnels aguerris généralement plus jeunes que leurs collègues policiers. L'âge des départs à la retraite des militaires de la Défense est en effet l'un des plus précoces parmi tous les autres fonctionnaires. Il s'ensuit que si les valeurs d'ordre, de maîtrise de soi et de loyauté, qui font la spécificité de leur ethos sont *a priori* très appréciées des employeurs, c'est une ressource supplémentaire qui conforte un calcul implicite de l'entreprise jouant de cette jeunesse relative comme d'un gage de souplesse et d'adaptation futures. On pense que ces fonctionnaires seront mieux capables de se plier ou de se former à la gestion du (dés)ordre interne de l'entreprise, même s'ils n'y sont pas bien préparés. Si l'on présume qu'ils ne disposent sans doute pas tous d'un capital de ressources relationnelles aussi étoffé que leurs homologues conceptuels de l'encadrement policier, les employeurs les créditent en général de mieux savoir que d'autres comment collecter du renseignement stratégique aux meilleures sources et au bon moment. Or, dans une conjoncture dangereuse où de grandes entreprises sensibles doivent apporter la preuve de leur conformité aux attentes de la mise en sécurité globale prêchées par les États-nations face à des risques majeurs, quelle meilleure facilité pour l'entreprise que de pouvoir ainsi attester de ces gestes de bonne volonté ?

Cette demande rencontre par ailleurs une offre de plus en plus offensive : les militaires et gendarmes en voie de reconversion ont appris à s'organiser bien plus rapidement que ne l'ont fait des policiers plus individualistes, par le biais du recours à des associations dédiées à l'apprentissage des techniques de reconversion, les retours d'expériences et des incitations de leur ancien ministère de tutelle[6], recyclant abondamment dans les entreprises concluant d'importants marchés d'armement avec lui.

---

6 Un arrêté du 10 juin 2009 du ministère de la Défense a même doublé les ardeurs de ces associations en créant une agence d'aide à la reconversion de ses fonctionnaires, dite «Défense Mobilité».

Une troisième raison plus fondamentale tient à ce que de tels phénomènes émergent dans le contexte d'une militarisation des appareils de police occidentaux (Lemieux, Dupont, 2005). Cette tendance a été bien documentée dans le domaine du contrôle des foules, du renseignement ou de l'information de sécurité, et dans les sphères d'éclatement des espaces de souveraineté traditionnels, qui ont vu monter une offre de sécurité commerciale globale parallèlement au développement d'entreprises à implantations mondiales (Johnston, 2005). Or, on s'est sans doute trop attaché à ce sujet à l'étude de l'externalisation des savoir-faire militaires et à leurs reconversions au sein de sociétés militaires privées, auraient-elles pour vocation principale à accomplir des opérations de maintien de la paix. Mais nous avons peut-être oublié, en France du moins, des phénomènes plus discrets liés à l'internalisation de la « culture militaire du risque et des dangers » au sein des grandes entreprises. Si l'attrait pour importer une culture militaire dans l'entreprise est devenu si puissant, il pourrait bien s'expliquer en définitive par une représentation devenue dominante. Les militaires apporteraient une présence rassurante, étant dotés de pouvoirs surnaturels quant à la maîtrise et à la conjuration des incertitudes liées à une perte progressive de rationalité stratégique dans des entreprises plongées dans des environnements complexes, dangereux et quasiment immaîtrisables.

III. Remarques conclusives

Que l'incertitude soit ou non rationnellement conjurée par les chocs engendrés par les crises répétitives du capitalisme financier ou des catastrophes majeures, que le chaos ne soit pas nécessairement à la porte de nos démocraties engagées dans des pratiques de sécurisation globale, la vigilance de tous exige néanmoins de savoir rester en éveil.

Les directeurs de sûreté des entreprises véhiculent des systèmes de valeurs composites (Ocqueteau, 2011) qui sont encore le meilleur garant d'un style de management non unifié. Elles sont la garantie d'une possibilité de transparence à l'égard des collectifs des salariés au travail. Si la hantise de l'espionnage industriel et la défense du patrimoine restent une obsession commune aux sommets de l'État et de ses « fleurons industriels », alors que les dispositifs de mise en protection internes de l'infor-

mation sont censés devenir de plus en plus transparents, tel n'est pas le phénomène majeur auquel on assiste. On voit plutôt de puissants lobbies se presser auprès des pouvoirs publics pour obtenir de l'État de partager avec lui une part de ses secrets pour peu qu'ils concernent leur domaine sensible ? L'objectif serait d'opposer à la justice une norme de « Secret des affaires » analogue au référentiel du « Secret Défense » ou du « Confidentiel Défense », prérogatives souveraines consenties à la haute police de l'État (Ocqueteau, 2012).

À cet effet, une nouvelle incrimination vient de faire son entrée au sein du Code pénal, dans la foulée de la proposition du député B. Carayon (Carayon, 2011), qui pénalise toute « atteinte au secret des affaires », en la justifiant comme riposte en légitime défense (Bolle, 2011) à toute attaque extérieure ou intérieure susceptible de mettre l'existence même de l'entreprise en péril. Les dirigeants d'une entreprise « sensible » sont désormais assurés de définir par eux-mêmes unilatéralement le périmètre des informations sensibles qu'ils vont juger utile de soustraire au regard des salariés et des concurrents s'avisant de les faire fuiter… La sanction encourue serait de 3 ans d'emprisonnement et 375 000 euros d'amende. Or, le caractère très élastique (juridique, financier, commercial, économique, industriel, scientifique et technique) de ces informations dites « à caractère économique protégé » ne laisse pas d'inquiéter pour la transparence de « l'information » capable d'aisément se retourner contre les salariés eux-mêmes. Leur désignation relèverait en effet de la seule responsabilité des dirigeants de l'entreprise. N'est-ce pas vouloir en définitive obscurcir la mise à jour des pratiques douteuses des directions ? La défense du « secret des affaires » ne deviendrait-elle pas la justification la plus menaçante pour le reste des libertés conquises par les salariés sous un État-providence s'effaçant progressivement, laissant la place à un état de « guerre économique » où tous les coups étant permis, les salariés ne seraient plus contraints qu'à une *omertá* totalement paralysante… s'ils entendent encore travailler ?

Ne serions-nous pas alors déjà confrontés au plus grand démenti possible à la prétendue « démocratie d'entreprise » de naguère ? Et plus fondamentalement, ne serions-nous pas en train de nous préparer à la pire des sociétés de défiance et de soupçon qui soient ?

BIBLIOGRAPHIE

BOLLE, P.-H., «La légitime défense en affaires», (2011) 8 *Sécurité et Stratégie*.

CARAYON, B., «Protéger le secret des affaires : un enjeu national», (2011) 8 *Sécurité et Stratégie*.

DEHARO G., «L'identification biométrique dans l'entreprise», dans A. CEYHAN, P. PIAZZA, *L'identification biométrique, champs, acteurs, enjeux et controverses*, Paris, éd. MSH, 2011, p. 143-160.

ÉCO, U., *Le cimetière de Prague*, Paris, Grasset, 2011.

FOREST, D., *Abécédaire de la société de surveillance*, Paris, Syllepse, 2009.

FOREST, D., *Droit des données personnelles*, Paris, Galino Lextenso, 2011.

JOHNSTON, L., «Le *policing* privé transnational : l'impact de la sécurité commerciale globale», dans F. LEMIEUX, B. DUPONT, (dir.), *La militarisation des appareils policiers*, Québec, Presses de l'Université Laval, 2005, p. 217-240.

JUILLET, P., J.-P. VUILLERME, «L'entreprise face aux fuites d'informations», (2011) 5 *Sécurité et Stratégie*, p. 17-26.

KALIFA, D., *Naissance de la police privée*, Paris, Hachette, 2000.

LEMIEUX, F., B. DUPONT (dir.), *La militarisation des appareils policiers*, Québec, Presses de l'Univiversité Laval, 2005.

MARTRE, H., P. CLERC, C. HARBULOT, *Intelligence économique et stratégie des entreprises*, Commissariat général au plan, Paris, La documentation française, 1994.

OCQUETEAU, F., *Les défis de la sécurité privée*, Paris, L'Harmattan, 1997.

OCQUETEAU, F., «La collaboration policière, confiance et défiance dans le partage de l'information policière», dans J.-P. BRODEUR, F. JOBARD (dir.), *Citoyens et délateurs, la délation peut-elle être civique ?*, Paris, *Autrement*, n° 238, 2005, p. 88-104.

OCQUETEAU, F., «Chefs d'orchestre de la sûreté des entreprises à l'ère de la sécurité globale», (2011) 8 *Champ Pénal/Penal Field,* Varia. En ligne: <http://champpenal.revues.org/8142>.

OCQUETEAU, F., «Privatisation de la haute police: comment en explorer l'hypothèse?», (2012) 9 *Champ Penal/Penal Field*, dossier «Hommages à Jean-Paul Brodeur», à paraître.

OCQUETEAU, F., D. VENTRE, (dir.), «Contrôles et surveillances dans le cyberespace», (2011) 988 *Problèmes politiques et sociaux*, Paris, La documentation française.

ROUACH, D., *La veille technologique et l'intelligence économique*, Paris, PUF, QSJ, nº 3086, 2010.

STRUGALA, C., «Développement de la biométrie et droit au respect de la vie privée: un droit lacunaire?», dans A. CEYHAN, P. PIAZZA (dir.), *L'identification biométrique, champs, acteurs, enjeux et controverses*, Paris, éd. MSH, 2011, p. 275-302.

VUILLERME, J.-P., «L'entreprise en guerre économique?», (2011) 8 *Sécurité et Stratégie.*