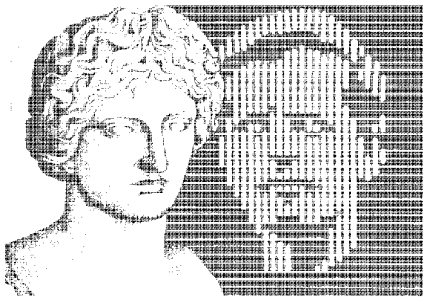

RAPPORT D'ÉTUDE ET DE CONSULTATION PUBLIQUE

LA CYBERSURVEILLANCE DES SALARIES DANS L'ENTREPRISE

M. Hubert BOUCHET, vice-président délégué de la CNIL

Mars 2001

Rédacteurs : Mme Sandrine MATHON, attachée à la direction juridique
M. Jean-Paul MACKER, chargé de mission à la direction de l'expertise informatique
Mme Sophie NERBONNE, chef de service
M. Roger N'GO, directeur informatique et M.. Joël BOYER, secrétaire général, affaires juridiques
Avec la complicité active de Mme Brigitte HUGER, assistante à la direction juridique

SOMMAIRE

RAPPORT D'ÉTUDE ET DE CONSULTATION PUBLIQUE

LA CYBERSURVEILLANCE DES SALARIES DANS L'ENTREPRISE ET LOI "INFORMATIQUE ET LIBERTES":

Dans son rapport "Les libertés publiques et l'emploi" [1], le professeur Gérard Lyon-Caen rappelait que le débat sur la vie privée du salarié au sein de l'entreprise qui met en cause tout à la fois le lien de subordination qui caractérise le contrat de travail et la part irréductible de liberté des hommes et des femmes dans une société démocratique, n'était pas nouveau. Il soulignait cependant que le développement des moyens de contrôle technique lié aux nouvelles technologies nécessitaient de le revisiter. "*La ligne de partage [entre lien de subordination et vie privée] ne saurait plus être tracée à la sortie des lieux de travail et à l'expiration de l'horaire. Tout est devenu plus complexe et plus flou*". L'auteur du rapport évoquait un "*nouvel* espace police, *véritable ordre technologique qui n'a plus rien de commun avec l'ancienne subordination car le salarié n'est plus sous les ordres de quelqu'un. Il est surveillé par la machine, à la limite par lui-même, par tous et par personne*". S'agissant des messageries électroniques, le professeur Lyon-Caen annonçait : "*le strict respect des correspondances a vécu dans ce domaine*". Nous étions en 1991...

La surveillance cantonnée par le droit

A la suite de ce rapport, la loi du 31 décembre 1992 a posé les jalons d'un droit "informatique et libertés" dans l'entreprise. Principe de proportionnalité ("*nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas proportionnées au but recherché*" - art L 120-2 du code du travail) ; consultation du comité d'entreprise lors de l'introduction de nouvelles technologies (art L 432-2) ; information préalable des salariés (art L 121-8).

Ces principes et droits font écho à la loi du 6 janvier 1978 qui impose que tout traitement de données personnelles soit déclaré à la CNIL, que les salariés soient informés de son existence et de ses caractéristiques et qu'ils aient accès aux informations les concernant.

---

[1] *Rapport pour le ministre du travail, de l'emploi et de la formation professionnelle, décembre 1991, Document française*.

C'est sur la base de ces principes que, dès 1984, la Commission a établi, par le biais d'une recommandation qui devait trouver son prolongement dans une norme simplifiée, des règles d'usage des autocommutateurs téléphoniques qui permettent à l'employeur de connaître les numéros de téléphone appelés par un salarié depuis son poste [2].

Ces mêmes principes trouvent application en matière de vidéo-surveillance dans l'entreprise et la chambre sociale de la Cour de cassation donnera sa substance à ces principes : nul moyen de preuve ne peut être opposé par l'employeur aux salariés si le dispositif de contrôle a été mis en oeuvre à leur insu.

Mais jusqu'à présent, qu'il s'agisse d'autocommutateur téléphonique, de badges et de contrôle d'accès ou de vidéo-surveillance, la surveillance concernait principalement la présence ou la localisation physique de l'individu. En un mot, les technologies demeuraient encore à la périphérie du processus de travail.

Sans doute, le développement des écoutes téléphoniques dans le milieu du travail a-t-il signé un changement. La multiplication des services par téléphone et des centres d'appels a conduit les entreprises à surveiller la qualité du service, c'est-à-dire celle de la réponse apportée par le salarié. Sur ce point, la CNIL a développé un corpus de recommandations pratiques qui paraît être très largement respecté.

Cependant, avec l'émergence des nouvelles technologies de communication et tout particulièrement l'introduction d'internet dans l'entreprise, c'est une véritable migration des technologies de contrôle de la périphérie jusqu'au coeur du processus de travail proprement dit qui s'opère.

La cybersurveillance au coeur du processus de travail

Le recours de plus en plus systématique aux nouvelles technologies de réseau a des incidences considérables sur le rapport salarial.

Progressivement, l'information dont disposent les entreprises est numérisée, quelque soit la nature de cette information. Dès lors qu'elle est informatisée et susceptible d'accès par internet ou intranet, des risques d'accès indus à cette information sont réels. Pour l'entreprise, les nouvelles technologies de l'information et de la communication vont naturellement poser des problèmes nouveaux en matière de sécurité dès lors que se trouvent externalisées des informations sur toute la vie de l'entreprise, ses fichiers de personnels, la gestion des commandes, ses secrets de fabrique, etc. Pour les salariés, la différence de nature entre les NTIC et tout ce qui précède réside en la capacité nouvelle de la technologie de conserver toutes les traces laissées par la personne connectée.

---

[2] *cf. 5 ème rapport d'activité de la CNIL, 15 ème rapport d'activité, p 74.*

Ainsi, la technique pose de façon nouvelle des questions qui avaient été réglées dans un contexte ancien. Un message électronique que le salarié a cru supprimer peut avoir été sauvegardé sur un serveur de messagerie ou sur un support magnétique de sauvegarde. Et ce salarié serait abusé si nul ne lui avait exposé que le message qu'il avait reçu de son épouse pour lui rappeler de ne pas oublier de faire une course avant de rentrer à son domicile, et qu'il avait aussitôt effacé de sa messagerie, avait été conservé à son insu.

L'équilibre est délicat à trouver.

L'ouverture de l'entreprise sur le monde, grâce à internet, et l'utilisation des réseaux d'information, la rendent plus vulnérable à des attaques informatiques venues de l'extérieur. La mise en place de mesures de sécurité constitue à cet égard une nécessité pour éviter les intrusions et pour protéger des documents confidentiels, des secrets de fabrique, ou encore les fichiers de l'entreprise. Or, ces mesures de sécurité auront précisément pour objet de conserver trace des flux d'informations, directement ou indirectement nominatives, afin de mieux prévenir les risques et de repérer l'origine des problèmes.

Par ailleurs, ces technologies qui sont tout à la fois, ergonomiques, faciles d'emploi et parfois ludiques, peuvent conduire les entreprises à veiller à ce que leurs salariés n'en fassent pas un usage abusif, sans lien avec leur activité professionnelle. Ce contrôle de productivité du "cyber-travailleur" s'exercera d'autant plus que toute architecture en réseau a pour effet d'éloigner géographiquement le salarié de sa hiérarchie.

L'évolution aura été constante. D'abord, le contremaître, personne repérable, chargé de contrôler la présence physique du salarié sur son lieu de travail et en activité. Puis, les "contremaîtres électroniques" chargés du contrôle de la présence physique : les badges d'accès. S'ouvre désormais l'ère du "contremaître virtuel" pouvant tout exploiter sans que le salarié en ait toujours parfaitement conscience et permettant, le cas échéant, au-delà des légitimes contrôles de sécurité et de productivité des salariés, d'établir le profil professionnel, intellectuel ou psychologique du salarié "virtuel".

Des entreprises de plus en plus nombreuses adoptent des chartes d'information précisant les mesures de sécurité à prendre et les usages qu'il peut être fait par les salariés des nouveaux outils informatiques mis à leur disposition. L'examen de ces chartes qui sont très rarement négociées avec les représentants du personnel ou leurs syndicats, manifeste un déséquilibre patent entre les prérogatives de l'employeur et les droits des salariés.

C'est ainsi que la plupart des chartes dont la CNIL a eu à connaître prévoient que l'ensemble des données de connexions qui peuvent révéler à l'administrateur du système, ou au chef de service, ou au directeur de personnel, l'usage qui est fait de l'outil (les sites qui ont été consultés, les messages qui ont été adressés) sont conservées pendant des durées très longues et font l'objet d'analyses individualisées.

De la même façon, les salariés sont le plus souvent contraints par ces chartes à n'utiliser le courrier électronique qu'à des fins exclusivement professionnelles, certaines sociétés, notamment des filiales de groupes américains, précisant même que tout message électronique envoyé par un salarié doit être considéré comme un "enregistrement permanent, écrit, pouvant à tout moment être contrôlé et inspecté" (sic).

Cependant, les salariés demeurent encore largement ignorants des possibilités de traçage que les nouvelles technologies offrent à l'employeur et, de fait, l'équilibre nécessaire entre contrôle légitime exercé par l'entreprise et respect des droits des salariés ne paraît pas assuré dans bien des cas.

*

Cet état des lieux a conduit la CNIL à entreprendre une étude d'ensemble de ces questions dans le souci de suggérer aux entreprises et aux salariés utilisateurs l'adoption d'une règle du jeu équilibrée, comme les autorités de protection des données l'ont fait lors de l'apparition des précédentes technologies : badges, autocommutateurs, vidéosurveillance, etc.

Le projet de la Commission est d'abord une méthode : consultation d'experts informatiques et tout particulièrement d'experts en réseau, consultation des syndicats de salariés, contact avec celles des entreprises qui ont déjà élaboré des chartes d'usage des intranets.

La CNIL a ainsi rencontré le chargé de la sécurité informatique des Aéroports de Paris, le responsable de la sécurité informatique de Thomson Multimédia, le délégué à la sécurité des systèmes d'information du CNES (centre national d'études spatiales). Elle a participé aux groupes de travail d'entreprises mettant en oeuvre ces technologies comme Thalès ou EADS et a consulté les organisations syndicales des salariés (CGT, CFDT, FO, CFTC et CGC) et patronales (MEDEF et CGPME). Elle a eu également à connaître une cinquantaine de chartes "informatiques et libertés" adoptées par les entreprises qui ont sollicité son avis ou son conseil.

C'est sur la base de cette matière que la CNIL a élaboré le présent rapport autour duquel elle souhaite que s'engage un débat entre entreprises et salariés, responsables informatiques et juristes, instances représentatives et organisations professionnelles.

Cette initiative porte la marque d'une conviction : celle que l'entrée de nos pays dotés d'une législation de protection des données dans la société de l'information ne saurait se faire sans les utilisateurs de ces nouveaux outils, ni si ces outils suscitent la méfiance des salariés.

Quatre questions doivent nourrir la réflexion :

1. En quoi les technologies en réseau seraient-elles de nature différente que les précédents outils mis en place dans les entreprises ?

2. Quelle est la part de la vie privée et des libertés individuelles garantie aux salariés qui sont liés à l'employeur par un contrat de travail qui est d'abord lien de subordination ?

3. Quel usage à des fins privées d'outils mis à la disposition des salariés par leur employeur est-il admis ?

4. Y a-t-il des limites au contrôle et à la surveillance que les employeurs peuvent exercer sur les salariés ?

Toutes ces questions ne relèvent évidemment pas de la seule compétence de la Commission nationale de l'informatique et des libertés. Mais, imbriquées les unes aux autres, elles constituent naturellement, prises ensemble, un champ de préoccupations communes aux employeurs et aux salariés à l'heure de la société d'information. La CNIL souhaite, par ce rapport d'ensemble, offrir divers éclairages que son expertise autorise : aspects techniques, rappel du droit, panorama jurisprudentiel, étude des pratiques comparées et, au titre des questions encore à débattre, quelques recommandations pratiques.

Des technologies et des traces

Le traçage est inhérent à l'informatique

Certaines applications ont, par nature, vocation à fournir à l'entreprise, par traçage informatique, le moyen de prouver la réception des ordres envoyés par la clientèle, l'accomplissement d'une prestation ou l'exécution d'une procédure.

Dans de nombreux cas, l'application informatique n'est qu'un système de traçage à l'état pur, se surajoutant en quelque sorte à une opération manuelle ou intellectuelle. Le traçage informatique vient en renfort dans le seul but de noter tous les gestes exécutés, les décisions prises, afin de permettre la vérification ou d'apporter la preuve que tout a été exécuté selon les règles : le contrôle aérien, les manœuvres sensibles dans les centrales nucléaires, le suivi d'une chaîne de production dans un atelier...

Ce traçage trouve sa légitimité dans le fait qu'il est destiné à conserver la mémoire de l'exécution des tâches accomplies. Il participe la plupart du temps d'une "démarche qualité".

C'est aussi ce traçage qui constitue une des meilleures mesures de sécurité des fichiers informatiques, sous l'appellation de système de "journalisation". Qui a consulté quoi ? A quel moment ? Qui a procédé à la modification de telle information enregistrée dans un fichier ?

Les logiciels de gestion du travail de groupe (Work-flow)

A travers ces logiciels, une entreprise automatise la circulation des documents par modélisation de ses procédures de travail. Elle pourra contrôler et suivre en temps réel l'état d'avancement des dossiers, mesurer et optimiser les coûts.

En début de chaîne (par exemple le service du courrier), un premier utilisateur-aiguilleur a la responsabilité de sélectionner la catégorie de traitement que devra suivre chaque nouvelle "tâche" générée par l'arrivée d'un nouveau document dans l'entreprise. Ce choix conditionne l'envoi des documents vers les corbeilles (boîtes aux lettres électroniques) des premiers destinataires.

Chaque utilisateur peut choisir de traiter immédiatement une tâche ou de la mettre en attente dans

une autre corbeille. A la fin d'une tâche, le logiciel de work-flow gère automatiquement le "routage", c'est-à-dire la détermination de l'utilisateur suivant dans la procédure de traitement. En cas d'absence de la personne habilitée, le logiciel routera automatiquement le document vers un tiers. Si une personne oublie de consulter sa corbeille, le logiciel pourra également décider, passé un certain délai, de router le document vers une autre personne.

Pour obtenir une traçabilité complète, un fichier historique est généré à chaque création de tâche. Ce fichier est ensuite enrichi par le positionnement exact de la tâche dans la procédure de traitement, le chemin qu'elle a déjà parcouru, les alertes émises, les messages d'erreurs.

L'activité d'un salarié peut être suivie très finement, en temps réel, par l'intermédiaire d'un logiciel de work-flow. A partir du besoin légitime de l'entreprise d'optimiser la gestion de ses dossiers, on pourrait aboutir sans effort particulier puisque toute l'information est déjà disponible, à un profilage implicite de l'activité des salariés.

Les outils techniques de surveillance du réseau

Les réseaux informatiques qui relient les sites informatiques centraux et les postes de travail comportent de nombreux composants (armoire de brassage, routeurs, multiplexeurs, cartes réseaux). La topologie du câblage peut avoir des variantes (anneau, réseau en étoile ...). Les protocoles, c'est-à-dire les langages informatiques qui formalisent les procédures d'échange de données entre ces composants, sont également nombreux comme le protocole TCP/IP bien connu du monde internet, mais également les protocoles propriétaires très répandus (SNA d'IBM, DSA de Bull). Enfin, différents protocoles peuvent être implémentés sur un même réseau physique. L'ensemble constitue ce que l'on appelle "l'architecture réseau" de l'entreprise.

Toute informatique d'entreprise ou d'administration comporte une fonction de *gestionnaire de réseau*. Ce métier consiste à installer ou à maintenir les éléments actifs énumérés ci-dessus, à installer les logiciels réseau sur les ordinateurs centraux et les postes de travail, à les mettre à niveau quand de nouvelles versions sont mises sur le marché par les fournisseurs, etc. Mais l'une des activités principales du gestionnaire de réseau réside dans la surveillance du réseau, pour détecter les pannes, déceler les engorgements, mieux répartir les charges. Ce contrôle peut être permanent ou réalisé "par campagne". Les outils de surveillance mis à la disposition de l'administrateur réseau vont du plus frustre à des systèmes très sophistiqués.

Le logiciel de surveillance collecte des informations sur les différents points sensibles du réseau en interrogeant les composants actifs ou par l'intermédiaire de sondes placées aux points névralgiques. Ces sondes, véritables "pinces d'écoute", sont soit des équipements matériels, soit des "sondes logiciel" simulant le fonctionnement d'une "sonde matériel". La collecte de données par le logiciel de surveillance ne se fait pas en continu, la charge supplémentaire occasionnée serait trop importante ; elle a lieu à des intervalles périodiques, toutes les 30 secondes par exemple. L'administrateur peut raccourcir l'intervalle s'il désire mener une surveillance plus serrée.

Entre le logiciel de surveillance, les composants actifs et les sondes, existe un protocole (langage)

de supervision, le SNMP, qui permet au logiciel d'indiquer à "ses mouchards" quelles sont les informations qu'il désire recevoir, sous quelle forme, à quelle cadence. Entre deux envois vers le logiciel de surveillance, les composants actifs ou les sondes collectent les données qui transitent et les stockent sous une forme appropriée dans des structures pouvant constituer de véritables petites bases de données locales. Les résultats des traitements effectués sur ces données collectées sont affichés en temps réel sur un ou plusieurs écrans. C'est essentiellement là que se situent les différences entre les logiciels de surveillance. En outre, les données transitant sur le réseau peuvent être stockées dans des fichiers de traces (fichiers logs) pour une analyse ultérieure, en différé.

Le premier type de traçage se situe au niveau de la *couche logicielle* la plus primitive, la couche dite "basse" : tout ce qui sort ou entre dans l'ordinateur par la voie du réseau, le moindre bit, est mémorisé dans un fichier de traces. L'objectif de ce traçage est de permettre aux informaticiens de rechercher les causes de "bogues" de logiciel ou de mauvaises performances du système.

Le niveau suivant en matière de traçage est celui du *moniteur transactionnel* qui connaît la notion de transaction c'est-à-dire des séquences plus élaborées que les simples séquences de bits et ayant un sens sémantique plus riche. Il génère ses propres fichiers de traces. La lecture d'un fichier de traces d'un moniteur transactionnel est de ce fait plus facilement exploitable et instructive : on pourrait y lire, sans grande peine, qui a fait quoi et à quelle heure.

Le dernier niveau de traçage est celui fourni par *l'application (traces ou logs)*. Dans la plupart des cas, les informaticiens développeurs y ont implémenté une fonctionnalité qui permet de tracer de façon synthétique, presque en clair, l'activité des utilisateurs.

En résumé, certains produits permettent, d'origine ou selon le paramétrage effectué, seulement de mesurer des débits. D'autres vont permettre la surveillance simultanée de plusieurs routeurs. D'autres encore permettront, par exemple, de mesurer le nombre d'appels, les durées des consommations et les seuils d'alerte. Cela signifie qu'il est possible de savoir qui s'est connecté, à quel site, à quelle heure et pendant quelle durée, quelles sont les tentatives de connexion qui ont échoué, etc.

Les logiciels de télé-maintenance des postes de travail

Quand le parc des terminaux est important ou géographiquement dispersé, l'équipe informatique s'aide souvent d'un logiciel de télé-maintenance pour réagir plus rapidement aux attentes des usagers, notamment pour la détection des pannes et leurs corrections. Ces logiciels permettent, en temps réel et à distance, c'est-à-dire à partir du poste de travail de l'informaticien, de voir, comme par décalque[3], tous les faits et gestes qu'un usager est en train d'accomplir sur son poste de travail.

Le principe de fonctionnement de ces logiciels de surveillance est simple : un logiciel dit client est

[3] : C'est d'ailleurs le nom de l'un de ces produits, CarbonCopy

installé sur chaque poste de travail à surveiller pour intercepter toutes les opérations déclenchées sur le micro : appui sur une touche du clavier, déplacement ou clic de la souris, affichage sur l'écran, pour les transmettre vers le poste de surveillance sur lequel l'opération est resimulée.

Certains logiciels plus sophistiqués permettent à l'informaticien de prendre le contrôle, toujours à distance, du poste de travail d'un salarié. L'informaticien peut ensuite agir à sa guise, comme s'il faisait face au micro-ordinateur dont il a pris le contrôle. Il peut donc voir les textes qui sont tapés par la personne, ses fautes de frappe et leur correction en direct, il peut aller modifier un fichier sur le disque dur du salarié sans que celui-ci ne s'en aperçoive autrement qu'en constatant que le fichier n'est plus ce qu'il était lorsqu'il l'avait fermé, il peut enfin créer des fichiers ou en supprimer à sa guise.

Les pare-feu ou "firewall" : le "check-point charly" entre l'entreprise et internet

Tout serveur accessible à partir d'internet, soit directement soit indirectement par rebond, doit se protéger des attaques extérieures. Un pare-feu est un produit logiciel ou matériel assurant au minimum la protection d'un réseau interne d'attaques externes. Il permet également la protection des réseaux internes les uns par rapport aux autres, le filtrage des communications, l'authentification, le cryptage et le contrôle des accès utilisateurs par rapport aux réseaux.

En général, les pare-feu adoptent la politique suivante : initialement, tout le trafic sortant de l'entreprise, aussi bien local que distant est a priori autorisé ; le trafic entrant est restreint à la messagerie électronique. A partir de cette situation initiale, l'entreprise doit définir sa politique en matière de sécurité et de filtrage et la traduire en un ensemble de règles que le pare-feu devra appliquer, sachant que tout ce qui n'est pas expressément autorisé sera refusé.

Le pare-feu peut *authentifier* les personnes qui veulent se connecter (login). Traditionnellement, ce contrôle est réservé au système d'exploitation ou aux applications. Mais dans le cadre d'internet, ce schéma serait trop dangereux car les ordinateurs de l'entreprise seraient alors en contact direct avec des personnes qui ne se seraient pas encore authentifiées, ce que l'on souhaite éviter. La solution habituelle consiste à placer un serveur d'identification en frontal, derrière lequel s'abrite le réseau interne de l'entreprise, mais le pare-feu est également de plus en plus utilisé pour cette fonction.

Le pare-feu *protège* contre la propagation des virus, cookies, applets Java, ActiveX et les contenus Web indésirables. Ainsi, il permet de *filtrer* les URL suivant le principe de la liste noire [4].

Dans le même souci d'entretenir l'opacité protectrice entre l'extérieur et l'intérieur, le pare-feu permet le *masquage des adresses IP*. : Connaître l'adresse IP d'une machine, c'est déjà pouvoir commencer à entamer un dialogue avec elle, avec peut-être l'intention de nuire. Pour parer à ce

[4] *Les sites sont repérés sur Internet par leurs adresses IP, des nombres de 4 à 12 chiffres à laquelle correspond une notation textuelle appelée URL, par exemple www.cnil.fr. Une liste de filtrage peut, au choix, être conçue dans les deux sens : c'est la liste des sites autorisés mais ce peut être aussi la liste des sites non autorisés.*

danger, le pare-feu masque les adresses du réseau informatique interne, en présentant au monde extérieur des adresses IP formellement valides mais factices.

Les réseaux privés virtuels (extranet) : pour les entreprises installées sur plusieurs sites géographiquement distants, internet est une alternative flexible et peu coûteuse à la location de lignes spécialisées privées. Mais utiliser internet, c'est fragiliser la transmission des données en terme de confidentialité et d'intégrité. Le réseau privé virtuel est une réponse à ce problème grâce aux techniques de chiffrement qui permettent d'établir de véritables "tunnels de communication confidentiels" entre les différents interlocuteurs. Tous les échanges sont cryptés et les interlocuteurs sont authentifiés par des signatures numériques et des certificats.

En définitive, le pare-feu collecte et analyse une masse énorme de données sur l'utilisation d'internet. Le pare-feu est, de par sa nature, le meilleur gardien de l'entreprise puisque bien paramétré il protège efficacement l'entreprise des agressions extérieures et évite les connexions considérées comme inappropriées par l'entreprise. Mais il peut aussi devenir le meilleur "espion" de l'activité internet, rien ne peut se faire sans qu'il le ne le sache, jusqu'au plus petit détail. Il détiendra de ce fait toutes les traces de l'activité qui transite par lui : détails de la navigation sur internet (sites visités, heures des visites etc), les détails de messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe, et éventuellement texte du message.

Tous ces produits sont déjà largement diffusés aux USA depuis 5 ans. Le marché qui était naissant en Europe en 1998 est, à l'heure de la rédaction du présent rapport, en pleine expansion. En France, les professionnels de la sécurité estimaient en 1999 que le marché allait tripler dans les trois ans pour atteindre 3350 MF. Il ressort de cette étude que la grande majorité des grands comptes sont d'ores et déjà équipés en outils de sécurisation des systèmes d'information.

Les employeurs lors de leur décision de s'équiper d'un produit tel qu'un pare-feu prennent en compte, bien sûr, les qualités de sécurité offertes le produit. Mais ils s'intéressent de plus en plus fréquemment aux fonctions associées de surveillance de l'activité de l'entreprise. On constate que des produits au nom évocateur ont beaucoup de succès, par exemple et de façon non exhaustive : LanSpy, SuperScout, SurfControl, Cyberpatrol, Marshal Software, Winwhatwere. Toutefois, la "résistance" s'organise puisqu'il est possible de télécharger sur internet des outils (avec des noms tout aussi évocateurs) qui permettent au salarié de vérifier si son ordinateur a été utilisé en son absence (tel que Redhand), ou encore de faire face à l'arrivée impromptue du supérieur hiérarchique par des "boutons panique"qui affichent des graphiques très sérieux voire par des "fichiers son" simulant le bruit de la frappe sur le clavier (donsbosspage.com) !

Au-delà de cet aspect anecdotique l'entreprise a besoin d'une véritable politique de sécurité qui répondra aussi bien à son souci de protection vis-à-vis des flux entrants (contenus malveillants) que vis-à-vis des flux sortants (accès non autorisés ou la transmission de données confidentielles).

Les proxys ou le reflet de vos pages préférées

La fonction d'un serveur proxy est de mémoriser les pages web consultées par les internautes de sorte qu'en cas de nouvelles requêtes vers ces sites ou les pages des sites précédemment

consultés, il ne soit pas nécessaire d'accéder au serveur distant, ce qui économise ainsi de la bande passante et permet une connexion beaucoup plus rapide. Pour ce faire, chaque demande de consultation d'une page web sera précédée d'une requête vers le serveur proxy afin de savoir s'il ne détient pas une copie de la page ou si la page n'a pas été modifiée entre temps. Toutefois, un serveur proxy ne dispose pas d'un espace disque illimité, il lui faut constamment libérer de la place pour mémoriser de nouvelles pages en éliminant les pages les plus anciennes ou les moins référencées.

L'entreprise pourrait profiter de la fonction de mémorisation du serveur proxy pour surveiller l'utilisation d'internet de ses salariés puisqu'un serveur proxy connaît nécessairement l'adresse IP de l'internaute à qui il doit renvoyer une page web. Toutefois ce constat mérite d'être relativisé dans la mesure où la plupart des serveurs proxy sont hébergés hors de l'entreprise, chez le fournisseur d'accès par exemple, et qu'il n'est donc pas "sous les yeux" de l'employeur. Toutefois, la fonction proxy peut être intégrée dans un pare-feu comme le proposent certains fournisseurs.

Enfin, pour être tout à fait complet, il convient de préciser que tout internaute a le choix de renoncer à l'usage du proxy, mais au prix d'une baisse des performances, en "décochant" l'option proxy dans son navigateur.

La messagerie

La messagerie occupe une place de choix dans le monde de l'internet en permettant à deux internautes de communiquer à travers l'envoi et la réception de messages écrits identifiés par une adresse "e-mail".

Selon le choix technique fait par l'entreprise, le message peut être acheminé par le réseau téléphonique habituel à l'aide d'un modem ou emprunter le réseau local de l'entreprise jusqu'au serveur de celle-ci, qu'il soit situé à l'intérieur de l'entreprise ou chez un fournisseur d'accès. Dans ces deux cas, le logiciel utilisé est spécifique au service de messagerie.

Il est également possible d'utiliser les services de messageries offerts sur le web par des sites spécialisés. Cependant, dans un tel cas, la messagerie échappe au contrôle de l'entreprise mais également aux outils de sécurisation, c'est pourquoi cette possibilité est très souvent interdite par les entreprises.

Lorsque le message est acheminé par le réseau téléphonique à l'aide d'un modem, il n'y a aucun moyen technique simple pour l'entreprise de l'intercepter en interne (il faudrait placer la ligne téléphonique sous interception puis mettre en place un dispositif spécifique non disponible sur le marché grand public). Mais il convient de souligner que tout message transitant par un serveur de messagerie, son contenu peut en tout état de cause être accessible à l'employeur.

Lorsque le message emprunte le réseau local de l'entreprise, le message laissera des traces en deux endroits : sur le serveur où sont stockés les messages ou sur le pare-feu qui peut les filtrer. Dans le cas du serveur, l'administrateur de la messagerie et le personnel d'exploitation peuvent techniquement lire le contenu d'un message, pourvu qu'il ne soit pas crypté, au même titre qu'ils

peuvent lire n'importe quel fichier du serveur.

C'est la différence fondamentale entre un appel téléphonique et un message électronique. L'appel téléphonique est volatil et s'achève aussitôt le combiné raccroché. Le message électronique lui, repose dans le disque dur de l'utilisateur, et trace en est conservée sur le serveur de messagerie et au niveau du pare-feu.

De surcroît, des programmes peuvent également être écrits, sans difficultés particulières, pour "traiter" à des fins de surveillance et selon des critères tels que des mots clefs, la référence du destinataire, la présence et/ou le volume du fichier joint, le format (texte, image), le contenu des messages.

Quant au pare-feu, de par sa fonction, il permet de faire une surveillance en continu de ce qui entre ou sort de l'entreprise ; il peut être programmé pour filtrer et surveiller le contenu des messages, détecter les virus, etc.

Il faut toutefois noter le cas fréquent où il n'y a ni serveur ni pare-feu internes à l'entreprise si celle-ci choisit d'héberger la totalité de sa messagerie à l'extérieur. Dans ce cas l'entreprise ne peut exercer une surveillance sur la messagerie qu'en passant un accord commercial avec son hébergeur.

On rencontre également des situations mixtes, combinant un serveur de messagerie interne à l'entreprise et une messagerie hébergée à l'extérieur.

Le disque dur de l'utilisateur ou la boîte noire personnelle

L'ordinateur de l'internaute conserve en mémoire les pages qui ont été visualisées, dans le but de pouvoir les afficher plus rapidement et facilement si elles sont demandées de nouveau. L'ordinateur enregistre également les informations qui lui sont envoyées par les sites : les cookies ou les applets.

- **La mémoire cache**

L'utilisation de la mémoire cache est un moyen d'optimiser les temps de chargement et désengorger le réseau. Son principe est analogue à celui du proxy évoqué ci-dessus : éviter de solliciter inutilement les serveurs distants de site web quand l'internaute consulte fréquemment les mêmes pages. Mais à la différence du proxy qui est sur un serveur externe, ici les pages sont mémorisées sur le micro de l'internaute au fur et à mesure de leur consultation. Si cette fonctionnalité est présente sur le navigateur, lorsque une requête est lancée, le navigateur commence par aller voir sur un répertoire du disque dur si la page HTML demandée n'aurait pas été chargée auparavant. Si tel n'est pas le cas, il effectuera alors la requête auprès du proxy, puis auprès du serveur distant, mais lorsque son résultat arrive, il sera enregistré sur le disque en même temps que présenté à l'écran. La fois suivante, si la même requête est lancée, le navigateur ira simplement la lire sur le disque. Cette mémoire est très souvent appelée "Temporary Internet Files" ou "cache" dans l'arborescence du disque dur.

La rubrique “Vos traces” sur www.cnil.fr explique aux internautes comment effacer leurs traces, s’ils le souhaitent.

- **Les cookies**

Un cookie est un enregistrement d'informations par le serveur dans un fichier texte situé sur l'ordinateur client, informations que ce même serveur (et lui seul) peut aller relire et modifier ultérieurement. La technique des cookies repose sur le protocole HTTP, qui est le langage de communication du web. Il ne faut donc pas voir des cookies partout : seul un serveur web peut en envoyer et aller les relire pour exploiter leur contenu.

Les sites web utilisent la technique du cookie pour faire un suivi des internautes qui les consultent, le terme “suivi” pouvant aussi bien signifier “apporter une aide” (par exemple, pour éviter à l’internaute d’avoir à taper son numéro de compte chaque fois qu’il accède au service consultation par internet de sa banque), qu’un traçage (permettant au site web de savoir qu’il a affaire au même internaute malgré des consultations espacées dans le temps) ou un profilage (en mémorisant le détail du comportement de l’internaute lorsqu’il navigue entre les pages du site). Si le contenu du cookie n’est pas codifié, l’employeur curieux pourrait, dans une certaine mesure, avoir des renseignements sur ce que son employé a fait durant ses navigations sur le web, mais cette hypothèse il est vrai, demeure très limitée. D’ailleurs, une méthode bien plus commode, pour connaître les noms du site qu’un internaute a récemment consultés, est d’afficher par simple clic, le “volet d’exploration historique” situé sur la fenêtre de son navigateur.

La rubrique “Vos traces” du site de la CNIL explique également aux internautes comment effacer les informations enregistrées dans ce volet.

- **La messagerie**

La messagerie installée sur un ordinateur stocke tous les messages envoyés et reçus par cet ordinateur. La suppression d’un message sur un ordinateur demande deux opérations : la suppression de la boîte à lettre active, de “réception” pour un message reçu ou “d’envoi” pour un message envoyé, puis la suppression du fichier dit “poubelle” dans lequel il a été stocké après la première opération. Mais de telles opérations sont vaines, du point de vue de la discrétion, si une sauvegarde des données existe par ailleurs. Aussi, est-il essentiel que tout salarié soit informé de l’existence d’une sauvegarde et de la durée pendant laquelle les données sont conservées.

Enfin, la configuration basique de l’ordinateur, sa nature même, permet de retrouver tout ce qui a été fait sur cette machine. En effet, l’information est stockée en mémoire (la capacité mémoire est un des arguments de vente). Cette mémoire permet de retrouver toute l’information traitée sur cet ordinateur, y compris en cas de suppression ou en cas de perte dû à un arrêt brutal du travail en cours. Tel est l’avantage.

Le revers de cette fonction de base est qu’elle permet de retrouver, sans utiliser les technologies déjà détaillées, disséminés dans le disque dur, l’heure de la dernière modification d’un fichier quel qu’il soit (y compris ceux que le salarié aurait enregistrés dans son répertoire dit “personnel”), les pages internet visitées, les messages envoyés et reçus. Il convient de noter que des outils à coût

modique permettent de récupérer des fichiers effacés, invisibles pour l'utilisateur, mais toujours présents sur le disque dur.

En définitive, les traces peuvent être classés en trois catégories :

- pour les besoins de l'entretien du système à titre préventif ou curatif : détecter les pannes, améliorer les performances ;
- pour les besoins de sécurité, en n'autorisant l'accès au système qu'aux seuls utilisateurs habilités et savoir qui fait quoi ;
- pour restreindre, par filtrage, certaines actions des utilisateurs (censure) considérées par les entreprises comme étant hors du champ de leurs activités.

L'informatique ne peut fonctionner sans trace, sinon l'informaticien aurait à gérer le système en aveugle, les événements survenant dans un ordinateur étant trop nombreux et se déroulant trop vite. En outre, en informatique, toute activité d'un utilisateur est "traçable"... y compris sa non activité.

*

Cette brève description des effets de la technique illustre un point essentiel : c'est la technique qui crée ou provoque la "trace". Qu'il s'agisse d'architecture informatique en réseau ou du protocole TCP/IP, les données transactionnelles qui sont générées sont nécessaires à leur bon fonctionnement. La CNIL l'a à plusieurs reprises affirmé. "*Jadis, nous étions fichés parce que quelqu'un souhaitait nous ficher. Aujourd'hui, nous pouvons aussi être fichés du seul fait de la technologie qui produit des traces sans que nous en ayons toujours pleinement conscience*" [5].

Ces technologies ne sont pas, en tout cas principalement, conçues pour nous surveiller, mais elles permettent d'exercer une surveillance et qui peut être redoutable tant les données susceptibles d'être exploitées sont nombreuses et précises.

On parle en droit pénal et en criminologie "d'armes par destination" pour évoquer des objets qui ne constituent en rien des armes, mais qui ont pu être utilisés comme telles. Ainsi, d'un chandelier s'il est jeté au visage d'autrui. Si les architectures en réseau et les protocoles de l'internet ne sont pas des outils de surveillance par nature, ils peuvent être incontestablement des outils de surveillance par destination.

Dès lors, la réflexion sur la mise en oeuvre des nouvelles technologies de l'entreprise interroge plusieurs champs du droit et des libertés : les conditions de mise en place des outils de surveillance dans l'entreprise, les conditions de mise en oeuvre de traitement de l'information nominative, les conditions d'utilisation à des fins personnelles d'outils professionnels mis à la disposition des

---

[5] *20ème rapport d'activité pour 1999 , avant-propos du président Michel Gentot.*

salariés par l'employeur.

De l'émergence de la vie privée du salarié dans l'entreprise à la discussion collective sur les technologies de surveillance et de contrôle

Des lois "Auroux" aux lois "Aubry"

Comme le relève le professeur Lyon-Caen dans son rapport, la loi du 4 août 1982 relative aux libertés des travailleurs "*s'est attaquée à la plus vieille institution du droit du travail : le règlement intérieur, acte dans lequel s'exprime le pouvoir réglementaire privé du chef d'entreprise*".

En précisant que le règlement intérieur ne pouvait apporter aux droits et libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nécessité de la tâche à accomplir ni proportionnées au but recherché, l'article L 122-35, dans sa rédaction issue de la loi de 1982, a donné, selon l'éminent professeur, un "coup de clairon" qui a "ouvert les oreilles" et permis à la jurisprudence de livrer ses premiers arbitrages.

Ainsi, pour s'en tenir à quelques exemples dans lesquels, sans qu'il s'agisse encore de nouvelles technologies ou d'ordinateurs, il était déjà question de "fouille" et "perquisition", il a été jugé que l'ouverture des armoires et vestiaires mis à la disposition des salariés pour en contrôler l'état et le contenu sans information préalable des salariés concernés et hors leur présence, excédait l'étendue des restrictions que l'employeur pouvait légalement apporter aux droits des personnes et aux libertés individuelles (Conseil d'Etat, 12 juin 1987, 8 juillet 1988, 12 novembre 1990[6]).

Faire procéder systématiquement à des vérifications relatives aux objets emportés par les salariés et leur demander de se soumettre à une fouille corporelle a également été considéré comme illicite (Cass Crim 1er décembre 1987[7]). Seule une nécessité particulière liée par exemple à des vols ou disparitions pourrait justifier de telles pratiques à la condition que la fouille ait lieu en présence d'un tiers et avec le consentement du salarié (Conseil d'Etat 19 juin 1989[8]).

Cette jurisprudence illustre que le rapport de subordination du salarié sur son lieu de travail ne saurait justifier des mesures disproportionnées de contrôle ou de surveillance. Qu'il y a une part, sans doute résiduelle mais en tout cas irréductible, de liberté et de vie privée dans l'entreprise.

---

[6] *: Droit social 1987 p 645 et D 1990 sommaire p 134*

[7] *: Jur UIMM 88 p 503 ; Droit ouvrier 1989 p 138*

[8] *: Jur UIMM 89 p 499*

Mais encore, la loi du 4 août 1982 ne posait-elle de limites tenant à la proportionnalité des moyens employés au regard des fins poursuivies qu'au seul règlement intérieur, laissant hors de portée les stipulations du contrat lui-même et les documents annexés au contrat individuel qui peuvent contenir d'importantes restrictions aux libertés personnelles.

La loi du 31 décembre 1992, très largement inspirée des propositions du rapport Lyon-Caen et de la doctrine dégagée par la CNIL en matière de traitements automatisés d'informations nominatives viendra compléter et renforcer ce dispositif.

Ainsi, l'interdiction d'apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché, n'est plus cantonnée par l'article L 120-2 du code du travail au seul règlement intérieur et s'impose à tous ("*Nul ne peut apporter aux droits...*"). Parallèlement, l'article L 122-39 soumet au même régime juridique que le règlement intérieur lui-même toutes les notes de service ou tout autre document qui portent prescriptions générales et permanentes dans les matières qui relèvent du règlement intérieur, c'est-à-dire notamment les conditions d'utilisation des équipements de travail et les règles générales et permanentes relatives à la discipline.

Il en résulte que de telles notes de service ou documents portant prescriptions générales doivent désormais être soumis à l'avis du comité d'entreprise ou, à défaut, à l'avis des délégués du personnel (article L 122-36) et que l'inspecteur du travail peut à tout moment exiger le retrait ou les modifications des dispositions qui seraient considérées comme portant une atteinte disproportionnée aux droits des salariés (article L 122-37).

Dans le même esprit, la loi du 31 décembre 1992 fera obligation à l'employeur d'informer et de consulter le comité d'entreprise, préalablement à la décision de mise en oeuvre de moyens ou de techniques permettant un contrôle de l'activité des salariés (article L 432-2-1) et, prolongeant les principes de la loi "informatique et libertés" dans le code du travail, précisera qu'"*aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à l'emploi*".

Les trois limites au pouvoir de direction de l'entreprise en matière de contrôle et de surveillance des salariés

Ainsi, trois limites se trouvent imposées au pouvoir de direction de l'entreprise en matière de contrôle et de surveillance des salariés : la transparence, la proportionnalité et la discussion collective.

- **La transparence**

Elle résulte désormais de l'article L 121-8 du code du travail (*"Aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à l'emploi").*

L'obligation de transparence inspirait déjà la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui soumet tout traitement automatisé d'informations nominatives à déclaration préalable auprès de la CNIL, interdit que les données soient collectées par un moyen frauduleux, déloyal ou illicite et impose une obligation d'information des personnes concernées notamment sur les destinataires des données et le lieu où s'exerce le droit d'accès et de rectification.

La transparence, entendue comme l'information préalable et la loyauté, est donc une condition nécessaire. Elle n'est pas suffisante.

- **La proportionnalité**

Sans doute plus subjectif et plus délicat de mise en oeuvre, le principe de proportionnalité ne s'en impose pas moins comme une condition indispensable à la régularité d'un système de contrôle et de surveillance d'un salarié sur son lieu de travail. Mais proportionné par rapport à quoi ?

La valeur protégée est, selon les textes considérés, la "vie privée" (article 9 du code civil : "*Chacun a droit au respect de sa vie privée"*) ou les "*droits des personnes et libertés individuelles*" invoqués par l'article L 120-2 du code du travail ou encore *"l'identité humaine, les libertés individuelles ou publiques*" au sens de l'article premier de la loi du 6 janvier 1978. Mais il ne s'agit ici que de textes nationaux. Ils ne sont, cependant pas seuls en cause.

En effet, la Cour européenne des droits de l'Homme a eu l'occasion d'invoquer l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950 dans des domaines relevant de la vie professionnelle ("1. *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2. Il ne peut y avoir 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 sécurité 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 de la protection des droits et libertés d'autrui"*).

La CEDH a, par deux arrêts de 1992 et 1997, invoqué les dispositions de l'article 8 relative à la vie privée dans des espèces où l'atteinte qui y avait été portée avait eu lieu dans des locaux professionnels.

Dans l'affaire N c. Allemagne du 23 novembre 1992, il s'agissait d'une perquisition dans le cabinet d'un avocat. La Cour européenne a récusé l'argument du Gouvernement allemand soutenant l'inapplicabilité de l'article 8 dans le cadre des activités professionnelles ou

commerciales. *"Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables. Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de "vie privée" comme excluant les activités professionnelles ou commerciales; après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur. Un fait, souligné par la Commission le confirme : dans les occupations de quelqu'un, on ne peut pas toujours démêler ce qui relève du domaine professionnel de ce qui en sort"*

Dans l'affaire H c. Royaume Uni du 27 mai 1997, il s'agissait d'écoutes téléphoniques opérées sur la ligne téléphonique professionnelle du requérant La Cour européenne a confirmé qu'il ressortait *"clairement de sa jurisprudence que les appels téléphoniques émanant de locaux professionnels, tout comme ceux provenant du domicile, peuvent se trouver compris dans les notions de "vie privée" et de "correspondance" visées à l'article 8-1"* [9].

Les motivations réitérées de la Cour européenne consacrent l'idée que le lieu de travail, commercial ou salarié, n'est pas exclusif du droit à la vie privée

- **La discussion collective**

Organisée par le code du travail lors de l'introduction dans l'entreprise de traitements automatisés de gestion du personnel ou de moyens et techniques permettant un contrôle d'activité du salarié (article L 432-2-1 du code du travail), la discussion collective donne sa substance au principe de proportionnalité. Le rapport inégal entre l'employeur et ses salariés, consubstantiel à la nature même du contrat de travail et au lien de subordination qui le caractérise, ne garantit pas naturellement la proportionnalité. Trop souvent, sous l'influence sans doute des entreprises américaines, les employeurs soumettent individuellement aux salariés, des chartes, des engagements écrits équivalant à une abdication complète par les salariés de leurs droits.

Cette manière de procéder réalise à coup sûr l'obligation d'information préalable. Mais en se dispensant de la consultation du comité d'entreprise ou des délégués du personnel, elle peut méconnaître les dispositions du code de travail, ainsi que cette idée, sans doute neuve encore, mais essentielle : dans ce lieu de la subordination qu'est l'entreprise, la vie privée ne se défend pas seul mais à plusieurs.

La consécration de ces principes au plan européen et mondial

Transparence, proportionnalité, discussion collective sont loin d'être des principes franco-français. Ils ont été clairement consacrés au plan européen et international par deux textes sans valeur normative mais qui manifestent leur pertinence.

- **Recommandation n° R (89) du comité des ministres du Conseil de l'Europe aux Etats membres sur la protection des données à caractère personnel utilisées à des fins d'emploi,**

[9] *Tous les arrêts de la CEDH sont en ligne sur www.dhdirhr.coe.fr*

du 18 janvier 1989

3. Information et consultation des employés

3.1 Conformément aux législations et pratiques nationales et, le cas échéant, aux conventions collectives, les employeurs devraient informer ou consulter leurs employés ou les représentants de ceux-ci préalablement à l'introduction ou à la modification de systèmes automatisés pour la collecte et l'utilisation de données à caractère personnel concernant les employés.
Ce principe s'applique également à l'introduction ou à la modification de procédés techniques destinés à contrôler les mouvements ou la productivité des employés.

3.2 L'accord des employés ou de leurs représentants devrait être recherché avant l'introduction ou la modification de tels systèmes ou procédés lorsque la procédure de consultation mentionnée au paragraphe 3.1 révèle une possibilité d'atteinte au respect de la vie privée et de la dignité humaine des employés, à moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationale.

- **Recueil de Directives pratiques sur la protection des données personnelles des travailleurs Bureau international du travail, 7 octobre 1996**

Le Bureau International du Travail a adopté le 7 octobre 1996 un recueil de directives pratiques, sur le projet duquel la CNIL avait formulé des observations.

Ce document vise à fournir les orientations sur la protection des données personnelles des travailleurs liés à la relation d'emploi. Ce document, et en particulier les débats qui ont précédé son adoption, avaient largement appréhendé l'utilisation des nouvelles technologies comme moyen de surveillance des salariés.

Ainsi, prévoit-il que "*les données personnelles collectées en relation avec la mise en oeuvre de mesures techniques ou d'organisation visant à garantir la sécurité et le bon fonctionnement des systèmes d'information automatisés ne devrait pas servir à contrôler le comportement des travailleurs"* (point 5.4 du recueil).

Ce recueil de directives pratiques prévoit cependant qu'une surveillance électronique peut être mise en oeuvre à certaines conditions : d'une part, les données recueillies à cette occasion ne doivent pas être l'unique source de l'évaluation du salarié, d'autre part, dans les cas où une surveillance est mise en oeuvre les salariés doivent avoir été informés à l'avance des motivations de cette surveillance, des périodes concernées, des techniques utilisées ainsi que des données collectées (point 6.4 du recueil).

Il est ainsi indiqué qu'une surveillance permanente ne saurait être autorisée que pour des raisons de santé et de sécurité et en vue de protéger les biens de l'entreprise.

Il est également indiqué que la surveillance ne saurait être secrète sauf si elle est autorisée par la législation nationale, et s'il existe des "*soupçons raisonnablement justifiés d'activités criminelles ou d'autres infractions graves*", au titre desquelles il convient d'inclure le harcèlement sexuel.

Une illustration : le contrôle de l'usage du téléphone et les écoutes téléphoniques sur les lieux de travail

Autocommutateur téléphonique et repérage des communications passées à titre privée

Les autocommutateurs téléphoniques installés dans les entreprises permettent notamment de conserver en mémoire les numéros de téléphone composés par les salariés depuis leur poste de travail. Dès 1984, la CNIL a élaboré une recommandation concernant leur usage sur les lieux de travail puis, compte tenu de la généralisation de tels systèmes, a élaboré, par délibération du 20 décembre 1994, une norme simplifiée constituant l'encadrement juridique de l'usage des autocommutateurs [10].

Il résultait clairement de ces textes que l'usage à des fins privées des lignes téléphoniques professionnelles était admis. En effet, cette norme précise que l'une des finalités de l'autocommutateur vise à permettre à l'employeur d'exiger, le cas échéant, de ses salariés, le remboursement des communications téléphoniques à titre personnel.

La CNIL s'est attachée en outre à préciser des règles minimales applicables aux autocommutateurs.

Ainsi, si elle a admis que l'employeur puisse avoir connaissance de l'intégralité des numéros appelés, poste par poste, la Commission a précisé que l'édition des listes de numéros appelés par poste ne devait en aucun cas permettre de porter à la connaissance d'un salarié l'intégralité des numéros appelés par un autre salarié. C'est la raison pour laquelle les quatre derniers chiffres du numéro appelé doivent être systématiquement occultés sur les documents qui sont diffusés dans l'entreprise. En revanche, en cas de contestation, le salarié concerné doit pouvoir avoir accès, dès lors que son employeur en a connaissance, à l'intégralité des numéros qu'il lui est reproché d'avoir appelés.

Dans le même souci d'équilibre et de confidentialité, la CNIL a demandé que les numéros de téléphone appelés ne soient pas conservés au delà d'une durée de six mois, ce délai permettant à l'employeur d'exercer son contrôle - fût-ce avec retard - mais protégeant le salarié d'une surveillance constante de nature inquisitoriale.

En outre, la CNIL a demandé que des mesures particulières soient prises afin que les conditions de mise en oeuvre d'un autocommutateur n'entravent pas l'exercice des droits reconnus par la loi aux salariés protégés. A cet effet, les salariés protégés doivent pouvoir disposer d'une ligne téléphonique non connectée à l'autocommutateur.

---

[10] *Les libertés et l'informatique. Vingt délibérations commentées. CNIL. La documentation française*.

Enfin, et conformément aux dispositions du code de travail, les organismes de représentation du personnel doivent être consultés avant toute mise en place de l'autocommutateur.

Ces mesures illustrent qu'un juste arbitrage peut être réalisé entre les impératifs de l'entreprise et les droits des salariés.

Ecoutes téléphoniques sur les lieux de travail

Là encore, il s'agit d'un exercice pratique d'arbitrage entre intérêts contradictoires, tant la multiplication des services par téléphone et des centres d'appel a conduit les entreprises à surveiller la qualité du service, c'est-à-dire celle de la réponse apportée par le salarié.

La loi du 17 juillet 1970 qui a consacré le droit au respect de la vie privée incriminait par l'article 368 du code pénal *"quiconque aura volontairement porté atteinte à l'intimité de la vie privée d'autrui en écoutant, en enregistrant ou transmettant au moyen d'un appareil quelconque des paroles prononcées dans un lieu privé par une personne, sans le consentement de celle-ci"*. Cette disposition, désormais codifiée, à peu près dans les mêmes termes, sous l'article 226-1 du code pénal, a donné lieu à une abondante jurisprudence et a soulevé diverses difficultés d'application lorsque l'écoute était opérée sur le lieu de travail. Y avait-il ou non, dans un tel cas atteinte à la vie privée ?

.La loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications

Cette difficulté est levée depuis la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications qui a introduit, dans le code pénal, une disposition de plus large portée, codifiée sous l'article 226-15 du nouveau code pénal. Cet article incrimine *"le fait, commis de mauvais foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions"*. Ainsi, la circonstance que les propos relèvent de la vie privée ou de la vie professionnelle est-elle désormais indifférente comme l'est la circonstance que la communication soit passée depuis son domicile privé ou depuis son bureau. C'est le fait matériel de l'interception qui est désormais puni et non plus, strictement, l'atteinte à la vie privée. Seules échappent à l'incrimination les interceptions commises de bonne foi.

De surcroît, le code pénal subordonne la détention d'appareils conçus pour réaliser de telles interceptions à une autorisation délivrée par une commission instituée par l'article R 226-2 du code pénal et présidée par le Secrétariat général de la défense nationale (SGDN).

. Un doute juridique

La première difficulté d'application de ce dispositif de protection était d'ordre juridique. Le législateur avait-il ou non entendu interdire les interceptions de communications téléphoniques opérées par un employeur ou, pour poser plus exactement le problème, un employeur ayant

préalablement informé ses salariés de leur mise sur écoute échappait-t-il à l'incrimination pénale nouvelle au motif que la bonne foi serait alors acquise ? Le ministère de la justice, interrogé par la CNIL sur ce point, avait estimé, en 1994, qu'en l'absence de jurisprudence, la seule réalisation d'une information préalable ne donnait pas l'assurance qu'un tel système serait régulier.

La prudence d'une telle réponse était d'ailleurs compréhensible : suffirait-il qu'un employeur informe ses salariés pour pouvoir les placer continûment sur écoutes téléphoniques sans limitation de durée et sans autre garantie ? Que deviendrait alors les droits particuliers des salariés protégés ? Un tel procédé serait-il admissible ?

Une première réponse, indirecte, a été apportée par la directive européenne 97/66 du 15 décembre 1997 qui fait obligation aux Etats-membres de garantir, par leur législation, la confidentialité des communications passées par la voie des télécommunications et d'interdire *"à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées"*.

Le texte européen, qui n'a pas à ce jour été transposé en droit interne mais dont la modification est déjà envisagée par la Commission européenne, ménage une exception en admettant la régularité *"des enregistrements légalement autorisés de communications, dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale*".

- **Quelques recommandations**

C'est au regard de ces éléments, et saisie de plus en plus fréquemment de traitements automatisés liés à des systèmes d'écoutes téléphoniques, que la CNIL, en liaison avec la commission consultative chargée de délivrer les autorisations de détention de matériel d'écoute, a élaboré un corpus de recommandations [11] .

La finalité du dispositif d'écoute doit être précisée : elle peut résulter de certains textes, ainsi les textes particuliers applicables au passage d'ordres boursiers ; l'écoute peut être opérée à des fins de contrôle de la qualité du service téléphonique ; elle peut, dans certains cas, avoir pour objet l'enregistrement de la preuve d'un ordre commercial passé par un client avec une entreprise ne travaillant que par téléphone (banque à domicile, assurance par téléphone, etc).

Les salariés concernés doivent être prévenus, préalablement à la mise en place de tout système d'écoute, de son existence, des conséquences individuelles qui pourront en résulter et des périodes pendant lesquelles leurs conversations seront enregistrées ; le contrôle de la qualité des réponses ne peut justifier un placement sur écoute continu et doit être opéré par "campagnes".

Les salariés doivent pouvoir disposer de lignes non connectées au dispositif d'écoute pour toutes les conversations qui ne sont pas directement liées au motif de l'écoute, qu'elles soient privées ou professionnelles.

---

[11] *18ème rapport d'activité de la CNIL pour 1997 p. 286 ; rapport d'activité de la CNCIS, pour 1999, p 34*

Lorsque l'écoute est opérée à des fins de contrôle de qualité de la réponse téléphonique, les salariés doivent pouvoir avoir connaissance à bref délai du compte rendu de la conversation enregistrée et doivent pouvoir formuler leurs observations. Les enregistrements effectués doivent être effacés ou détruits dès lors que l'analyse de la réponse a été faite, dans un délai de l'ordre de quinze jours à un mois.

Enfin, les clients appelants doivent également être informés de l'enregistrement de leurs appels.

Dans tous les cas, à l'exception des salles de marchés qui sont régies par une réglementation professionnelle particulière, la Commission instituée auprès du SGDN, subordonne, jusqu'à présent, l'autorisation de détention de matériel d'interception ou d'enregistrement à la condition que la durée de conservation des enregistrements n'excède pas deux mois.

Ainsi, malgré une relative imprécision des termes de la loi du 10 juillet 1991 appliquée aux écoutes téléphoniques sur les lieux de travail, et dans l'attente de la transposition de la directive européenne 97/66, des garanties sont offertes par l'effet combiné de la loi du 10 juillet 1991 (secret des correspondances émises par la voie des télécommunications) et de la loi du 6 janvier 1978 (lorsque les informations directement ou indirectement nominatives font l'objet d'un traitement automatisé).

Mais sans doute, le panorama juridique ne serait-il pas complet si n'était évoqué la jurisprudence.

Panorama de la jurisprudence française

Les décisions de jurisprudence intéressant directement ou indirectement la matière sont nombreuses[12], abondamment commentées, et pas uniquement depuis que l'on évoque la surveillance des messageries électroniques. Evidemment, elles relèvent, le plus souvent, du contentieux disciplinaire et du licenciement dans le cadre du contrat de travail et non pas directement de la vie privée. Cependant, qu'il s'agisse de l'usage à des fins privées des outils mis à la disposition des salariés sur leur lieu de travail ou des moyens de surveillance et de contrôle utilisés par l'employeur, c'est une jurisprudence de la "proportionnalité" qui s'esquisse, dessinant les contours du respect de la vie privée des salariés par leur employeur [13].

La plupart des commentaires que ces décisions ont suscités s'attachent cependant principalement au contentieux de la preuve (à quelles conditions la preuve rapportée d'un comportement fautif du salarié peut-elle être admise au procès ?), sans s'attarder sur le fond du droit, pourtant essentiel : que reste-t-il de la vie privée du salarié sur le lieu de travail, une fois la justice passée ? Les décisions les plus importantes, publiées ces dernières années, méritent d'être explorées dans cette perspective.

Le contentieux de la preuve

Il peut être décliné en quelques principes simples, mais dont chacun doit être nuancé.

- **Récusation de la preuve rapportée par un dispositif de contrôle mis en place à l'insu du salarié.**

C'est un important arrêt de la Chambre sociale de la Cour de Cassation du 20 novembre 1991[14] qui en a confirmé le principe. Une caméra de vidéosurveillance avait permis de repérer que la caissière d'une cordonnerie détournait de l'argent. Licenciée pour faute grave, la caissière contestait ce mode de preuve. La Cour de Cassation a estimé que "*si l'employeur avait le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, tout enregistrement, quels qu'en soient les motifs, d'images ou de paroles à leur insu, constituait un mode de preuve illicite*". Dans le cas d'espèce, la caméra ayant été dissimulée et aucune information préalable des salariés n'ayant été effectuée, l'arrêt de la Cour d'Appel qui avait estimé régulier le licenciement a été cassé.

---

[12] *: Il est à noter que la jurisprudence relative aux fonctionnaires est peu abondante sur ces sujets.*

[13] *: "Le pouvoir de direction et les libertés des salariés" - Philippe Waquet - Droit Social, déc 2000.*

[14] *: D 1992 jurisprudence p 73*

Il doit être observé que cet arrêt ne concerne nullement la vie privée sur les lieux de travail mais exclusivement le principe de loyauté, loyauté dans le travail et loyauté des moyens de preuves recherchés par l'employeur, comme l'a nettement précisé l'avocat général dans ses conclusions[15].

Aussi, la même juridiction a-t-elle pu estimer régulier un licenciement pour faute grave dont la preuve avait été rapportée par une caméra de vidéosurveillance qui avait été mise en oeuvre sans information préalable des salariés, dans la mesure où la caméra était installée dans des entrepôts où les salariés n'avaient pas à pénétrer. *"L'employeur est libre de mettre en place des procédés de surveillance des entrepôts de rangement dans lesquels les salariés ne travaillent pas*" (Cass. Soc, 31 janvier 2001[16]).

. Récusation de la preuve rapportée par un traitement automatisé d'informations nominatives non déclaré à la CNIL.

La Cour d'Appel de Paris a jugé que la production d'un listing de relevés de communications téléphoniques émanant du poste d'un salarié et obtenu au moyen d'un autocommutateur était illicite au motif qu *"en toute hypothèse, l'obligation de déclaration préalable faite à l'entreprise par l'article 16 de la loi du 6 janvier 1978 n'avait pas été respectée, et où ce relevé ne pouvait être conservé pour un motif autre que la facturation éventuelle à la salariée de ses communications personnelles"*. Dans cette affaire, la lecture du listing des relevés de communications établissait, aux yeux de l'employeur, une concomitance parfaite entre les dates d'appels passés par le salarié auprès de ses anciens collègues et les réclamations que ces derniers avaient adressées à l'entreprise (Cour d'Appel de Paris, 7 mars 1997[17]).

Mais la Cour de Cassation a jugé, dans une autre espèce, que ne constituait pas "*un mode de preuve illicite la production par l'employeur des relevés de facturation téléphonique qui lui ont été adressés par la société France Telecom pour le règlement des communications correspondant au poste du salarié*" (Cass. Soc, 11 mars 1998[18]).

Il résulte clairement de cet arrêt que tout mode de preuve du comportement fautif d'un salarié résultant d'un "système d'information" n'est pas subordonné à une information préalable des salariés. En revanche, lorsque la preuve est issue d'un traitement automatisé d'informations nominatives mis en place dans l'entreprise même, la licéité de la preuve est alors subordonnée à celle du traitement, c'est-à-dire, au regard de la loi du 6 janvier 1978, à la déclaration préalable de ce traitement à la CNIL et à l'information préalable du salarié.

---

15 : *conclusions de M. Yves Chauvy, avocat général, Dalloz, 1992, jp, p. 73.*

16 *: pourvoi n° 98-44.290 en ligne sur www.net-iris.com*

17 *: Gaz Pal 21-01-99 p 30*

18 *: pourvoi n° 96-40147 sur www.jurifrance.fr ou Juris Data sur www.juris-classeur.com*

• Récusation de la preuve rapportée par un traitement d'informations nominatives régulièrement déclaré à la CNIL lorsque l'information en cause est sans rapport avec la finalité du traitement.

Un arrêt de la Cour de Paris, en date du 31 mai 1995[19] a jugé que le système informatique de réservation de billets de train dénommé "Socrate" ne pouvait être utilisé à l'insu du personnel pour contrôler son temps de travail. La Cour d'Appel a annulé le blâme qui avait été prononcé à l'égard d'un guichetier de la SNCF auquel la direction avait fait reproche, sur la base des informations consignées dans "Socrate", de s'être absenté de son poste de travail. Il est intéressant de relever que la Cour d'Appel de Paris sans retenir explicitement l'argument du salarié invoquant le détournement de finalité du système a souligné que "*l'absence de précision de la supérieure hiérarchique quant au mode de contrôle personnel effectué, dans les conditions contraires à l'exécution de bonne foi des obligations contractuelles, du système Socrate à des fins de surveillance du personnel et non pas d'enregistrement des réservations constitue un ensemble d'éléments qui laisse un doute sur la régularité des constatations d'absence de M. X et sur la réalité de celles-ci*".

Les juges ne sont pas loin du terrain du détournement de finalité, au moins implicitement, et, en invoquant "*la réalité de l'absence*", de douter de la crédibilité de la preuve informatique. Il est vrai que la jurisprudence paraît exiger de la preuve informatique une qualité particulière.

• Exigence de qualité de la preuve

Trois arrêts méritent d'être cités à ce titre.

Dans un arrêt du 4 janvier 1994, la Cour d'Appel d'Aix-en-Provence a jugé qu'un enregistrement de vidéosurveillance attestant la mauvaise tenue du rayon "fruits et légumes" d'un magasin de nature à justifier , selon l'employeur, le licenciement de son responsable, n'était pas probant. La Cour d'Appel, après avoir relevé que le salarié contestait la matérialité des faits, a souligné que "*compte tenu des possibilités de montage et de trucage qu'offre l'évolution des techniques, ce document ne présente pas de garanties suffisantes d'authenticité, d'impartialité et de sincérité concernant tant sa date que son contenu*". En conséquence, la juridiction d'appel a considéré que le licenciement était sans cause réelle et sérieuse. On pouvait imaginer que cet arrêt fût d'espèce et demeurerait isolé.

Pourtant, dans une affaire il est vrai très différente, la Cour d'Appel de Paris a également estimé qu'un enregistrement de vidéosurveillance ne pouvait fonder une accusation de vol. Il était fait reproche à une caissière d'avoir volé un sac contenant des espèces, ce que cette dernière contestait en s'en remettant à la caméra de vidéosurveillance installée dans le local où elle était chargée d'entreposer les fonds. La juridiction parisienne, après avoir constaté qu'une période de 10 minutes n'avait pas été enregistrée, a constaté que nul ne pouvait savoir ce qui s'était passé dans

[19] *: pourvoi n° 95/30208 index SVP 17 juin 99, Liaisons Sociales du 16 juin 1995*

le local pendant ce laps de temps et a, en conséquence, relaxé la prévenue (Cour d'Appel de Paris, 12 mai 1999[20]).
Cette exigence de qualité de la preuve n'est pas seulement liée à la vidéosurveillance. Ainsi, dans une espèce où le salarié d'un fabricant bien connu d'ordinateurs avait adressé à quelques amis des photographies téléchargées depuis des sites pornographiques sur internet , avant que son supérieur hiérarchique ne découvre, coincée dans l'imprimante couleur, le corps du délit, le Conseil des prud'hommes de Nanterre, dans un jugement du 13 janvier 2000[21], a estimé que le disque dur de l'ordinateur du salarié qui avait été produit à l'audience ne constituait pas un mode de preuve adéquat, l'employeur ayant omis de placer le disque dur sous scellés "*alors que celui-ci pouvait être manipulé sans difficulté entre la date des faits et celle des débats*".

- **Quelques interrogations**

Ce bilan pourrait paraître univoque et signifier qu'une preuve n'est opposable au salarié que si le dispositif de contrôle a été porté à sa connaissance et, lorsque ce dispositif constitue un traitement automatisé d'informations nominatives au sens de la loi du 6 janvier 1978, s'il a été déclaré à la CNIL. Cependant, quelques décisions plus récentes méritent attention.

Ainsi, dans un arrêt du 14 mars 2000[22], la Chambre sociale de la Cour de cassation a jugé dans une affaire dans laquelle le salarié d'une société de bourse s'était livré pendant le temps du travail à des jeux de hasard avec des tiers, tels que des paris sur l'élection présidentielle ou le résultat de matches de football, que les enregistrements de conversations téléphoniques qui témoignaient de ses activités extraprofessionnelles étaient réguliers, "*seul l'emploi de procédé clandestin de surveillance étant illicite*". La Cour de cassation avait pris soin de relever que "*les salariés avaient été dûment avertis de ce que leurs conversations téléphoniques seraient écoutées*".

Certes, l'espèce se situe dans le domaine particulier des sociétés de bourse où une réglementation professionnelle autorise l'enregistrement des ordres d'achat passés par téléphone. Mais il convient de relever que la Cour de cassation n'a pas retenu l'argument du salarié indiquant que l'information qui avait été faite par la direction présentait le système comme devant permettre, en cas de litige avec un client, de justifier les ordres reçus, et nullement comme impliquant l'enregistrement de leurs conversations personnelles. La jurisprudence de la Cour de cassation ne marquerait-t-elle pas une inflexion au regard de la décision de la Cour d'appel de Paris sur le système Socrate[23] ? La récusation du contrôle "*clandestin*" n'est-elle pas de portée plus réduite que celle du contrôle "*à l'insu*" ?

Dans un arrêt plus récent encore (Cass Soc, 18 juillet 2000[24]), la Cour de cassation avait à se prononcer sur la régularité du licenciement d'un auditeur bancaire dont l'exploitation des connexions grâce à un système de traçage avait révélé qu'il consultait, par pure curiosité

---

[20] *: Droit ouvrier 1999 p 460*

[21] *: Gaz pal 28.10.2000 p 34*

[22] *: pourvoi n° 98-42090 www.jurifrance.fr ou Juris Data sur www.juris-classeur.com*

[23] :*précité*

[24] *: pourvoi n° 98-43.485 www.jurifrance.fr ou Juris Data sur www.juris-classeur.com*

personnelle, de nombreux comptes individuels. Le salarié contestait la régularité de son licenciement au motif principal que la preuve de ses agissements avait été rapportée par un système d'espionnage électronique mis en place sans autorisation des représentants du personnel et sans que les salariés en aient été avisés.
A suivre la jurisprudence antérieurement dégagée, les arguments du requérant paraissaient ne pas manquer de force au moins sur le terrain de la licéité de la preuve. Or, la Cour de cassation précise *"que le fait pour une banque de mettre en place un système d'exploitation intégrant un mode de traçage permettant d'identifier les consultants des comptes, ne peut être assimilé ni à la collecte d'informations personnelles au sens de l'article L 121-8 du code du travail, ni au recours à une preuve illicite, le travail effectué par utilisation de l'informatique ne pouvant avoir pour effet de conférer l'anonymat aux tâches effectuées par les salariés*".

Il est intéressant de noter que les juridictions saisies n'ont pas recherché si le système de journalisation des connexions ayant permis d'identifier les agissements fautifs du salarié en cause constituait un traitement automatisé au sens de la loi du 6 janvier 1978 et avait été déclaré à la CNIL et, en tout état de cause, n'ont pas tiré de l'absence d'information spécifique des personnes concernées sur le fondement de la loi du 6 janvier 1978 de conséquences particulières.

Il convient sans doute de se montrer prudent sur la portée de cet arrêt. D'une part, la Haute Juridiction n'en a pas décidé la publication, ce qui signifie qu'il ne constitue pas, à ses yeux, un revirement de jurisprudence. D'autre part, la Cour de cassation s'est appliquée, dans un deuxième attendu, à relever les spécificités de l'espèce : le salarié concerné ne contestait pas les faits qui lui étaient reprochés ; le devoir de discrétion et le secret bancaire avaient été méconnus par celui-là même qui devait, par profession, en assurer le respect. Il pouvait y avoir de la part du salarié fautif quelque impudence à invoquer à son bénéfice une règle qu'il avait méconnue au détriment de tiers.

En définitive, il pourrait être soutenu que ces deux décisions, loin de manifester une inflexion vers plus grande rigueur à l'égard des salariés, peuvent être interprétées comme s'inscrivant en droite ligne de la jurisprudence précédemment dégagée.

En effet, à en rester sur le terrain de la validité de la preuve, on reste sur le terrain de la loyauté. L'article 1134 du code civil précise que les conventions légalement formées tiennent lieu de lois à ceux qui les ont faites et doivent être exécutées de bonne foi. La loyauté est le complément nécessaire du contrat. Elle apporte d'ailleurs au salarié des garanties essentielles. Mais la loyauté n'est pas à sens unique : là où elle interdit à un employeur de procéder clandestinement ou à l'insu du salarié, elle peut priver un cadre pleinement conscient des usages des écoutes téléphoniques, des architectures en réseau ou d'internet de l'argument consistant à reconnaître qu'il a failli mais que la preuve rapportée devrait être récusée au motif qu'il n'avait pas formellement été informé d'un système dont il ne pouvait ignorer ni l'existence, ni la portée.

En tout état de cause, ce rappel jurisprudentiel manifeste que l'on ne saurait limiter le débat sur la vie privée ou la surveillance dans le milieu du travail à une seule bataille de procédure, quelquefois décisive mais toujours incertaine. Au demeurant, nul n'aurait à y gagner. En tout cas, pas les salariés puisque à ne se situer que sur le terrain de l'information préalable, il suffirait à un employeur d'informer précisément les salariés de ses choix de direction pour priver ces derniers de l'ensemble de leurs droits et libertés. C'est précisément ce que proscrit le principe de

proportionnalité auquel les juridictions veillent, notamment dans le cadre du contentieux des sanctions disciplinaires et du licenciement.

Le contentieux du fond : secret des correspondances et usage à des fins privées d'outils mis à disposition par l'employeur

. Correspondances écrites reçues sur le lieu de travail

C'est bien sûr dans ce domaine que la jurisprudence est la plus ancienne. Le secret de la correspondance est une liberté publique et le principe qui domine toute la matière est celui de l'inviolabilité des correspondances. Qu'en est-il des correspondances écrites reçues sur les lieux de travail ? [25]

Reconnaissons-le, la jurisprudence après avoir été, semble-t-il, univoque est désormais beaucoup plus nuancée.

Dès 1938, la Cour d'appel de Paris a considéré comme fautif le directeur d'un journal pour avoir ouvert la correspondance reçue par un des rédacteurs, sous pli fermé, à son nom et au siège du journal (Paris, 17 juin 1938[26]). La Chambre criminelle a eu plusieurs fois l'occasion de statuer dans le même sens. Ainsi, dans un arrêt du 18 juillet 1973[27], a été retenue la culpabilité d'un employeur qui avait ouvert un pli rédigé au nom d'une employée.

Cependant, c'est aux juridictions du fond, d'apprécier chaque cas d'espèce. Ainsi, la Cour de cassation a confirmé un arrêt de Cour d'appel ayant estimé non réunis les éléments constitutifs du délit de violation de correspondance dans une espèce où un chef de bureau du CNRS avait transmis ouvertes à son destinataire trois correspondances envoyées à ce dernier à l'adresse du CNRS. La Cour d'appel avait relevé que les trois lettres ouvertes comportaient seulement le nom du plaignant et son appartenance au CNRS, sans indication sur les enveloppes du caractère privé de la correspondance (Cass. crim, 16 janvier 1992[28]).

Evidemment rien n'interdit à un employeur de proscrire l'envoi à l'adresse de l'entreprise de courriers destinés personnellement aux salariés. Mais une telle interdiction ne lui permettrait ni d'ouvrir ni de retenir le courrier litigieux si l'enveloppe porte la mention "personnelle" ou "confidentiel".

. Utilisation à des fins personnelles de la ligne téléphonique professionnelle

Là encore, la jurisprudence est abondante, compte tenu surtout du développement des autocommutateurs téléphoniques. A déjà été évoquée la jurisprudence récusant comme moyen de preuve un listing de numéros appelés issus d'un autocommutateur non déclaré à la CNIL (Paris,

---

[25] *Gaz Pal 1994, jp, note Philippe Waquet*

[26] *: DH 1938.520*

[27] *: Bull cass n° 336*

[28] *: Gaz Pal 1992, 296*

7 mars 1997 précité) mais admettant que soit opposé aux salariés, sans information préalable, la facturation détaillée établie par France Télécom (Cass. soc, 11 mars 1998[29]).

Dans de nombreuses affaires, l'usage du téléphone à des fins privés a été jugé constitutif d'une faute grave. Ainsi, le fait pour un salarié d'avoir *"usé du téléphone de l'entreprise de façon continuelle et journalière à des fins privées"* (Cass. soc, 7 novembre 1995), le fait pour le manager d'un club de football de passer de *"nombreuses communications à destination de départements étrangers à l'activité du club, le montant des factures ayant très nettement augmenté à son arrivée et diminué après son départ*" (Rennes, ch. soc. 30 septembre 1999[30]), le fait pour un cadre chargé de l'adaptation du système informatique d'avoir utilisé à des fins personnelles le téléphone dans l'entreprise, notamment pour s'entretenir avec des sociétés pour lesquelles il effectuait des prestations informatiques sans lien avec l'employeur, alors que de surcroît, il avait été précédemment mis en garde officiellement (Rennes, ch. soc. 3 juin 1999[31]).

Dans d'autres espèces cependant un usage du téléphone à des fins privés, s'il peut constituer une cause réelle et sérieuse de licenciement, n'est pas jugé constitutif d'une faute grave justifiant un licenciement sans préavis. Ainsi, constituent des causes réelles et sérieuses de licenciement et non des fautes graves, le fait pour le salarié responsable d'une station essence d'avoir entreposé du matériel lui appartenant dans les locaux de l'entreprise sans autorisation de l'employeur pour se livrer à une activité parallèle de vendeur de meubles, opérant par téléphone (Nancy, ch. soc., 12 janvier 2000[32]), le fait pour la responsable d'un magasin d'avoir passé *"en six mois de nombreux appels ne correspondant à aucun numéro professionnel ou attribué à ses proches et 87 appels à son numéro personnel, de préférence quand elle était seule au magasin"* (Reims, ch. soc. 18 août 1999[33]), le fait pour une secrétaire d'avoir passé *"en dix mois 33 heures au téléphone à des fins privées mais alors qu'elle n'avait pas été mise en garde au préalable et que la bonne marche de l'entreprise ne s'en était pas trouvé affectée"* (Paris, 24 février 1999[34]), une utilisation répétitive et délibérée du téléphone par un mécanicien soumis à une astreinte de nuit mais alors que la convention des parties n'interdisait pas l'usage du téléphone à des fins privées (Cass soc, 3 février 1999[35]).

Enfin, une légitime protection du salarié est offerte par la jurisprudence qui annule le licenciement, fondé sur l'usage à des fins privées du téléphone professionnel, lorsqu'il paraît disproportionné aux faits de la cause. Ainsi, a été jugé que ne constituait pas une cause réelle et sérieuse de licenciement un usage du téléphone à des fins privées connu depuis plus de deux mois alors qu'aucun reproche n'avait été précédemment fait au salarié (Cass. soc. 30 mars 1999[36]), l'usage

---

[29] *: pourvoi n° 96-40147 www.jurifrance.fr ou Juris Data sur www.juris-classeur.com*

[30] *: Juris Data n° 111761*

[31] *: Juris Data n° 111761*

[32] *: Juris Data n° 103666*

[33] *: Juris Data n° 107991*

[34] *: Juris Data n° 022688*

[35] *: pourvoi n° 97-40495 www.jurifrance.fr ou Juris Data sur www.juris-classeur.com*

[36] *: pourvoi n° 97-40850 www.jurifrance.fr ou Juris Data sur www.juris-classeur.com*

par un conducteur du téléphone portable qui lui avait été confié par l'entreprise alors que "*ses conditions de travail le contraignait à appeler sa famille pour l'avertir de ses retards et la rassurer*" et que le salarié proposait de rembourser les sommes dues à l'employeur (Nancy, ch. soc. 1er mars 1999[37]), "*un usage n'ayant entraîné qu'un coût modique (moins de 150 F) et alors que l'employeur n'avait fixé aucune règle à cet égard ni mis à la disposition des salariés un point phone*" (Montpellier, ch. soc. 18 février 1999[38]), un usage du téléphone à des fins personnelles lorsque "*l'employeur a reçu sans réserve de la part du salarié concerné le remboursement d'une partie des communications et n'avait nullement interdit un tel usage"* (Cass. soc, 18 novembre 1998[39]), une utilisation prétendument abusive du téléphone par le salarié lorsque aucune corrélation ne peut être faite entre son départ et la baisse de facturation (Pau, ch. soc. 24 mai 1995[40]).

Ainsi, au travers du contentieux de la régularité du licenciement, la jurisprudence dessine-t-elle les contours d'un usage admissible du téléphone professionnel à des fins privées. Bien naturellement, tout est question de mesure et, au fond, de loyauté dans les relations réciproques entre employeur et salarié. A défaut d'abus manifeste et caractérisé, un employeur ne saurait reprocher un comportement s'il n'a pas préalablement déterminé quelle était la règle. En outre, la jurisprudence, sous sa diversité, paraît exiger, en cette matière, qu'une mise en garde précède une sanction telle que le licenciement. Enfin, les juges s'attachent à l'ensemble des circonstances concrètes liées aux faits reprochés au salarié, n'hésitant pas à débusquer sous le prétexte d'un usage abusif du téléphone, la volonté réelle de l'employeur.

- **Utilisation du minitel à des fins privées**

Le recensement des décisions publiées à ce sujet manifeste encore une assez grande tolérance des juridictions à l'égard de l'usage par les salariés du minitel à des fins privées.

Certes, plusieurs décisions retiennent la faute grave. Ainsi, pour l'utilisation la nuit de façon abusive de la ligne téléphonique d'un client par un gardien détaché par une société de gardiennage, "*de tels agissements étant de nature à porter atteinte aux relations de l'employeur avec son client*" (Pau, ch. soc., 30 novembre 1989[41]) ou, dans même circonstance, une utilisation si abusive qu'elle s'apparente à une véritable *"prise de possession"* du minitel à l'insu de son titulaire, assimilable à un vol (Metz, ch. cor. 30 mai 1990[42]).

Plusieurs décisions récusent en revanche la faute grave pour ne retenir que la cause réelle et sérieuse du licenciement. Ainsi, le fait pour une secrétaire d'utiliser le minitel à des fins

---

37 *: Juris Data 041078*

38 *: Juris Data n° 034236*

39 *: n° pourvoi 96-43902 www.jurfrance.fr ou Juris Data sur www.juris-classeur.com*

40 *: Juris Data, n° 045026*

41 **:** *Juris Data, n° 048480*

42 *: Juris Data, n° 045294*

personnelles sans qu'il soit démontré que la totalité des communications lui soient imputables (Paris, ch 22 A, 30 avril 1997[43]).

Mais les décisions les plus nombreuses exonèrent le salarié de toute faute, généralement au motif que la preuve n'est pas rapportée que le salarié en cause ait été le seul utilisateur possible du minitel (en ce sens, Toulouse, ch. soc. 25 juin 1999[44]). En outre, le principe de proportionnalité est plusieurs fois rappelé par les juridictions. Ainsi, le fait pour un gardien qui utilisait à des fins personnelles le minitel pour accéder à des "messageries roses" n'est pas considéré comme "*suffisamment sérieux pour justifier le licenciement d'un salarié ayant dix ans d'ancienneté et qui n'avait jamais fait l'objet d'avertissement sur la qualité de son travail*" (Nancy, ch. soc. 3 juin 1992[45]).

- **Et internet ?**

Naturellement, les décisions de jurisprudence sont moins nombreuses et la plupart de celles qui sont connues relèvent, pour l'heure, des seuls Conseils de prud'hommes. Il est dès lors difficile d'en tirer un enseignement général même si les premières décisions connues paraissent témoigner d'une rigueur particulière à l'égard de l'usage à des fins privées de la messagerie électronique ou du web.

Si le licenciement de l'employé d'un fabriquant d'ordinateur ayant téléchargé des images pornographiques sur le web a été jugé sans cause réelle et sérieuse par le Conseil des prud'hommes de Nanterre dans son jugement du 13 janvier 2000, il a été précisé (cf. supra) que c'était au motif d'une contestation sur la preuve (le disque dur du micro ordinateur mis à la disposition du salarié n'avait pas été placé sous scellé et pouvait, selon la juridiction, avoir été manipulé entre la date des faits et celle du débat judiciaire).

En revanche, le Conseil des prud'hommes de Paris, dans un jugement du 1er février 2000, a jugé régulier le licenciement intervenu à la suite de l'envoi, par erreur, à l'ensemble des salariés de la société d'un message initialement destiné à un proche, extérieur à l'entreprise, révélant de manière explicite l'homosexualité de son expéditeur. La juridiction prud'homale s'est bornée à relever que les faits reprochés au salarié n'étaient pas contestés et qu'ils constituaient "*une infraction au règlement intérieur et aux règles propres à l'utilisation des micro ordinateurs*" caractérisant une cause réelle et sérieuse de licenciement [46].

---

[43] *: Juris Data, n° 021890 Dans le même sens, Paris, ch. soc, 13 octobre 1999, Juris Data n° 024664*

[44] *: Juris Data n° 109845*

[45] **:** *Juris Data, n° 042125 et, dans le même sens, même Cour, 12 février 1992, Juris Data n° 041208*

[46] **:** *édition du Juris-classeur, Travail et Protection sociale, janvier 2001*

Le Conseil des prud'hommes de Montbeliard[47], dans un jugement du 19 septembre 2000, a de même considéré comme régulier le licenciement d'une salariée à laquelle il était reproché d'avoir utilisé à des fins personnelles et pendant son temps de travail "*le matériel de l'entreprise en entretenant au moyen de la messagerie électronique, une correspondance avec une ex-salariée à laquelle ont notamment été communiquées des informations sur la réorganisation en cours de l'entreprise"*.

La salariée en cause ne contestait pas la réalité des faits mais faisait reproche à son employeur de n'avoir pas informé les salariés, ni consulté le comité d'entreprise sur le dispositif de contrôle de la messagerie. La juridiction prud'homale qui observe que la salariée mise en cause a produit elle-même à l'audience le compte-rendu des messages contestés sans démontrer que son employeur avait pu en avoir connaissance dans des conditions frauduleuses, relève qu'une note de la direction avait rappelé que la messagerie électronique était réservée à une utilisation professionnelle et que l'employeur conservait un droit de regard à tout instant. Cette décision a été diversement commentée [48].

Mérite également d'être cité un jugement, non définitif, de la 17 ème Chambre correctionnelle du tribunal de grande instance de Paris du 17 novembre 2000[49] dans une affaire qui a été fort commentée. L'affaire opposait deux étudiants en informatique travaillant dans le même laboratoire scientifique. Les suspicions portées contre l'un deux d'avoir procédé, par dépit amoureux, à diverses manipulations informatiques et intellectuelles au détriment de sa collègue (disparition des fichiers enregistrés dans le micro ordinateur, fausse lettre portant une signature falsifiée demandant le retrait de publication d'un article scientifique rédigé par son amie, etc.) ont conduit les responsables du laboratoire à surveiller les flux de courrier électronique de l'établissement, avant de placer la messagerie du suspect sous surveillance dans le but de contrôler la provenance et la nature des messages reçus ou adressés à l'étudiant en cause. Ce dernier se constitua partie civile pour atteinte à l'intimité de la vie privée, accession frauduleuse à un système de traitement automatisé et atteinte au secret des correspondances.

La 17ème chambre du tribunal de Paris a requalifié les faits sous la prévention de violation de correspondance effectuée par la voie des télécommunications par personne chargée d'une mission de service public et a estimé, en l'espèce, le délit constitué.

Le tribunal a considéré que la loi du 10 juillet 1991 sur le secret des correspondances émises par la voie des télécommunications s'appliquait à "*toutes les communications à distance actuellement connues*" y compris le réseau internet, que la messagerie électronique de l'intéressé à laquelle il n'était possible d'accéder qu'en utilisant son mot de passe était protégée par le secret des correspondances, et que "*l'interception"* incriminée par le code pénal résultait de la *"prise de connaissance par surprise de certains des messages personnels adressés à l'intéressé et contenus dans sa messagerie électronique*". Enfin, le tribunal qui a relevé que l'excuse de bonne foi n'est

---

[47] *: Gaz pal 14 décembre 2000 p 39*

[48] *fav. Lamy Prud'homme actualités, n° 20 novembre 2000 ; def. Transfert.Net "Les prud'hommes adoubent le flicage des mails"*

[49] *: Bul Lamy droit de l'informatique et des réseaux novembre 2000 p 25 et 26*

pas prévue lorsque le délit est commis par une personne en charge d'une mission de service public (à la différence de l'article 226-15 applicable à tout particulier) a estimé que les mobiles étaient indifférents.

Ce jugement a généralement été interprété comme un renforcement de la protection du secret des correspondances émises par la voie de la messagerie électronique. Il convient cependant, à supposer même qu'il soit confirmé en appel, de se montrer prudent dans l'interprétation.

S'il ne fait guère de doute qu'un message électronique relève de la loi du 10 juillet 1991, il ne bénéficie pas pour autant d'une garantie d'absolu secret. La loi de 1991 autorise, en effet, dans certaines circonstances et à certaines conditions, les interceptions ordonnées par l'autorité judiciaire, les interceptions dites de sécurité, et elle ménage, hors le cas dans lequel le fait punissable est commis par une personne dépositaire de l'autorité publique, l'excuse de bonne foi, justification légale de l'interception, qui fait alors tomber l'infraction. Aussi, un employeur peut-il, dans les mêmes conditions juridiques, intercepter un message électronique ou faire procéder à une écoute.

En outre, le point de savoir si la lecture d'un message stocké dans le disque dur de l'ordinateur du salarié ou par un dispositif technique mis en oeuvre au niveau du pare-feu, s'apparente ou non à une "interception" au sens de la loi de 1991 demeure entier. A suivre le jugement de la 17 ème chambre, la réponse paraît être positive, cette juridiction précisant que constitue une interception la "prise de connaissance par surprise".

Mais des décisions existent apparemment en sens contraire. Ainsi, dans un arrêt du 12 décembre 1996, la chambre d'accusation d'Aix-en-Provence[50], dans une affaire, il est vrai fort différente, relative à l'exploitation par les services de police des messages enregistrés par un appareil Tam-Tam, a estimé, sans contester que cet appareil soit un enregistreur de messages acheminés par le réseau de télécommunications, qu'une telle prise de connaissance des messages ne relevait pas des dispositions de la loi de 1991 "*les fonctionnaires de police n'ayant installé aucun branchement, et aucune dérivation pour intercepter des messages*". Cette analyse a été confirmée par la Chambre criminelle de la Cour de cassation dans un arrêt du 14 avril 1999[51] relatif à un appareil de messagerie unilatérale ("tatoo") "*ne saurait constituer une interception de correspondance émise par la voie des télécommunications, au sens de l'article 100 du Code de procédure pénale, les simples lectures et transcription par les policiers, sans artifice ni stratagème, des messages parvenus sur la bande d'un récepteur de messagerie unilatérale*".

*

[50] *: Dr. pén. 998 comm n° 29 et*

[51] **:** *Dr pén 99 comm n° 124 pour un appareil "tatoo"*

En définitive, il résulte de ces quelques décisions que les messages électroniques échangés par des salariés ne sont pas protégés de manière absolue par le secret des correspondances. Ils ne le sont que de manière relative. Et relative à deux égards :

- d'une part, parce que la loi de 1991 ne prive pas un employeur de la possibilité de placer les salariés sous écoute téléphonique, dès lors qu'il peut attester de sa bonne foi,

- d'autre part, parce qu'il est trop tôt pour considérer comme incontestablement établi, compte tenu des termes divergents de la jurisprudence à cet égard, que la lecture d'un mail stocké sur un serveur de messagerie ou sur le disque dur d'un micro ordinateur serait constitutif d'une interception de communication au sens de l'article 226-15 du code pénal.

De surcroît, les premières jurisprudences prud'homales paraissent, en l'état, témoigner d'une sévérité plus grande à l'égard de l'usage à des fins privées des messageries professionnelles qu'à l'égard de moyens plus traditionnels de communication, tels que le téléphone ou le minitel.

Si elle devait se confirmer, faudrait-il déduire d'une telle tendance jurisprudentielle que cette sévérité spécifique à l'internet serait liée à la nouveauté ? Cette question mérite d'être éclairée par une brève étude des pratiques européennes.

Petit tour d'horizon européen

La jurisprudence

. BELGIQUE

Deux décisions du Tribunal de travail de Bruxelles pourraient manifester que nos voisins ont moins de préventions à l'égard d'internet que les Français ou, pour mieux dire, qu'ils appliquent à internet et à la messagerie électronique, la jurisprudence nuancée des juridictions françaises à l'égard d'un usage à des fins privées du minitel ou du téléphone.

Dans une première affaire jugée le 10 avril 1999[52], il s'agissait d'un salarié qui exerçait une activité de travailleur indépendant de revendeur de matériel informatique, en dehors de ses heures de travail, par le biais de sa messagerie professionnelle.

La 16ème chambre du Tribunal de travail de Bruxelles a estimé que l'attitude indélicate et fautive du salarié pouvait justifier une mise en garde, voire un licenciement moyennant un préavis, mais non un licenciement pour faute lourde. La juridiction motivait ainsi son jugement : *"Dès lors en effet, que le nombre des courriers électroniques privés n'est pas déraisonnable compte tenu de l'usage généralement admis - qui en est fait depuis son apparition - et que les activités de Monsieur X en octobre 1997 apparaissent exceptionnelles, le tribunal considère que la faute commise par Monsieur X -dont l'activité et l'assiduité au travail n'ont jamais fait l'objet même à ce jour de la moindre remarque- ne présentait pas un caractère de gravité tel que les relations de travail devaient être rompues immédiatement et définitivement."*

Dans une deuxième affaire[53], il était reproché à l'employé d'une étude d'huissier de justice d'avoir entretenu une abondante correspondance électronique de nature privée avec une de ses collègues. Le Tribunal de travail de Bruxelles a d'abord estimé que les messages échangés entre les deux collaborateurs ressortissaient à leur vie privée, au sens de l'article 8 de la Convention européenne. Puis, il a précisé que le droit à la protection à la vie privée n'était pas absolu *"notamment lorsque cette protection se heurte à des droits opposés tel le droit de contrôle de l'employeur"*, le contrôle peut s'avérer légitime dès lors qu'il est "*nécessaire et indispensable*" et "*proportionnel*".

Le tribunal poursuivait : "*Le fait d'avoir échangé un très grand nombre de messages avec une autre employée de l'étude, par la messagerie électronique interne, ne présente pas le degré de gravité suffisant pour constituer un motif grave. Le tribunal est très fortement influencé dans son appréciation par la circonstance que l'employeur s'est abstenu de tout contrôle sur le travail fourni avant de demander le rapport en janvier 1999, alors qu'il avait confié une tâche qu'il qualifie d'importante à l'employé, tâche à accomplir dans un délai donné, et qu'il disposait de moyens de contrôle puisqu'il avait chargé l'employé de travailler sous l'autorité d'un huissier, lequel était donc normalement en mesure de comprendre le travail de M. X, d'en mesurer l'avancement, et le cas échéant, d'identifier les causes de retard. L'intensité même des occupations extra-professionnelles les rendait perceptibles : l'employeur pouvait ignorer ce que faisait l'employé penché sur son ordinateur, mais il devait constater que celui-ci ne produisait pas ou trop peu. Le tribunal estime que la persistance du laisser faire a réduit la gravité de la faute, en deçà du seuil de gravité nécessaire pour constituer un motif grave"*.

L'intérêt de cette décision est de souligner, avec quelque bon sens, que des salariés ont pu ne pas consacrer la totalité de leur temps de présence à leur travail ou être distraits de leur tâche, avant internet et que cet outil, encore récent, ne saurait conduire à substituer au contrôle normal de productivité la surveillance électronique.

. ESPAGNE

---

[52] *: www.droit-technologie.org*

[53] : *Tribunal du travail de Bruxelles 2 mai 2000 www.droit-technologie.org*

Le Tribunal Superior de Justicia de Cataluña[54] a jugé, dans une décision du 14 novembre 2000, que le licenciement d'un salarié qui avait émis de nombreux messages sans lien avec le travail depuis sa messagerie électronique professionnelle (140 en 5 semaines) était justifié, étant observé que l'entreprise avait adopté un code de conduite interdisant l'usage du courrier électronique à des fins personnelles pendant le temps de travail. Sans se prononcer sur une éventuelle violation de la vie privée du salarié, argument qui n'avait pas été invoqué, les juges se sont bornés à constater que le manquement du salarié tant par son contenu que par sa réitération dans le temps constituait une faute disciplinaire.

Les lois étrangères et les recommandations des autorités européennes de protection des données

- **"Messieurs les Anglais, tirez les premiers !"**

La loi britannique du 24 octobre 2000 autorisant le contrôle des salariés (contrôle des mails échangés sur le lieu de travail) par les employeurs et plus largement le contrôle des communications électroniques par le Gouvernement a fait couler beaucoup d'encre et donné lieu à des interprétations parfois erronées. Il s'agit en fait d'une juxtaposition de textes intervenus pour donner un nouveau cadre juridique à l'interception des communications (télécommunications régulations 2000) et aux pouvoirs d'investigation existant en la matière (Regulation of Investigatory Powers Act 2000), après la condamnation du Royaume-Uni par la Cour européenne des droits de l'homme, (cf supra).

Le RIP Act pose le principe d'interdiction de telles interceptions, sauf dans trois circonstances :

- sur autorisation du Gouvernement pour des motifs de sécurité publique ;

- si les deux parties prenantes ont donné leur accord, par exemple au titre du contrôle de la qualité du service téléphonique d'un centre d'appel ;

- s'il s'agit d'une pratique professionnelle légitime dans un but de contrôle ou de preuve d'échanges professionnels.

Pour autant, et s'agissant du contrôle relatif aux salariés, ces derniers doivent en être informés, contrairement à ce qui a pu être dit ou écrit.

Il est vrai que le Commissaire anglais à la protection des données avait, dès le mois de mars 2000, rédigé une note à l'attention du Parlement et a émis plusieurs remarques sur le projet de loi qui ont été prises en compte dans le texte définitif. Il avait notamment indiqué la nécessité impérieuse d'informer les personnes préalablement à la mise en oeuvre de système de surveillance, et suggéré que le consentement des personnes soit recueilli. Ce dernier point n'a cependant pas été retenu.

---

[54] : *Liaisons Sociales Europe n°22 du 20 décembre 2000*

- **Le Commissaire britanniques à la protection des données personnelles**

En octobre 2000, le Commissaire britannique a mis en ligne sur son site[55], pour consultation publique, un projet de code de conduite couvrant tous les traitements de données pouvant être mis en oeuvre dans le cadre de la relation de travail, depuis le recrutement des candidats jusqu'à la conservation des données relatives aux anciens salariés, en passant par la gestion du personnel y compris la surveillance exercée à leur égard.

Le chapitre 6 de ce projet de code concerne les contrôles effectués sur les salariés. Il y est rappelé que ces contrôles peuvent permettre l'analyse quantitative ou qualitative du travail fourni et d'évaluer le "comportement" du salarié.

Le Commissaire pose en préalable que l'interdiction faite par un employeur d'utiliser la messagerie électronique à des fins personnelles ne relève pas d'un problème de protection des données (aucune disposition relative à la protection des données n'impose, il est vrai, à un employeur d'autoriser un usage à des fins privées de l'outil professionnel). La problématique de protection des données apparaît en revanche lors du contrôle que l'employeur peut exercer pour s'assurer du respect des règles qu'il a fixées. Un tel contrôle, souligne le Commissaire, n'a pas seulement des incidences sur la vie privée ou le comportement du salarié, qui n'a pas à être connu de son employeur, mais doit également être apprécié au regard du fait que l'employé a droit à la confiance de son employeur et à la liberté de déterminer un certain nombre d'actions dans le cadre de son activité professionnelle sans être constamment épié.

Aussi, ce code préconise-t-il l'établissement d'une politique claire de l'entreprise sur les modalités d'utilisation des réseau et le respect du principe de proportionnalité.

Selon le Commissaire, le principe de proportionnalité implique que :

- le contrôle ne soit pas continu mais occasionnel ;
- si le même résultat peut être atteint avec une autre méthode, il convient alors de choisir cette autre méthode ;
- les syndicats soient consultés ;
- les personnes concernées soient informées du but recherché sauf dans des cas exceptionnels (recherche d'infraction, informer nuirait au but recherché) ;
- l'information recueillie au travers du contrôle ne soit pas utilisée pour un motif autre, sauf s'il révèle une activité criminelle ou un manquement important aux obligations du salarié ;
- les employés soient en mesure de s'expliquer sur les éléments constatés compte tenu du fait qu'ils peuvent être tronqués, falsifiés...
- l'espionnage ne saurait être justifié en dehors des cas où une activité criminelle a été identifiée et s'il est établi que les seules preuves possibles ne peuvent être établies que par ce moyen ;
- en outre, dans cette hypothèse, doivent avoir été évalués le risque d'informer les employés et la durée de ce contrôle.

Dans ce contexte, le Commissaire britannique propose :

---

[55] *: www.dataprotection.gov.uk*

- l'établissement d'une charte par l'employeur indiquant clairement les conditions d'utilisation de tous les moyens de communication ;
- d'évaluer le caractère proportionné du contrôle au regard, non pas de l'énoncé de la charte, mais de la pratique effective de l'employeur ;
- de s'assurer que les employés ont bien connaissance des modalités de contrôle ;
- d'analyser l'impact du contrôle sur l'autonomie des employés dans leur vie professionnelle ;
- de prendre en considération le fait que la vie privée ne concerne pas seulement les appels personnels mais aussi professionnels ;

- de se montrer réaliste dans l'appréciation des avantages retirés du contrôle (ainsi, on met souvent en avant le risque de divulgation de secrets d'affaire ou de fabrique qui peuvent être éventés par bien d'autres moyens, d'où la nécessité de justifier le contrôle et de le limiter aux personnes concernées) ;
- à moins que cela ne rende le contrôle inefficace ou que des circonstances particulières le justifient, limiter les contrôle aux données de trafic plutôt qu'au contenu des communications, de procéder à des pointages et non à un contrôle en continu, d'automatiser le contrôle au maximum et de le focaliser sur les zones à risque exclusivement.

S'agissant des connexions à internet, les recommandations britanniques sont les suivantes :

- le contrôle doit être préventif plutôt qu'une surveillance a posteriori ; les moyens techniques de restreindre l'accès sont préférables à la surveillance des connexions ;
- si une utilisation à des fins privées est admise, il n'est pas possible de justifier le contrôle du contenu mais seulement du temps de connexion ;
- faire prévaloir les durées de connexion sur l'analyse du contenu des sites visités ;
- en cas d'utilisation de résultats d'une surveillance des connexions, intégrer la facilité avec laquelle s'effectue la navigation sur internet et qu'il est très facile d'avoir des réponses biaisées de moteurs de recherche, liens hypertexte peu clairs, bannières publicitaires trompeuses... ; certaines connexions peuvent donc ne pas résulter de la volonté manifeste de l'internaute ;
- dans la mesure où les employés peuvent utiliser internet à des fins personnelles, s'assurer que les enregistrements des sites visités et le contenu des pages visualisées n'est pas concerné et si ce n'est techniquement pas possible, informer les salariés de ce qui est conservé et pour quelle durée.

- **La Commission de la protection de la vie privée belge**

La Commission de la protection de la vie privée belge a émis un avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail en date du 3 avril 2000. Cet avis s'articule autour des principes de transparence et de proportionnalité.

La politique de contrôle de l'employeur doit préciser les modalités d'utilisation du courrier électronique et de l'internet, les finalités et les modalités du contrôle de cette utilisation, l'existence d'un stockage des données de télécommunication et la durée de ce stockage, les décisions pouvant être prises par l'employeur à l'endroit de l'employé contrôlé, le droit d'accès de l'employé aux données le concernant.

La proportionnalité et la nécessité impliquent que le contrôle soit ponctuel et justifié par des indices laissant supposer une utilisation abusive des outils de travail, le contrôle ne doit porter que

sur les données nécessaires à ce contrôle, c'est ainsi que la prise de connaissance du contenu des informations n'est pas nécessaire à l'exercice du contrôle.

A cette fin, l'autorité belge recommande d'utiliser des logiciels permettant de cibler les courriers suspects plutôt que de lire tous les courriers. S'agissant du contrôle des connexions aux sites internet, il est recommandé de procéder par liste noire, par temps de connexions avant de s'intéresser aux auteurs des connexions.

- **Le Commissaire néerlandais**

L'autorité de contrôle néerlandaise a publié sur son site internet un rapport sur le bon usage des réseaux[56].

Ce rapport précise que la surveillance systématique de l'utilisation des NTIC est disproportionnée et indique que le salarié fait son travail selon son propre jugement sans pour autant avoir son supérieur constamment dernière son dos ("*without having his boss looking over his shoulder*"). Le Registratiekamer précise également que le mode de contrôle doit être le moins intrusif et propose quelques règles d'ordre général :

- envisager le travail en ligne de la même façon que le travail hors ligne ;
- avoir des règles claires en accord avec les représentants du personnel ;
- publier les règles de façon accessible pour les salariés ;
- déterminer l'usage privé admis et quels sont les logiciels de filtrage utilisés par l'entreprise ;
- rendre impossible les utilisations interdites par un système logiciel ;
- n'avoir que des statistiques anonymes ;
- prendre en considération les données sauvegardées par le système ;
- garantir l'intégrité des responsables du réseau dans l'entreprise ;
- discuter des comportements douteux avec la personne concernée aussi rapidement que possible ;
- évaluer les règles périodiquement ;
- faire en sorte que les messages électroniques professionnels et privés soient séparés, en cas d'impossibilité éviter les messages privés ;
- limiter les contrôles à des objectifs prédéfinis, tels que : l'évaluation individuelle, les fichiers, la protection du réseau, le contrôle des secrets de l'entreprise, la prévention de la publicité négative, le harcèlement sexuel, le respect des accords définissant les usages interdits, évaluer les coûts d'utilisation des matériels ;
- limiter la surveillance autant que possible ;
- limiter l'utilisation des logiciels utilisés pour les messages électroniques et pour le surf sur internet ;
- ne pas conserver les logs plus longtemps que nécessaire soit un mois pour les e-mails et pour les données de connexions au web ;
- éviter les échanges avec les représentants syndicaux et le médecin de l'entreprise.

Il résulte de ce panorama européen des autorités de protection des données de fortes lignes de convergence et un grand souci du pragmatisme.

---

[56] : "Goed werken in netwerken" sur www.registratiekamer.nl

Au moment de conclure...
Des principes et des pratiques

La sécurité informatique dans l'entreprise est un objectif qui doit être partagé et qui ne peut être atteint que dans un climat de loyauté et de confiance réciproque.

Cet objectif ne peut être parfaitement réalisé que si les salariés sont convaincus qu'il n'est en rien contraire à leur intérêt, à leurs droits et à leurs libertés.

A/ La transparence et la loyauté

C'est autour de la confiance, érigée en principe fondateur, que doit se construire la surveillance. L'efficacité est à ce prix pour la meilleure implication des parties prenantes dans l'entreprise. Cette dernière a le devoir de se protéger et ses dirigeants doivent exercer le contrôle de l'exécution du contrat de travail. De leur côté, les salariés ont droit au respect de leur vie privée laquelle ne peut s'arrêter en pratique à la porte de l'entreprise.

La loyauté s'impose en pratique pour établir le point d'équilibre entre droit de l'employeur à connaître ce qui est nécessaire à l'exercice de sa fonction dirigeante et le droit du salarié à protéger sa vie privée dont l'essentiel n'a pas à être exposé dans la relation de travail.

L'établissement du point d'équilibre ne va pas de soi. Il ne peut résulter que d'un compromis dont le débat seul peut inscrire les conditions. En faire l'économie revient à entraver l'implication des salariés. Cette dernière postule la certitude que la sécurité informatique dans l'entreprise ne soit en rien contraire aux intérêts, aux droits et à la liberté des salariés.

L'ignorance des principes ou la précipitation ont guidé la rédaction de chartes éloignées de l'application du principe de confiance.

Certaines chartes d'usage adoptées par des entreprises françaises relatives à l'utilisation par les salariés des outils mis à leur disposition (et notamment, l'accès internet et la messagerie électronique) cumulent, le plus souvent, sans souci de la pédagogie, les prohibitions de toute sorte. Elles avisent de la mise en place d'un véritable arsenal d'outils de surveillance et de la conservation pendant de longue durée des données de connexion permettant l'identification des

agissements des salariés. Pour mieux se garantir encore, certaines entreprises soumettent à la signature des salariés de telles prescriptions, comme s'il s'agissait d'engagements librement consentis par eux. De telles méthodes manquent à leur objectif de sécurité juridique et peuvent même s'avérer tout à fait contre productives.

L'information préalable assurée dans de telles conditions ne priverait nullement le juge de procéder au traditionnel contrôle de proportionnalité entre le manquement reproché au salarié (et qui, à s'en tenir à quelques chartes, est quasiment inévitable) et la sanction prononcée, ni même au contrôle de proportionnalité entre la surveillance ainsi exercée et le respect de la vie privée garanti par l'article 8 de la Convention européenne des droits de l'Homme, et qui ne s'interrompt pas à la porte des entreprises.

De surcroît, le cumul de tant d'interdictions d'usage et de tels avertissements peut être de nature à entamer la productivité des salariés qui ne peut se développer que dans un climat de confiance. Au demeurant, les premières jurisprudences des juridictions de l'Union européenne évoquent les "*usages généralement et socialement admis*" de la messagerie et du web à des fins privées et paraissent admettre, comme les juridictions françaises l'ont fait pour d'autres outils, tels que le téléphone ou le minitel de l'entreprise, un usage à des fins privées dans des limites raisonnables.

B/ Les limites à la mise en oeuvre de la sécurité informatique dans l'entreprise

Devoir éminent de l'employeur soucieux de gérer en "bon père de famille", la sécurité conditionne la pérennité de l'entreprise. Elle peut faire l'objet d'un plan d'ensemble porté à la connaissance des salariés et de leurs représentants dans les instances de l'entreprise.

Les mesures de sécurité informatiques arrêtées dans le cadre d'un plan d'ensemble et qui permettent de conserver trace des flux d'informations dans l'entreprise doivent être exposées de manière claire et précise aux salariés, à leurs représentants et au comité d'entreprise. Cette information préalable, dont la majorité de la jurisprudence française paraît admettre le caractère obligatoire, soit au titre du principe de loyauté, soit parce qu'il s'agit de traitements automatisés d'informations nominatives, constitue en tout état de cause la meilleure prévention possible des abus.

. Lorsqu'un pare-feu est mis en place, associé ou non à d'autres outils, la signification des informations enregistrées et leur durée de conservation doivent être précisées aux salariés.

. Lorsqu'une copie de sauvegarde des messages est effectuée, la durée pendant laquelle les messages sont conservées sur la copie de sauvegarde doit être précisée.

. L'interdiction faite aux salariés de disposer d'une messagerie sur un serveur de messagerie gratuite peut constituer une mesure de sécurité légitime pour l'entreprise, compte tenu des risques (contamination de virus, intrusion, etc).

. De même, l'interdiction faite aux salariés de laisser leur mail professionnel dans des forums de discussion peut, dans certains circonstances, être jugée pleinement justifiée et proportionnée à un objectif de sécurité de l'entreprise.

. Les systèmes de journalisation des connexions destinés à sécuriser l'accès à des fichiers informatiques, et tout particulièrement à ceux qui comportent des données à caractère personnel, sont non seulement légitimes mais indispensables. Les salariés doivent en être informés ainsi que de leurs conséquences, ce qui constitue là encore la meilleure manière de prévenir tout accès non autorisé.

. Les administrateurs de système habilités à avoir accès aux données de connexion doivent être identifiés. En outre, les salariés de l'entreprise devraient être informés des autorités hiérarchiques habilitées à requérir des administrateurs des mesures de surveillance particulières lorsque des dérives de nature à porter atteinte à l'intérêt des entreprises seraient constatées. Dans une telle hypothèse, les règles de procédures, d'information du personnel ou de leurs représentants devraient être précisées.

C/ L'utilisation à des fins personnelles des moyens de communication l'entreprise par ses salariés

Le web et la messagerie focalisent l'attention sur les usages extraprofessionnels des moyens mis à disposition des salariés. La crainte de certains employeurs concerne le risque de détournement par le salarié d'un temps contractuellement dédié au travail. Elle concerne ainsi plus concrètement la crainte de l'attrait de sites particuliers tels les sites pornographiques et les sites de jeux.

S'agissant de l'usage à des fins extraprofessionnelles par les salariés des moyens mis à leur disposition (web, messagerie), il y a lieu d'observer que seule est en cause la crainte de certains employeurs que la diversité de l'offre de contenus sur internet soit de nature à distraire dans des proportions inacceptables le salarié de sa tâche.

Les mêmes craintes ont été exprimées, en France, lors de la montée en charge du minitel. Or, la jurisprudence comme la pratique de la plupart des employeurs témoignent d'une saine tolérance, non exclusive de sanctions en cas d'abus.

Internet est sans doute plus attractif que le minitel, mais la durée de connexion est beaucoup moins coûteuse. S'il est légitime que les salariés soient soumis à des contrôles de productivité ou de qualité de leur travail, de tels contrôles ne sauraient être abandonnés à une implacable et systématique surveillance électronique comme l'a souligné le Tribunal du travail de Bruxelles.

. Navigation sur le web à titre privé

La solution du filtrage de certains sites - bien que n'étant pas parfaitement efficace - paraît préférable à une interdiction absolue et de principe faite aux salariés de naviguer sur le web.

Il devrait être admis, par la plupart des entreprises, que les salariés peuvent se connecter au web au moins hors de leur temps de travail, quitte à ce que soient posées certaines interdictions à l'égard de sites web à caractère particulier (pornographie, négationnisme, jeu, etc).

Dans une telle hypothèse, le contrôle a posteriori de l'usage fait par les salariés d'une telle tolérance peut être légitime. Cependant, un tel contrôle peut être gradué et ne devrait pas porter, sauf circonstances exceptionnelles, sur une analyse individuelle des sites consultés et de leur contenu. Peut être mis en place un contrôle du temps de connexion par poste sans identification des sites consultés, ou encore un contrôle des sites les plus souvent consultés depuis l'entreprise sans ventilation par poste. De tels contrôles dépourvus de caractère nominatif devraient dans la plupart des cas s'avérer largement suffisants. Les salariés devraient en tout état de cause en être informés.

- Utilisation à titre personnel de la messagerie

L'interdiction de principe faite aux salariés d'utiliser la messagerie électronique à des fins non professionnelles paraît tout à la fois irréaliste et disproportionnée.

La sécurité de certaines entreprises particulières peut sans doute justifier que soit opéré un contrôle a posteriori de l'usage des messageries. Mais un tel contrôle doit pouvoir être effectué à partir d'indications générales de fréquence, de volume, de la taille des messages, du format des pièces jointes, sans qu'il y ait lieu d'exercer un contrôle sur le contenu des messages échangés.

En tout état de cause, s'agissant des messages "entrants" (adressés par une personne extérieure à l'entreprise à un salarié sur son lieu de travail), toute indication portée dans l'objet du message et conférant indubitablement à ce dernier un caractère privé devrait interdire à l'employeur d'en prendre connaissance, selon les principes posés par la jurisprudence sur la correspondance postale.

D/ <u>La confiance par l'information et la négociation</u>

La sécurité et l'usage des moyens mis à la disposition des salariés par l'entreprise revêt une dimension nouvelle que la société de l'information amplifie. Les risques pour la sécurité sont accrus par l'avènement de l'information comme matière première principale de l'entreprise et du travail. L'information s'enrichit de l'échange d'interlocuteurs qui la captent et l'enregistrent avant de la remettre en circulation sur le réseau. L'entreprise est un réseau d'informations qu'il convient de protéger.

De son côté, au travail, le salarié dispose de droits et de libertés qui peuvent être encadrés ou restreints, mais ne peuvent être supprimés. Toute restriction ou encadrement doit être proportionné et ne saurait être excessif au regard des nécessités de l'activité professionnelle.

Pour ce qui est de l'utilisation non professionnelle et privée des outils mis à disposition du salarié par l'entreprise, la notion d'usage raisonnable a déjà porté ses fruits aux étapes antérieures de la technologie.

Cela conduit la CNIL à recommander une installation des préoccupations liées aux usages de l'informatique au coeur de la négociation entre les employeurs et les salariés aux différents niveaux interprofessionnels de branches et d'entreprises. Le parti prix de la confiance, pour l'efficacité, implique la discussion éclairée.

La discussion doit se dérouler dans les instances qui existent et déboucher sur le compromis entre les parties.

Le document adopté (charte, code de conduite...) prescrirait de façon détaillée les applications diverses avec leur finalité pour satisfaire au principe de proportionnalité. De ce point de vue, l'entreprise n'est pas uniforme et il convient d'approprier la proportionnalité et la finalité à chaque situation particulière. Toutes n'exigent pas le même degré de sécurité et de surveillance.

L'extrême rapidité de l'évolution des techniques et l'adjonction de fonctionnalités nouvelles doivent conduire à ce que tout accord fasse l'objet d'une mise à jour périodique. A cette fin, on pourrait par exemple envisager que le bilan social de l'entreprise comporte un chapitre dédié au traitement des données personnelles et aux outils de surveillance mis en oeuvre dans l'entreprise.

Enfin, les incidences d'une surveillance électronique sur la vie du salarié dans l'entreprise, sur l'idée qu'il se fait de la confiance qu'on lui accorde et sur l'estime de soi pourraient conduire à conférer une responsabilité particulière, en ce domaine, au comité d'hygiène, de sécurité et des conditions de travail (CHSCT) afin que ces questions puissent être évoquées périodiquement.

A l'heure des nouvelles technologies, la définition d'une politique de sécurité informatique dans l'entreprise révèle, accessoirement mais indubitablement, le sens d'une politique sociale.

I

ELÉMENTS POUR LA PRATIQUE

' Tout document doit être rédigée dans un langage clair et compréhensible.
' Le principe de la politique de sécurité doit être définie et clairement exposée pour être comprise des salariés.
' Il doit clairement indiquer les règles d'usage des ressources mises à la disposition de l'utilisateur.

' Il doit préciser les potentialités techniques des outils et les utilisations effectivement mises en oeuvre, notamment en matière d'utilisation de traces.
' Le document doit être négocié avec les représentants du personnels et faire l'objet d'évocation périodique par les instances de négociation.
' Il devra être régulièrement mis à jour pour tenir compte de l'évolution du parc technologique.

' Si des traitements destinés à mesurer et qualifier l' activité sont mis en oeuvre, les utilisateurs doivent être informés qu'ils disposent d'un droit d'accès (ainsi que de ses modalités) aux informations les concernant issues de ces traitements et doivent connaître la marche à suivre pour exercer ce droit.
' L'utilisation de l'intranet et de la messagerie par les institutions représentatives du personnel sont à définir par un accord spécifique.
' Dans le cas d'intégration au règlement intérieur le respect des formes s'impose : soumission au CE, à l' inspection du travail, au conseil des prud'hommes et affichage dans les locaux.

POLITIQUE DE SÉCURITÉ DE L'ENTREPRISE ET RÈGLES D'USAGE

D’une manière générale l’utilisateur doit s’imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire, sur le harcèlement sexuel/moral.

1) Sécuriser l'accès à votre compte

Le contrôle d’ accès logique permet d’ identifier toute personne utilisant un ordinateur. Cette identification permet, à chaque connexion, l’attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.

Une identification (login + mot de passe) unique est confiée à chaque utilisateur. Ce dernier est personnellement responsable de l’ utilisation qui peut en être faite, et ne doit en aucun cas la communiquer.

Chaque mot de passe doit obligatoirement être modifié selon une fréquence à déterminer. Un mot de passe doit pour être efficace comporter 8 caractères alphanumériques. Il ne doit pas être, notamment, identique au login, même en inversant les caractères, comporter le nom et/ou prénom de l’ utilisateur ou de membres de sa famille, le numéro de téléphone, la marque de la voiture ou toute référence à quelque chose appartenant à l’utilisateur, être un mot ou une liste de mots du dictionnaire ou un nom propre, nom de lieu, être écrit sur un document et être communiqué à un tiers.

2) Le courrier électronique

Les éléments de fonctionnement de la messagerie à considérer sont les suivants :

- Un message envoyé par internet peut potentiellement être intercepté, même illégalement, et lu par n’ importe qui. En conséquence, aucune information stratégique ne doit circuler de cette manière, sauf à la crypter. [*Préciser si cette possibilité est offerte, si oui dire laquelle et comment, si non dire quel mode de transmission utiliser*].

- Il est [*interdit*/*permis*] d'utiliser des services d'un site web spécialisé dans la messagerie.

- Lors du départ d'un collaborateur, il doit être indiqué au responsable de l’administration du système ce qu’ il sera fait des fichiers et courriers électroniques de l’ utilisateur.

‘ - Les messages électroniques sont conservés sur le serveur de messagerie pendant une période de [*n*] jours et il existe des copies de sauvegarde pendant une période de [*n*] jours.

- Ces copies de sauvegarde conservent tous les messages au moment où ils passent sur le serveur de messagerie, même s'ils ont été supprimés ensuite par leur destinataire.

2.1 Utilisation privée de la messagerie

L' utilisation du courrier électronique à des fins personnelles est autorisée dans des proportions raisonnables à la condition de ne pas affecter le trafic normal des messages professionnels.

2.2 Contrôle de l'usage

Dans l'hypothèse la plus courante, le contrôle éventuellement mis en oeuvre porte sur :

- Le volume des messages échangés [*de façon globale/par service/par utilisateurs*].
- La taille des messages échangés.
- Le format des pièces jointes.

3) Utilisation d'internet

Chaque utilisateur doit prendre conscience qu'il est dangereux pour l'entreprise et doit tenir pour acquis ou conditionnel :

- De communiquer à des tiers des informations techniques concernant son matériel.
- De connecter un micro à internet via un modem, [*sauf autorisation spécifique*].
- De diffuser des informations sur l'entreprise via des sites internet.
- De participer à des forums, [*même professionnels*].
- De participer à des conversation en ligne (Chat).

3.1 Utilisation d'internet à des fins privées

L' utilisation d'internet à des fins privées est tolérée dans des limites raisonnables à condition que la navigation n'entrave pas l'accès professionnel.

3.2 Contrôles de l'usage

Dans l'hypothèse la plus courante, le contrôle porte sur :

- les durées des connexion [*de façon globale/par service/par utilisateurs*].
- les sites les plus visités [*de façon globale/par service*]

La politique et les modalités des contrôles fait l'objet de discussions avec les représentants du personnel.

4) Les pare-feu

Le [*les*] pare-feu vérifie[*nt*] tout le trafic sortant de l'entreprise, aussi bien local que distant. Il vérifie également le trafic entrant constitué de [*la messagerie électronique, et/ou l'échange de fichiers, et/ou la navigation sur internet*].

‘ - Il détient toutes les traces de l’ activité qui transite par lui : s'agissant de la navigation sur internet (sites visités, heures des visites, éléments téléchargés et leur nature texte, image, vidéo ou logiciels), s'agissant des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe, [*et éventuellement texte du message*].

‘ - Il filtre les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont : les sites diffusant }{des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes.

5) Les sauvegardes

La mise en oeuvre du système de sécurité [*ne*] comporte [*pas*] de[*s*] dispositifs de sauvegarde des informations [*et/ou*] un dispositif miroir destiné à doubler le système en cas de défaillance.

Ceci implique entre autre que la suppression par un utilisateur d'un fichier de son disque dur n’est pas absolue et qu’ il en reste une copie :

‘ - sur le dispositif de sauvegarde ou miroir,
‘ - sur le serveur,
‘ - sur le proxy,
‘ - sur le firewall
‘ - chez le fournisseur d’ accès.

((((