Chronique droit du travail et TIC

par Jean-Emmanuel RAY

Professeur à l'université Paris I (Panthéon-Sorbonne)

Le but de cette chronique semestrielle (1) est d'informer le lecteur de *Droit social* des évolutions juridiques récentes en matière de TIC (2).

Cette matière en construction, où chacun cherche ses marques mais peut aussi apporter sa pierre, est passionnante à plus d'un titre.

• Elle oblige d'abord le travailliste (3) à sortir de son pré carré et à s'intéresser à des matières généralement bien éloignées de ses préoccupations (droit de la presse, de la communication, de l'informatique) sinon de sa culture : davantage porté vers les sciences sociales, comme de nombreux juristes il garde depuis l'école primaire de cuisants souvenirs des mathématiques, statistiques et autres sciences exactes. Qu'il soit juge (4), universitaire ou praticien, s'il s'aventure sur ces nouveaux terrains il fera donc bien de prendre contact avec des informaticiens (parlant français) ou l'un des cinq cents correspondants aux données personnelles désignés par les entreprises depuis le décret du 20 octobre 2005. Les problèmes auxquels il se heurte car les insolubles font parfois sourire ces spécialistes de la culture de résultat, qui les règlent techniquement en deux minutes (ex. : comment lutter contre les connexions internet illégales, les envois en masse). Mais ils ont la même réactivité, sinon une immense créativité dans des circonstances sensibles où le juriste serait d'une immense prudence.

Nombre de responsables informatiques considèrent en effet ce dernier comme un être au mieux naïf, au pire malfaisant et souvent sournois. Comment expliquer à l'administrateur-réseau d'une grande entreprise, par définition chargé de la sécurité et de la fluidité des systèmes d'information vitaux pour tout le monde, qu'il risque d'être condamné en Correctionnel (5) car il a pris connaissance de courriels qualifiés de « Personnel »… qui n'avaient finalement rien de personnel mais permettaient de faire partir à la concurrence des milliers de données confidentielles ? N'a-t-il pas fait que son devoir face à des risques qui ont décuplé, l'adolescent d'hier, passionné d'informatique et voulant épater ses camarades, ayant été remplacé par de vrais professionnels de l'extorsion de fonds ou de l'espionnage économique ? N'a-t-il pas ainsi protégé des emplois ? En privé, il souligne d'ailleurs que *rien* de ce qui circule dans les NTIC (Nouveaux tuyaux de l'information et de la communication) n'est vraiment confidentiel si on y met le prix ou le temps : du Blackberry des dirigeants qui transite par le service central américain au courriel amoureux des collaborateurs, qui prennent pourtant soin de mettre à la poubelle leurs envois les plus compromettants. Mais si la poubelle est effectivement vide *à l'écran*, la trace de leurs frasques subsiste ailleurs : il suffit, comme avant, de « faire les poubelles ». Un directeur des systèmes informatiques (DSI) est d'ailleurs le premier à ne rien écrire de vraiment confidentiel ou d'intime sur son ordinateur ou dans un courriel professionnel : le traçage et la mémoire étant inhérents à l'outil, tout le monde peut se mettre un jour à l'écoute de tout le monde (6).

Le travailliste doit parfois même sortir du Code du travail : ainsi des fort délicates questions posées par les sites syndicaux internet (cf. cour d'appel de Paris, 16 juin 2006) ou par les blogs de salarié ou d'ex-salarié (tribunal correctionnel de Paris, 16 octobre 2006 (7)), où s'appliquent la loi pour la confiance dans l'économie numérique du 21 juin 2004, mais aussi le très dérogatoire droit de la presse.

• Si au siècle dernier (8), les non-juristes parlaient volontiers du fameux « vide juridique », voire d'Internet comme d'une « zone de non-droit » peuplée de sympathiques outlaws un peu turbulents, depuis le 11 septembre 2001 au niveau mondial, et les attentats de Madrid puis de Londres au niveau européen, nous sommes au contraire confrontés à un trop plein.

— Trop plein de toutes provenances : ratification en mai 2006 de la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 (9) voulant construire « une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale », avec les deux décrets du 23 mars 2006. Mais aussi textes en provenance de Bruxelles : nombreuses « directives Télécom », directive du 12 juillet 2002 dite « Vie privée et communications électroniques » (10), entre autres. Et peut-être, dans quelques années, adoption de celle relative « *au traitement des données à caractère personnel et à la protection de la vie privée des travailleurs dans le contexte professionnel* » (11).

Même si elle est pour l'instant dénuée de toute valeur juridique en droit *interne* (12), la charte des droits fondamentaux de l'Union contient non seulement un intéressant article 7 (« *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* »), mais également un plus novateur article 8, spécifique à « *la protection des données à caractère personnel* (13) » domaine d'aujourd'hui aussi essentiel que méconnu, sinon méprisé car mal connu. Comme le remarquait Alex Türk, président de la CNIL le 3 novembre 2006, « *les règles de protection des données protègent des personnes, et leur droit à ne pas être fichées, surveillées, contrôlées de façon incontrôlée* ». Et d'ajouter que ce thème n'a rien d'abstrait, malgré une double invisibilité toujours croissante : *virtuelle* d'abord car des millions d'informations qui, il y a vingt ans, représentaient plusieurs dizaines de kilos de papier peuvent être envoyés en deux secondes à l'autre bout du monde. Invisibilité *réelle* ensuite car les micro caméra-vidéo par exemple ont la dimension d'une punaise ; et entre les clefs USB, les nouveaux portables et autres Ipod Nano, la miniaturisation devient telle que leur propriétaire les égare régulièrement : heureusement pour le portable, un autre téléphone permettra de le géolocaliser grâce à sa si personnelle sonnerie.

Soulignant la difficulté de son rôle alors que les lois antiterroristes se multiplent dans tous les pays (14) sous la pression de l'opinion publique, avec un effet de contagion sinon de perroquet (« Nos voisins font beaucoup mieux » : cf. la vidéo-surveillance à Londres permettant en 2007 d'y filmer un piéton 220 fois par jour), Alex Türk constatait l'ambivalence du progrès technique, parfois aussi utilisé de façon totalement différente de celle prévue (15) par ses concepteurs.

— Trop plein de toutes natures : soft (charte à laquelle l'arrêt du 21 décembre 2006 (n° 3003-FD) donne une valeur proche du réglement intérieur, à propos d'un cadre??? utilisé le code d'un autre salarié pour accéder au poste de direction de la société : « ce comportement, contraire à l'utilisation de respect de la charte informatique en vigueur dans l'entreprise,???? maintien dans l'entreprise » (faute grave)), semi-hard (convention collective, règlement intérieur), hard (loi pour la confiance dans l'économie numérique…), voire très hard côté entreprise : ainsi des sanctions pénales manifestement disproportionnées édictées par la loi du 6 août 2004 refondant la loi Informatique et Libertés de janvier 1978 : 300.000 euros et cinq ans d'emprisonnement pour des crimes aussi abominables qu'envoyer le dossier personnel d'un collaborateur dans un pays non reconnu comme Safe Harbour, ou encore avoir surpris grâce à une caméra de vidéo-surveillance bien visible une vendeuse en train de voler ; mais le système ayant été déclaré à la CNIL comme destiné à lutter contre les vols opérés par les *clients* : collecte illicite *et* détournement de finalité.

• Les NTIC ont enfin induit de nouvelles technologies *juridiques* : ainsi du « Tout Partenaires Sociaux » concernant le télétravail. C'est en effet l'accord national interprofessionnel du 19 juillet 2005 qui a transposé l'emblématique accord européen du 16 juillet 2002 voulant tenir à distance la Commission et le Conseil. Grande première pour la France, comme le rappelle le préambule de cet ANI pour une fois *unanime* : « Les signataires expriment leur volonté de donner une traduction concrète à l'approche nouvelle du dialogue social européen que constituent les accords volontaires. Elles entendent ainsi privilégier la voie conventionnelle pour transcrire (16) en droit interne les textes européens ».

Mélange explosif vie professionnelle/vie privée

L'achat d'un ordinateur équipé Microsoft XP *professionnel* réserve quelques surprises : y sont automatiquement pré-installés plusieurs dizaines de jeux de tous niveaux, du flipper sonore hyperréaliste aux jeux de cartes les plus divers. Sur les portables ou les mobiles professionnels, il est fréquent que la page d'accueil fasse apparaître un splendide bébé ou l'amoureux du moment, et que leur mémoire soit embouteillée de vidéos aussi lourdes que personnelles. La fameuse « convergence » permise par les DTIC (dernières TIC : le Web mobile, c'est-à-dire accéder à ses courriels à partir du portable) conduit ainsi à un joyeux mélange au sein du PDA ou du Smartphone, véritable mini-ordinateur de poche : des rendez-vous, courriels et plans tout à fait professionnels y voisinent avec des musiques, courriels, photos très personnelles.

« Business together » annonce Orange (17). Qu'il s'agisse du télétravailleur à domicile ou de travail en réseau mondial, l'arrivée du très haut débit et les performances nouvelles des ordinateurs permettent enfin de réellement surfer, et non plus de ramer entre deux décrochages internet comme à la fin du siècle dernier, après l'interminable ouverture de la page d'accueil. L'arrivée de l'Internet mobile (18) va renforcer cette tendance à l'imbroglio : s'il fallait hier déjà trouver un ordinateur, puis pouvoir se connecter à Internet, les appareils de troisième génération (3G) et le Wifi installé partout permettent aujourd'hui de rester en contact avec l'entreprise, les collègues et les clients, toujours et partout (19) : « Always on, 24/7 ».

Nous vivons une époque formidable (20).

Temps du juge et temps d'Internet

• « *Le temps technologique accélère sans cesse* (21), *tandis que le temps juridique reste lent, régi par le rythme des procédures démocratiques* » remarquait fin 2006 le président de la CNIL, cette autorité administrative indépendante désormais dotée de pouvoirs quasi-juridictionnels en matière d'investigations ou de sanctions. Avec ses possibilités de démultiplication à l'infini associée à des consultations ou envois quasi-gratuits et immédiats dans le monde entier par un simple clic, Internet défie le juriste, et le temps du juge n'est plus celui de la Toile (22).

Comme le montrait une étude du site legalis. net (23) de septembre 2005 (24), s'agissant des seuls contentieux liés aux NTIC, le juge de *l'urgence* qu'est le TGI statuant en référé rend son ordonnance dans un délai moyen de 43 jours : 28 jours à Paris, 73 en province avec de forts écarts-types. Dans l'affaire *Secodip-CGT* jugée le 15 juin 2006 par la cour d'appel de Paris à propos d'un site syndical ayant mis en ligne des informations confidentielles (voir *Droit social*, mars 2007), l'assignation en *référé* datait du *23 novembre 2004* et le jugement du TGI, finalement au fond, est intervenu le *11 janvier 2005*. La concurrence a donc largement eu le temps de faire son marché parmi la précieuse moisson d'informations mises en ligne. Même si la vicime peut ultérieurement agir au fond en responsabilité, le mal est fait : délais difficilement compatibles avec ce qu'attend le demandeur pour faire cesser un trouble *manifestement illicite*, trouble pouvant se *propager* dans le monde entier littéralement à la vitesse de l'éclair.

• D'où la multiplication en ce domaine de mécanismes en forme de privilège du préalable, transformant le demandeur en défendeur. Deux exemples.

— Site *intra*net syndical : le nécessaire accord collectif donnant accès aux NTIC de l'entreprise prend désormais soin de préciser qu'il ne s'agit en aucun cas d'un équivalent des panneaux papier légalement obligatoires, sur lesquels toute intervention patronale unilatérale est constitutive du délit d'entrave au droit syndical. Puis le même article autorise la direction, en cas de contenu délictueux ou d'illicéité mais aussi d'abus, à supprimer purement et simplement la page litigieuse, voire à suspendre provisoirement l'accès au site lui-même : sanction discrète, rapide, efficace et sans recours au juge. Ce sera le cas échéant au syndicat n'acceptant pas cette atteinte à sa liberté d'expression d'agir en justice ; s'il saisit le juge des référés, il devra tout d'abord démontrer que le retrait conventionnellement prévu constitue un trouble *manifestement* illlicite.

Il n'a pas échappé au lecteur de *Droit social* qu'en liant l'accès des syndicats aux systèmes d'informations de l'entreprise à la signature d'un accord collectif, la loi du 4 mai 2004 a mis l'employeur dans une confortable position de négociation : s'il craint d'éventuels débordements à l'occasion d'un conflit collectif dur ou d'une rude bataille électorale, il est en mesure d'imposer ce type de sanction rapide et efficace… pour les sites intranet. Et si en réaction, le syndicat crée un site internet ?

— S'agissant de site syndical *internet*, pouvant être consulté du monde entier par les salariés du groupe, mais aussi par la concurrence et les journalistes très friands de ces informations venant de l'intérieur, la loi pour la confiance dans l'économie numérique du 21 juin 2004 oblige son hébergeur, après mise en demeure de l'entreprise visée estimant que ce site lui porte un grave préjudice, à retirer immédiatement la page contestée, voire d'empêcher l'accès au site tout entier s'il ne veut pas voir engagée sa responsabilité (25).

Cette forme de justice privée peu regardante sur la liberté d'expression a évidemment de multiples avantages côté entreprise (26) : exceptionnelle rapidité, coût pour le moins réduit, et surtout remarquable discrétion, qui réduit à néant les tactiques de sites au nommage ou au contenu délibérément provocateurs pour qu'une assignation les sorte enfin de leur anonymat. Car il faudra beaucoup de témérité et/ou de redoutables juristes spécialisés à un hébergeur (français) pour refuser de suspendre un site ou quelques pages de celui-ci : en termes de gestion raisonnable des risques juridiques, le retrait s'impose s'il existe la moindre probabilité d'être ensuite civilement condamné.

Là encore, il reviendra au syndicat s'estimant injustement censuré de saisir la justice *au fond* pour obtenir réparation, au titre d'une bien banale responsabilité contractuelle client/hébergeur. Car à moins que ce dernier n'ait cédé à une objurgation sans aucun fondement, le « SAMU de la justice » qu'est le juge des référés ne pourra que bien rarement ordonner la réouverture du site au titre du trouble *manifestement* illicite causé par sa fermeture.

Plus généralement en ce domaine nouveau, chacun tâtonne (employeur, salarié, syndicaliste, juge, universitaire), chacun s'interroge sur la place du curseur. Mais a aussi le sentiment de participer à l'élaboration de cette branche d'un droit en devenir, lui aussi tâtonnant sinon parfois surprenant, mais essentiel pour l'avenir de notre société quand on prend conscience des changements majeurs que les TIC ont apportée depuis dix ans à notre vie quotidienne, professionnelle et personnelle.

Avec la redoutable ambivalence des TIC, ces braves tuyaux « d'information et de communication ».

TIC, tuyaux et communication moyen-âgeuse

1. Au quotidien, le *courriel* permet à des expatriés d'échanger quotidiennement photos et nouvelles avec leur famille restée en France ; pour nos seniors esseulés, les photos et textes ainsi envoyés sont un bonheur quotidien. Dans les entreprises, il permet un miracle que personne n'aurait imaginé il y a vingt ans : la diffusion quasi-gratuite d'informations à l'autre bout du monde, ou un travail collaboratif entre ingénieurs habitant aux quatre coins de la planète, avec une exceptionnelle réactivité.

Mais hélas aussi, le courriel mal utilisé est une véritable plaie moderne. Au-delà du spamming (plus de la moitié des flux mondiaux sur Internet), l'avalanche permanente de courriels au bureau devient source

d'exaspération ; car la plupart d'entre eux ne sont pas directement destinés à leur récipendaire mais permettent à l'expéditeur de montrer qu'il travaille beaucoup, ou de se couvrir si l'affaire tourne mal. Nombre de cadres en particulier ne supportent plus ce harcèlement courriel qui finit par littéralement les submerger, tout étant désormais qualifié d'urgent au détriment de l'important. Sans parler de ces collègues ne se parlant plus que par voie électronique alors qu'ils sont à 50 mètres l'un de l'autre : communication du XXI[ème] siècle mais indigne du Moyen-Âge sur le plan des relations humaines comme de l'efficacité. « Communiquer » avec les TIC ne signifie pas se comprendre ni être compris : rien ne peut remplacer le face à face.

Même ambivalence avec PowerPoint, qui permet parfois des présentations plus attractives et dynamiques que les vieux transparents. Mais aboutit le plus souvent à une succession saccadante sinon exaspérante de documents que l'intervenant lit mot à mot, avec nombre de petites astuces techniques et virevoltantes destinées à monter son savoir-faire, mais qui font littéralement « perdre de vue » son discours.

2. Si l'on prend plus de hauteur, la recherche du « 22 à Anières » a certes disparu ; et pour les travailleurs *du savoir* la forte sub/ordination taylorienne comme l'obligation de moyens du droit du travail d'hier s'éloignent à grands pas. Mais les mêmes salariés n'ont jamais connu une aussi contraignante sub/organisation (27), peuvent être désormais suivis à la trace dans leurs moindres déplacements physiques (géolocalisation) comme au moindre clic sur les autoroutes de l'information, ont du mal à se déconnecter intellectuellement des dossiers en cours (28), grâce aussi à la connexion internet très haut débit que leur entreprise leur a gracieusement fournie pour leur domicile.

Voilà qui nous oblige à un travail de vrai juriste : réfléchir sur la société dans laquelle nous voulons vivre, ces choix engageant nos enfants.

Sera traitée dans le présent numéro la question centrale pour le travailliste (29) de la cybersurveillance (I) ; les blogs (II) et autres Intranet et Internes syndicaux (III) seront abordés dans le prochain numéro.

I. — CYBERSURVEILLANCE APRÈS LES ARRÊTS DU 18 OCTOBRE 2006

Quelle vraie différence, nous dit-on, entre le contremaître d'hier et la caméra vidéo d'aujourd'hui ? Le contrôle des salariés par cet œil électronique diffère-t-il vraiment de l'œil humain (30) ? En quoi un autocommutateur est-il vraiment différent de la chef de service vérifiant que les secrétaires ne passent pas leur temps au téléphone ? L'employeur qui se voit aujourd'hui refuser le droit d'ouvrir les courriels personnels pouvait-il hier ouvrir les lettres roses et parfumées arrivant au service Courrier, avec au dos « Facteur, dépêche-toi, l'amour n'attend pas » ?

Existe-t-il une spécificité TIC en matière de surveillance ?

À l'évidence oui, pour au moins trois raisons.

1. Le contremaître modèle Boulogne-Billancourt ne pouvait « être partout, tout le temps ». Les logiciels de contrôle du courriel, des communications téléphoniques comme de géolocalisation (31), souvent pré-installés, enregistrent systématiquement *car automatiquement toutes* les actions du collaborateur, virtuelles (connexions internet) ou réelles (14 h 57 : arrêt de la voiture du commercial sur le parking du client… ou d'un hôtel).

2. Si l'appareil est en réseau, cette surveillance ne nécessitant aucun effort particulier et non soumise aux charges sociales peut se faire aussi facilement du sous-sol de la tour de La Défense qu'à 4 700 km de distance, par exemple à partir d'un pays n'appartenant pas à l'UE pour éviter le droit communautaire. Il est même à tout moment possible – facile – de prendre le contrôle de n'importe quel ordinateur en temps réel, toujours de l'autre bout du monde sans que son titulaire ne comprenne vraiment ce qui se passe. Chacun sait que « l'informatique » a le dos fort large (32).

3. Dépourvu du don d'ubiquité et souvent tenu à des micro-négociations bien humaines, notre brave agent de maîtrise avait aussi une mémoire limitée, malgré ses fiches bristol au bureau et son carnet à spirales dans la poche droite. La collecte automatisée des informations n'est jamais perdue : l'ordinateur les garde en mémoire, mais peut aussi les envoyer automatiquement à un service central qui a une mémoire… d'ordinateur.

Si bien sûr, cette surabondance d'informations semble renvoyer G. Orwell et son Big Brother à la Bibliothèque rose, et alimente les fantasmes les plus divers (un nouveau détecteur de fumée devient une mini-caméra cachée), son abondance même la rend globalement difficilement utilisable malgré les nombreux logiciels *ad hoc*. Mais s'il s'agit de cibler un collaborateur en particulier…

La *cyber*surveillance ? Ni tout à fait la même, ni tout à fait une autre.

A — UN DROIT, MAIS AUSSI UN DEVOIR

La cybersurveillance n'est pas seulement un droit dans le cadre de l'exécution du contrat *de travail* caractérisé par la subordination : c'est un devoir pour l'employeur-commettant ne voulant pas s'exposer trop facilement à la recherche de sa responsabilité (33) et à des condamnations à des dommages-intérêts (34), importants en France et punitifs aux États-Unis, du fait des frasques de l'un de ses préposés ayant envoyé des courriels discriminatoires ou très gaulois. C'est ce qu'a rappelé le 13 mars 2006 la cour d'Aix-en-Provence approuvant le raisonnement du TGI de Marseille (35) : « *Sur la responsabilité de la société Lucent Technologies (LT) en sa qualité d'employeur de Nicolas B.*

Il n'est pas contesté que le site litigieux a été réalisé sur le lieu de travail grâce aux moyens fournis par l'entreprise, Nicolas B. ayant pour fonction d'effectuer des

tests de qualité et de fiabilité du matériel fabriqué, et ayant utilisé le matériel mis à sa disposition à cette fin.

Une note du DRH en date du 13 juillet 1999 précise que les salariés peuvent utiliser les équipements informatiques mis à leur disposition et les accès réseau existants pour consulter d'autres sites que ceux présentant un intérêt en relation directe avec leur activité au sein de la société LT, dès lors que ces utilisations restent raisonnables, s'effectuent en dehors des heures de travail, et respectent les dispositions légales régissant ce type de communication et les règles internes à la société, l'accès à des sites à caractère explicitement sexuel et contrevenant aux valeurs de LT étant prohibé.

Ainsi la libre consultation des sites internet était autorisée, et aucune interdiction spécifique n'était formulée quant à l'éventuelle réalisation de sites internet ou de fourniture d'informations sur des pages personnelles.

Il y a donc lieu de constater que la faute de N.B. a été commise dans le cadre des fonctions auxquelles il était employé, et de déclarer la société LT responsable sur le fondement de l'article 1384, alinéa 5 ».

Sans doute, et comme souvent aujourd'hui en matière de TIC, ces décisions de première instance puis d'appel ne doivent pas se voir accorder l'importance d'un arrêt publié – voire mis en ligne *sur Internet*, le nec plus ultra – de la Cour de cassation. Mais la Deuxième Chambre civile avait rendu un arrêt tout aussi sévère le 19 juin 2003, à propos d'un agent d'assurances dont l'employée avait commis divers détournements grâce aux moyens informatiques (faux sinistres, paiement de ses dettes personnelles) pendant son temps de travail et dans les locaux professionnels. La cour de Lyon avait cru pouvoir affirmer que de tels actes avaient été commis hors fonctions puisque le matériel utilisé était directement fourni par la compagnie d'assurances, et que le logiciel ne permettait pas à l'employeur de contrôler les activités de sa salariée: elle avait donc mis le commettant hors de cause. Réponse cassante: « *La préposée avait agi au temps et au lieu de travail à l'occasion des fonctions auxquelles elle était employée, avec le matériel mis à sa disposition, ce qui excluait qu'elle ait commis ses détournements en dehors de ses fonctions* (36) ».

B — CYBERSURVEILLANCE ET PREUVES: L'ARROSEUR ARROSÉ

« Si l'employeur a le droit de contrôler et de surveiller l'activité de son personnel durant le temps de travail, il ne peut mettre en œuvre un dispositif de contrôle qui n'a pas fait l'objet, préalablement à son introduction, d'une information et d'une consultation du comité d'entreprise. Le système de vidéo-surveillance de la *clientèle* mis en place par l'employeur étant également utilisé pour contrôler les *salariés* sans information et consultation préalables du comité d'entreprise, les enregistrements du salarié constituaient un moyen de preuve illicite ».

L'arrêt du 7 juin 2006 (37) est tout à fait représentatif du *contentieux* en matière de cybersurveillance. Faute de n'avoir pas respecté l'une des quatre phases de mise en place d'un système de contrôle (information individuelle préalable (38); information et consultation préalable du comité d'entreprise (39) comme en l'espèce et demain sans doute du CHSCT au delà de sa???? propre au cas d'introduction de nouvelles technologies; déclaration à la CNIL (40) en cas de collecte de données personnelles, ce qui ici est toujours le cas; et enfin sur le fond, vérification de la conformité du contrôle à L. 120-2), ou *a fortiori* violé une interdiction (ouverture d'un courriel titré personnel), l'employeur voit sa preuve frappée d'inopposabilité. Comme souvent c'est la seule dont il dispose…

— De plus en matière disciplinaire, le doute profite au salarié. Et le doute en matière de TIC…

Cour de Metz, 14 décembre 2004 (41): « Il ne peut être exclu qu'un des collègues de M. X partageant le même bureau, dont l'un d'entre eux entretenait des relations conflictuelles avec l'intéressé, ait pu accéder aux données de son ordinateur, soit en ayant connaissance du code d'accès, soit que le titulaire du poste de travail informatique ait laissé celui-ci en fonctionnement durant son absence du bureau ».

Cour de Douai, 17 décembre 2004 (42): « Le dispositif ne permettant aucune ventilation nominative selon l'utilisateur concerné, auquel un mot de passe aurait été par exemple attribué, l'abus de M. Z. ne peut être établi ».

Cour de Rouen, 3 mai 2005 (43): « Rien ne permet de dire que ces téléchargements et les sites pornographiques consultés par lui et référencés sur l'ordinateur soient imputables à Éric D. Ce dernier n'était pas le seul utilisateur de l'ordinateur, mis à la disposition de toute personne ayant accès à la ludothèque: usagers, personnel et membres du conseil d'administration. À cet égard, le fait que ces téléchargements aient été classés dans un dossier « Éric », prénom de Éric D. n'est pas une preuve dans la mesure où il n'existait aucune sécurité, faute d'un code d'accès, personnel à chaque usager ».

— Mais parfois aussi, c'est la banale application des principes du Code civil qui conduit à la perte du procès côté entreprise. Ainsi de l'employeur invoquant une faute *grave*, comme c'est souvent le cas à la fois en raison du caractère intolérable de la faute, mais aussi pour éviter la question du préavis: il lui revient alors de la prouver.

D'où parfois de curieuses mais fructueuses coïncidences: cadre passant par là et très surpris par l'affichage sur l'écran de photos pornographiques; « faits découverts de manière fortuite, à la suite d'un incident technique sur le réseau informatique nécessitant l'installation d'un logiciel de maintenance » (cour administrative d'appel de Douai, 27 septembre 2006 (44)) ou le retour des bonnes vieilles???, ????? involontaire de courriels ou???? gauloises (CS 21 décembre 2006, n°3048-FD).

La chambre criminelle n'écartant pas automatiquement des preuves obtenues dans des conditions pour le moins créatives (45), des entreprises passent par la saisine du procureur (cour de Montpellier, 17 mai 2006 (46): « expertise du disque dur sur enquête diligentée par le procureur de la République (47) ») *ou* portent l'affaire devant le juge pénal pour lier ensuite le juge prud'homal (48). À l'inverse, la seconde chambre civile a rejoint fin 2004 la chambre sociale et l'arrêt fondateur *Néocel* du 20 novembre 1991 (49). Au visa de l'article 9 du NCPC et article 6 de la CESDH, les juges civils avaient estimé le 7 octobre 2004 que « *l'enregistrement d'une conversation téléphonique privée, effectuée et conservée à l'insu de l'auteur des propos invoqués, est un procédé de preuve déloyal rendant irrecevable en justice la preuve ainsi obtenue* ».

• Nécessaire loyauté de la preuve… au prix de l'impunité? Les juristes en général, et les juges en particulier dont le métier s'articule autour de procès, ne doivent pas penser que la technique juridique soit l'alpha et l'oméga de la régulation sociale. Au sein de l'entreprise, il reste bien étrange que tel collaborateur qui a escroqué son employeur ou consulté des sites pédophiles soit blanchi par la justice civile car la preuve apportée n'a pas été acceptée.

La Cour de cassation *belge* a ainsi reviré par l'arrêt du 2 mars 2005; une vendeuse surprise par une caméra vidéo en train de se servir dans la caisse, est licenciée. Elle invoque la convention collective n° 68, la caméra ayant été installée à son insu. La Cour de cassation avait en effet en juin 2004 écarté ce mode de preuve jugé illicite, mais les juges de la Cour de renvoi résiste et la Cour de cassation a finalement reviré: le juge belge peut désormais décider de ne pas écarter la preuve en motivant sa décision notamment sur la gravité de l'infraction, les soupçons légitimes de l'employeur, et le fait qu'aucune formalité prescrite à peine de nullité n'a été violée (50).

La loi britannique « Lawful Business Practice Regulations » entrée en application le 24 octobre 2000 assortit pour sa part l'interdiction de prendre connaissance des courriels privés de cinq exceptions la remettant en cause. L'entreprise peut en effet prendre connaissance du courriel si:

— il s'agit d'une communication de travail (et par définition, du bureau…),

— il s'agit de la conclusion d'un contrat,

— le système informatique nécessite une opération de maintenance,

— pour éviter ou contrer des interventions non autorisées,

— pour veiller à une utilisation licite du circuit ».

• Comme le rappelait le rapport de la CNIL sur la cyber-surveillance du 5 février 2002 (51) « *Première idée fausse: l'ordinateur personnel mis à disposition des utilisateurs sur le lieu de travail relèverait de la vie privée du salarié* (52) mais on passe la frontière devenu que les arrêts du 18 octobre 2006, la somme divise commune aux courriels et aux fichiers? ».

Dans l'affaire jugée par la cour d'appel de Versailles le 2 avril 2003 (53), l'employeur avait exigé la restitution immédiate du portable professionnel (54); et malgré les protestations du salarié lui ayant fait remarquer qu'il contenait également des dossiers personnels (dont sa thèse), l'avait ouvert en présence d'un huissier et y avait trouvé les preuves de la création d'une société concurrente, avec le site internet destiné à la promouvoir. Mais l'ayant fait « sans restituer au préalable au salarié qui en faisait la demande ses *fichiers* personnels, l'employeur a commis une violation du droit au *secret des correspondances*: le mode de preuve étant illicite, le licenciement de M. X. est dénué de cause réelle et sérieuse ».

C — COURRIELS PERSONNELS ET COURRIELS PROFESSIONNELS

De par leur caractère hybride, les courriels posent de fort délicates questions. Rédigés dans un style oral, sur un support virtuel rarement crypté, ils sont *techniquement* accessibles à tous et donc n'importe qui, et souvent reproduits sur papier: or ce simple changement de support peut à lui seul réserver quelques surprises. Outre l'orthographe souvent très créative, un adjectif un peu fort mais acceptable dans une conversation à mails rompus devient sur support papier diffamatoire ou injurieux, une mauvaise astuce ou la signature amusante du boute-en-train du service une faute grave même si la chambre sociale sait faire la part du feu (Cass. soc. 21 décembre 2006, n° 3040-FD, à propos d'un cadre ayant envoyé à ses collaborateurs un courriel « contenant une expression orale »; ni faute grave, ni cause réelle et sérieuse). Sans parler du « syndrome du gros doigt » « erreur d'adressage » ou là encore, la chambre fait preuve de compréhension « erreur de manipulation » par un salarié ayant 42 ans d'ancienneté, absence de cause réelle et sérieuse, CS 21 décembre 2006, n° 3018).

Sous un fort prestigieux visa (« *Vu l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, l'article 9 du Code civil, l'article 9 du nouveau Code de procédure civile et l'article L. 120-2 du Code du travail* »), l'arrêt *Nikon* du 2 octobre 2001 (55) avait voulu poser le principe du respect de la vie privée au bureau: « *Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée (56); celle-ci implique en particulier le secret des correspondances; l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* ».

Et dans une magnifique unanimité malgré (ou à cause de?) la complexité de la question, les juges du fond (57) mais également les inspecteurs du travail (58) ont suivi comme un seul homme la doctrine *Nikon*

(59). Formulation reprise intégralement par la chambre sociale le 12 octobre 2004 :

« *Vu l'article 8 de la CESDH, l'article 9 du Code civil l'article 9 du NCPC et l'article L. 120-2 du Code du travail.*

Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée, celle-ci impliquant en particulier le secret des correspondances. L'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à disposition pour son travail, ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur.

Pour décider que la mise à pied disciplinaire de Mme R. était justifiée, la Cour d'appel a notamment retenu que la salariée avait entretenu une correspondance avec une ex-salariée de l'entreprise au moyen de la messagerie électronique, pendant son temps de travail, avec le matériel de l'entreprise.

Pour établir ce comportement, elle s'est fondée sur le contenu des messages émis par la salariée, que l'employeur avait découvert en consultant l'ordinateur mis à la disposition de celle-ci par la société. En statuant ainsi, elle a violé les textes susvisés ».

• Seuls les courriels qualifiés de « *Personnel* » bénéficient donc de la protection jurisprudentielle : n'importe quel courriel ne peut se prévaloir du régime de la correspondance privée, comme l'a d'abord rappelé la Commission Nationale Informatique et Libertés dans son rapport 2004 (p. 21).

Confirmation prévisible par le Conseil constitutionnel, dans sa décision du 10 juin 2004 « Loi pour la confiance dans l'économie numérique » destinée entre autres à lutter contre le spamming :

« *Sur la définition du courrier électronique :*

Considérant qu'aux termes du dernier alinéa du IV de l'article 1er de la loi déférée : « On entend par courrier électronique tout message, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère »*;*

Considérant que cette disposition se borne à définir un procédé technique; qu'elle ne saurait affecter le régime juridique de la correspondance privée; qu'en cas de contestation sur le caractère privé d'un courrier électronique, il appartiendra à l'autorité juridictionnelle compétente de se prononcer sur sa qualification ».

Et dans son arrêt du 25 octobre 2000, la chambre criminelle a rappelé que « *les annonces émises ne peuvent avoir le caractère d'une correspondance privée* » si elles sont « *diffusées à des personnes indifférenciées : leur contenu ne peut par définition être personnel* ».

• Mais il revient donc *in fine* au salarié de qualifier ses courriels, comme d'ailleurs l'arrêt du 18 octobre 2006 visant les dossiers l'y incite. Il n'est pas certain que la différence dossier/courriels ait été vue par les juges : dans l'affaire *Nikon*, les courriels de M. O. avaient par exemple été rangés dans un *dossier* : « la Cour d'appel s'est fondée sur le contenu de messages émis et reçus par le salarié, que l'employeur avait découverts en consultant l'ordinateur mis à la disposition de M. Onof par la société *et comportant un fichier intitulé « Personnel »*). Or l'entrée et la sortie de courriels font l'objet de contrôles automatiques, ce qui n'est pas toujours le cas de dossiers entièrement créés sur place, et qui n'ont plus besoin des circuits informatiques de l'entreprise pour en sortir (disquette hier, clef USB aujourd'hui).

• Comment résoudre cette quadrature du cercle : protéger les courriels personnels couverts par le secret de la correspondance (bien qu'il s'agisse plutôt de cartes postales virtuelles), tout en permettant à l'employeur d'en limiter les éventuels abus ?

— La CFDT (60) propose « *la mise en place d'une boîte aux lettres personnelle (persopdurand@entreprise.fr) à côté de la boîte aux lettres professionnelle (pdurand@ entreprise. fr), sur le même Intranet d'entreprise, qui offre une solution pertinente pour répondre aux besoins de confidentialité des messages et de respect de la vie privée dans l'activité professionnelle* ». Mais les directions d'entreprise ne souhaitent guère montrer une aussi grande tolérance à l'égard des activités personnelles au bureau, même s'il n'est pas impensable de se servir de cette boîte personnelle pendant les pauses ou après le travail. Par ailleurs les courriels en question renvoient malgré tout à l'adresse de *l'entreprise*, créant ainsi un gros risque de réputation (cf. l'arrêt *Spot Image* à propos de courriels antisémites envoyés à un client israélien (61)) sinon de responsabilité civile, voire désormais pénale si l'auteur en est un organe ou un représentant.

— Autre solution proposée, pour éviter aussi que certains juges du fond voient des courriels personnels partout (62) : l'obligation, figurant au règlement intérieur pour être opposable (63), de titrer *obligatoirement* ce type de courriel « Privé » ou « PRV (64) ». Si l'employeur ne peut alors en prendre connaissance, il pourra le cas échéant tout de même s'étonner du *nombre* d'envoi de cette nature, de leur *volume* et/ou de celui des éventuelles *pièces jointes*.

Dans les deux arrêts visant le *courriel*, l'article L. 120-2 était cité *in fine*. Mais son principe de conciliation pas du tout utilisé, contrairement aux arrêts du 17 mai 2005 et du 18 octobre 2006 relatifs aux *dossiers* « identifiés comme personnels par le salarié ».

D — FICHIERS OU DOSSIERS PERSONNELS (Cass. soc. 17 mai 2005/Cass. soc. 18 octobre 2006)

Le secret des correspondances n'est plus ici en cause. Mais la *summa divisio* professionnel/personnel reste la même, au nom du nécessaire respect de la vie privée.

Il est très pédagogique que deux arrêts aient été rendus le 18 octobre 2006 : l'un portant sur des dossiers

électroniques, le second arrêt sur l'ouverture par l'employeur de documents papier.

• Dans le bureau d'un nouveau collaborateur, son supérieur trouve des liasses entières de documents très confidentiels provenant de son employeur précédent. Immédiatement licencié pour faute lourde, il conteste la rupture : pourquoi l'employeur a-t-il mis le nez dans ses affaires, lui étant en plus absent lors du constat d'huissier ? « *Les documents détenus par le salarié dans le bureau de l'entreprise mis à sa disposition sont, sauf lorsqu'il les identifie comme étant personnels, présumés avoir un caractère professionnel, en sorte que l'employeur peut y avoir accès hors sa présence* » : faute grave.

• Le second arrêt du 18 octobre 2006 (65) applique logiquement la même règle aux dossiers *électroniques* :

« Attendu que M. L. F. a été engagé le 2 octobre 2000 par la société Techni-Soft en qualité d'attaché technico-commercial ; que le 28 février 2002, il a été licencié pour faute grave ayant notamment consisté à empêcher l'accès à ses dossiers commerciaux sur son poste informatique de travail […].

Attendu que le salarié fait grief à l'arrêt attaqué d'avoir dit son licenciement fondé sur une faute grave, en violation de l'article L. 122-14-3 du Code du travail ;

Mais attendu que les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence ». Comme les bons vieux classeurs multicolores du millénaire dernier logique.

• S'agissant au contraire des dossiers *électroniques* qualifiés de *personnels*, l'arrêt du 17 mai 2005 (66) a maintenu le principe de l'interdiction de la fouille surprise, mais avec deux importantes limites.

1. L'employeur peut ouvrir le disque dur « *de l'ordinateur mis à disposition du salarié* » (bref, la propriété de l'entreprise) « *en présence de ce dernier ou celui-ci dûment appelé* ». Pour tenter d'éviter toute provocation ou insertion de dossiers compromettants, l'ouverture – parfois liée à des codes qu'il est le seul à connaître – doit donc en principe se faire en sa présence.

Mais cela ne signifie pas que l'accord du salarié en cause soit requis : s'il est « dûment appelé » mais refuse d'y participer, l'employeur peut, après s'être ménagé des preuves de cette convocation, faire procéder à l'ouverture des fichiers en question avec l'aide d'un spécialiste de l'informatique s'il veut éviter de se ridiculiser devant le juge (voir par exemple Cass. de Paris, 4ème ch. B, 17 novembre 2006, Sté Net Ultra c./ Aol France à propos d'un constat où l'hussier se voyait reproché d'avoir capturé une page figurant dans la mémoire d'un serveur proxey).

2. Reprenant presque mot pour mot l'arrêt du 11 décembre 2001 (67) visant l'ouverture d'armoires personnelles, en cas « de risque ou d'événement particuliers » la Cour de cassation permet donc à l'employeur de prendre connaissance de dossiers personnels sans la présence de celui-ci, ni même dûment prévenu.

Comme l'on devine l'enthousiasme des salariés en question, conviés à assister à l'ouverture de leurs dossiers personnels, voire à les ouvrir eux-mêmes (problème des codes d'accès, et des manipulations destinées à les faire disparaître (68)), la question essentielle devient alors la définition de cet *événement*, ou de *ce risque* particuliers.

Et c'est là que le bât blesse : s'agissant du contrôle des sacs personnels à l'entrée de l'entreprise – et donc forcément *en présence* de l'intéressé – l'arrêt *M6* du 3 avril 2001 (69) avait évoqué des « circonstances *exceptionnelles* », à l'époque tout à fait réelles et sérieuses (menaces terroristes).

Dans l'arrêt du 17 mai 2005, la découverte de cinquante photos érotiques dans le tiroir du salarié ne permettait pas, selon la Cour, d'ouvrir le disque dur hors la présence de l'intéressé, disque où avait été pourtant trouvé « *un ensemble de dossiers totalement étrangers à ses fonctions figurant sous un fichier intitulé « perso »* (70) ».

Cette analyse est peut-être de nature à rassurer ceux qui craignaient un excessif mouvement de balancier en réponse à l'arrêt *Nikon* : un « risque particulier » reste donc exceptionnel, comme nous le rappelle d'ailleurs le Littré : « *Risque : péril dans lequel entre l'idée de hasard ; cf. l'expression : à ses risques et périls* ».

Plus généralement, l'ouverture du disque dur et la lecture des dossiers *identifiés comme personnels par le salarié* ne peut constituer qu'une *ultima ratio*.

L'urgence est donc le premier critère à retenir : lorsque l'employeur ne peut attendre la présence du salarié comme en cas de commission de très graves délits pénaux (ex : menaces terroristes, pédophilie, proxénétisme). Hypothèses limites où il vaut évidemment mieux se tourner vers le procureur de la République et la justice pénale, ou commencer par s'en ouvrir auprès des nouveaux « correspondants cybercriminalité », policiers spécialisés présents dans les plus importants commissariats. L'extrême complexité technique et procédurale du droit probatoire en matière de TIC incite en effet l'employeur à ne pas se lancer dans des opérations aussi risquées, mais à se placer comme victime d'une infraction pénale afin de ne pas un jour risquer de passer pour complice, la chambre criminelle n'écartant pas automatiquement des preuves obtenues dans des conditions pour le moins créatives (71).

La prudence la plus élémentaire invitait déjà les collaborateurs avisés à ne pas laisser dans leur disque dur des données vraiment personnelles, voire touchant à l'intimité de leur vie privée (72).

E — CRYPTAGE ET MOTS DE PASSE DES COURRIELS ET DOSSIERS PROFESSIONNELS

Comme le rappelait encore la CNIL dans son rapport de février 2002, « *l'ordinateur mis à la disposition du salarié peut être protégé par un mot de passe ou un log-in, mais cette mesure de sécurité est destinée à éviter les utilisations malveillantes ou abusives par un tiers* (73)*: elle n'a pas pour objet de transformer l'ordinateur de l'entreprise en un ordinateur à usage privé* ».

• Position de bon sens reprise *in fine* par le même arrêt du 18 octobre 2006: « Jérémy L.F. avait volontairement procédé au cryptage *de son poste* informatique sans autorisation de sa société, faisant ainsi obstacle à la consultation: la Cour d'appel a pu décider que le comportement du salarié, qui avait déjà fait l'objet d'une mise en garde au sujet des manipulations sur son ordinateur, rendait impossible le maintien des relations contractuelles pendant la durée du préavis et constituait une faute grave ».

— Le 23 mai 2006, la cour de Besançon (74) avait également confirmé la faute grave d'une comptable ayant modifié son mot de passe juste avant son départ en vacances: « Mme X. ne pouvait ignorer qu'en agissant ainsi, elle risquait de paralyser le fonctionnement de l'association durant son absence, en mettant la présidente dans l'impossibilité d'accéder aux documents comptables et d'établir les bulletins de paye ».

— Dans son arrêt du 21 décembre 2006 (n° 3003 FD) la chambre sociale confirme la faute grave d'un directeur technique ayant « par emprunt de mot de passe d'un autre salarié, tente de se connecter sur le poste informatique du directeur de la société ».

Comme son nom l'indique, un code *d'accès* vise avant tout à limiter à certaines personnes l'accès (75) à des données ou des dossiers (ex.: plusieurs niveaux d'Intranet); certains ordinateurs de série sont d'ailleurs aujourd'hui fournis avec un système biométrique de reconnaissance de l'empreinte digitale de son propriétaire (76). Dans l'entreprise, un cryptage semble d'ailleurs indispensable pour le médecin du travail dont, secret médical oblige, les dossiers ne doivent être accessibles que de lui seul: il vaut toujours mieux protéger les *données* que limiter les *accès*.

Mais un salarié modifiant le code qui lui a été confié sans en informer au minimum le responsable informatique peut créer d'énormes retards. Entre les RTT, les congés et les arrêts-maladie, interdire ainsi à un employeur d'aller immédiatement chercher dans l'ordinateur d'un collaborateur le dossier d'un client grand compte revient à perdre ce dernier. Même s'agissant d'un salarié en congé-maladie, la chambre sociale veille donc à l'exécution de bonne foi du contrat de travail: « *La suspension du contrat de travail provoquée par la maladie, si elle dispense le salarié de son obligation de fournir sa prestation de travail, de telle sorte qu'il ne saurait être tenu de poursuivre une collaboration avec l'employeur, ne dispense pas le salarié, tenu d'une obligation de loyauté, de restituer à l'employeur qui en fait la demande les éléments matériels qui sont détenus par lui et qui sont nécessaires à la poursuite de l'activité de l'entreprise* » (Cass. soc. 6 février 2001 (77)). Et le 18 mars 2003, la même chambre sociale avait rappelé à une salariée en arrêt maladie qu'elle devait communiquer son mot de passe informatique à son employeur. Alors que la Cour d'appel avait estimé qu'un tel refus « ne pouvait être reproché sérieusement à une salariée se trouvant en arrêt-maladie, qui par ailleurs ne pouvait se trouver la seule détentrice de ce mot de passe »; cassation: « Le juge devait rechercher si l'employeur avait effectivement la possibilité, sans recourir à la salariée, d'avoir communication du mot de passe informatique, et si de ce fait, la salariée n'avait pas eu la volonté de bloquer le fonctionnement de l'entreprise ». Aux « éléments matériels » de l'arrêt de 2001 la Cour ajoute donc: « le salarié n'est pas dispensé de communiquer à l'employeur qui en fait la demande, les *informations détenues par lui* et qui sont *nécessaires à la poursuite de l'activité de l'entreprise* ».

Personnel ou professionnel? Entre le volumineux ordinateur de bureau d'hier et le petit mais plus puissant portable d'aujourd'hui ne quittant jamais son bénéficiaire, y compris pour les week-ends et pendant les vacances, le problème est évidemment plus compliqué, et il le sera encore davantage demain lorsque tout téléphone mobile sera devenu un « mini-ordi »: bien vieille question juridique que les rapports possession/propriété ■