



L'impact des NTIC sur le contrat de travail

publié le **23/09/2013**, vu **20951 fois**, Auteur : [Adrien LANCIAUX](#)

Etude de l'impact des NTIC sur la relation contractuelle de travail.

Sommaire

Titre 1. Les NTIC, instruments de gestion du contrat de travail

Chapitre 1. Les NTIC et la conclusion du contrat de travail

Chapitre 2. Les NTIC et l'évolution du contrat de travail

Titre 2. Les NTIC, instruments de contrôle du salarié

Chapitre 1. Un contrôle opéré au sein de l'entreprise

Chapitre 2. Un contrôle opéré en dehors de l'entreprise

Liste des abréviations

ADN : Acide désoxyribonucléique

ANI : Accord national interprofessionnel

Art. : Article

Bull. Civ. : Bulletin civil

CA : Cour d'appel

Cass.crim : Cour de cassation chambre criminelle

Cass.soc : Cour de cassation chambre sociale

CE : Comité d'entreprise

CEDH : Convention européenne des droits de l'Homme

CESDH : Convention européenne de sauvegarde des droits de l'Homme

Chbre : Chambre

CHSCT : Comité d'hygiène de sécurité et des conditions de travail

CIL : Correspondant informatique et liberté

CNIL : Commission nationale de l'informatique et des libertés

CPH : Conseil des prud'hommes

DDHC : Déclaration des droits de l'Homme et du citoyen

Délib. : Délibération

D.H : Droit hebdomadaire

Dr.soc : Droit social

DUDH : Déclaration universelle des droits de l'Homme

IRP : Institution représentative du personnel

JCP : JurisClasseur périodique

JCP E : JurisClasseur périodique Édition Entreprises et affaires

JCPS : JurisClasseur périodique Édition Sociale

J.O : Journal officiel

NTIC : Nouvelles Technologies de l'information et de la communication

OIT : Organisation internationale du travail

Ord. : Ordonnance

PUF : Presse universitaire de France

RDT : Revue de droit du travail

Rec: Recueil

RJS : Revue de jurisprudence sociale

Synd. : Syndicat

TIC : Technologie de l'information et de la communication

TGI : Tribunal de grande instance

USB : *Universal Serial Bus*

Web : Toile

Propos introductifs

« Les progrès technologiques ont indéniablement été plus rapides ces soixante dernières années que durant tout le développement humain. Or, l'intelligence artificielle se développe à une telle vitesse que d'aucuns se demandent si elle ne finira pas par dépasser l'intelligence humaine. Et

dès lors, ce serait la fin théorique de la domination du genre humain^[1]. »

L'étymologie du mot technologie renvoie au mot grec « Tekhnologia^[2] » lui-même composé des mots tekhnê « art », et logos « l'étude ». A l'origine, la technologie est donc l'étude des arts, de la technique. Depuis l'usage du premier outil, l'Homme n'a eu de cesse que d'améliorer sa technique et d'inventer de nouveaux moyens de production dans le but de se faciliter la tâche. On aura en tête les travaux d'Adam Smith^[3] qui a montré que le travailleur était l'un des premiers créateurs d'innovation. En effet, cherchant à développer sa productivité et à limiter ses efforts, le travailleur en contact direct avec sa tâche était le mieux à même de trouver des améliorations. Aujourd'hui, les innovations sont le plus souvent le fait de grands laboratoires financés par un budget spécifique dédié à la recherche et au développement.

Aujourd'hui, les nouvelles technologies de l'information et de la communication (NTIC) désignent les « *moyens matériels et les organisations structurelles qui mettent en œuvre les découvertes et les applications scientifiques les plus récentes*^[4] ». Pour l'administration, les « nouvelles technologies » doivent être entendues dans un sens large. « *Elles portent sur toute mesure d'automatisation, d'informatisation, de robotisation affectant les méthodes de gestion, de fabrication ou de production, ou encore toute mesure prise en matière d'audiovisuel, de biotechnologie*^[5] ». Elles constituent une innovation majeure au sein de l'économie. Or, le progrès technique constitue l'un des moteurs essentiels de la croissance économique, et donc de l'évolution de l'emploi et des rapports de travail. C'est Joseph Aloïs Schumpeter qui a montré que l'économie était rythmée par des cycles, eux-mêmes impulsés par l'apparition des innovations qui apparaissent en « grappe ». La réussite d'un entrepreneur entraînerait les autres dans son sillon, conduisant à une modification de l'organisation du travail. Selon Schumpeter, il convient de distinguer trois types de cycles. Les cycles courts dits « Kitchin » (5 ans), les cycles moyens ou « Juglar » (10 ans) et les cycles longs dits « Kondratieff » qui seraient d'une durée de 40 à 60 ans. Ces derniers apparaîtraient lors des très grandes innovations^[6]. Nous serions depuis les années 1990 dans un cycle impulsé par les technologies de l'information et de la communication, lequel devrait durer jusque 2020. Il est important de noter que chaque cycle est marqué par une période de croissance, de stagnation, et de récession. La période économique actuelle montre que l'Ecole économique néo Schumpétérienne est toujours d'actualité. Notre économie est en phase de destruction d'emploi. Les activités obsolètes disparaissent, et un nouveau cycle se prépare. Celui-ci devrait être marqué par les biotechnologies, la robotique, et par l'économie « verte ». Si on peut certes s'interroger sur l'existence des cycles économiques, pour lesquels certains affirment qu'ils n'existent pas^[7], on ne peut remettre en question le lien entre progrès technique et croissance économique. Selon l'INSEE, « *les nouvelles technologies contribuent fortement à la hausse de la productivité des entreprises. Les innovations techniques et l'ouverture à la concurrence remodelent progressivement les économies développées. Leurs effets ont d'abord été visibles aux États-Unis : l'expansion des années 90 trouve, pour une large part, son origine dans le déclin rapide du prix de l'informatique et le développement des nouvelles technologies de l'information et de la communication*^[8] ». Partant, celles-ci ont modifiés considérablement les modes de production, de management, et de contrôle des salariés. Dans les années 2000, l'assemblée parlementaire du Conseil de l'Europe appelait « *les États membres à prendre la mesure des mutations que les NTIC ont engendrées, de leurs effets sur la vie de l'entreprise et sur la vie du travailleur, et à veiller à ce que leur développement ne se fasse pas au prix d'un abaissement des protections dont il doit bénéficier tant au niveau de ses conditions de travail que de sa vie privée*^[9] ».

Les technologies de l'information et de la communication (TIC) sont apparues par vagues successives. La première d'entre elles a été guidée par l'apparition de l'ordinateur. Ce dernier, entraînant le remplacement de l'homme par la machine, et l'automatisation des tâches, a eu des

conséquences importantes sur l'emploi. Déjà à l'époque, les notions de compétence et de formation étaient primordiales pour que le salarié maintienne ou développe son employabilité. La seconde vague de TIC a été marquée par l'émergence de nouveaux moyens de contrôle du salarié (autocommutateur, caméra). Le modèle de l'autonomie organisationnelle du salarié porté par les entreprises Toyota et Volvo s'est vu minoré par un retour à une surveillance poussée de la productivité, et des faits et gestes du salarié. La vague actuelle de TIC se caractérise par la dématérialisation du travail et le Web 2.0. Sur le premier point, on voit se développer de façon importante le recours systématique aux courriels électroniques, et au décloisonnement du travail. Là où ce dernier représentait une sphère clairement professionnelle, il est aujourd'hui facile d'emporter des travaux chez soi, sans même parler du télétravail. Un grand nombre de cadres se trouvent ainsi en permanence connectés, de sorte que les frontières entre vie privée et vie professionnelle sont de plus en plus floues. Si elles ont permis d'alléger la charge de travail, et de libérer le salarié des tâches répétitives, les TIC posent la question du respect de la vie privée. Sur le second point, le Web 2.0 correspond au phénomène de simplification d'internet. Les utilisateurs ne sont plus simplement passifs, ils sont également acteurs. Ils ont aujourd'hui la possibilité d'échanger sur le Web, de partager des informations et de communiquer de façon instantanée par le biais des réseaux sociaux.

Pour les entreprises, les nouvelles technologies sont une source de gains de productivité importante. Confrontées à une forte concurrence, elles doivent s'adapter, et intégrer ces nouveaux outils. Leur présence dans les entreprises est aujourd'hui essentielle. Sans cela, ces dernières seraient incapables de gérer l'ensemble des informations utilisées. On pense ici aux tâches effectuées par le biais d'un "télétraitement" (la gestion des stocks, la comptabilité, la paie), mais aussi toutes les utilisations d'Internet (commerce électronique, recherche de fournisseur) et de l'Intranet d'entreprise (Intranet de gestion des ressources humaines), ou encore au recrutement par internet. Au sein de l'entreprise, les NTIC recouvrent également la téléphonie mobile, l'ordinateur, les logiciels, Internet, mais aussi la géolocalisation, la vidéosurveillance, les réseaux sociaux, ou encore la biométrie. Leur introduction dans le monde du travail a poussé le législateur et la jurisprudence à imposer des règles, visant à éviter tout abus dans l'utilisation de ces nouveaux moyens mis à la disposition des employeurs et des salariés. Face à l'apparition des TIC, le législateur n'est que très peu intervenu, si ce n'est pour préciser l'obligation de consulter les institutions représentatives du personnel (IRP) lors de la mise en place de moyens de contrôle, ou lors de tout projet important ayant pour but d'introduire des NTIC dans l'entreprise, ainsi que pour encadrer le télétravail. Le reste des règles en vigueur s'appuie sur des normes internationales, constitutionnelles ou légales préexistantes ayant fait l'objet d'une adaptation par la jurisprudence. Il n'existe pas de branche du droit du travail dédiée aux NTIC. Si le Droit du travail est mouvant, les technologies le sont encore plus, de sorte que légiférer en la matière serait particulièrement difficile. Face au renforcement des moyens mis à disposition de l'employeur, la jurisprudence s'affaire à renforcer les droits des salariés en ayant recours à des concepts fondamentaux tel que l'article 9 du Code civil sur le droit à la vie privée, et l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales qui consacre le droit à une vie familiale normale. La dispersion des règles, et les évolutions continues font de ce sujet une source d'études continue et infinie.

Si le Droit à la vie privée est au cœur du développement des TIC, d'autres questions se posent. Il existe un certain conflit d'intérêt entre les impératifs de l'entreprise, et les conditions de travail des salariés. Ce conflit permanent façonne ce qu'on appelle « les rapports de production^[10] », ou rapport de travail. En effet, « *si les nouvelles technologies ont potentiellement le pouvoir [...] de libérer du temps pour les salariés et de les soulager des tâches hier chronophages, il s'avère qu'il n'en est rien. Elles n'ont fait que véhiculer des rythmes encore plus rapides que les salariés doivent « dominer » mais qui sont le plus souvent subis^[11]* ». Au-delà des modifications de

l'économie, les NTIC ont un impact permanent sur les rapports de travail (individuels et collectifs), et plus particulièrement sur le contrat de travail. Celui-ci est communément défini comme la réalisation d'une prestation de travail en contrepartie d'une rémunération, sous la subordination d'un employeur. C'est ce dernier critère qui prédomine la qualification ou non d'une relation de travail salarié, et donc de l'application de la législation relative au droit du travail. Auparavant, la Cour de cassation considérait que le lien de subordination était un lien juridique qui tirait sa source du contrat^[12]. Les décisions jurisprudentielles récentes tendent à montrer que ce n'est plus tant le lien juridique qui conduit à la reconnaissance d'une relation de travail, mais les « *conditions de fait dans lesquelles est exercée l'activité des travailleurs* »^[13]. La subordination a été définie par l'arrêt Société Générale du 13 novembre 1996 dans lequel les hauts magistrats énoncent que « *le lien de subordination est caractérisé par l'exécution d'un travail sous l'autorité d'un employeur qui a le pouvoir de donner des ordres et des directives, d'en contrôler l'exécution et de sanctionner les manquements* »^[14]. Or, la subordination est directement impactée par les évolutions technologiques. Autrefois, le contrôle de l'employeur se faisait directement et physiquement sur le lieu de travail. Le développement de nouvelles formes d'organisation, tel que le télétravail, pose à nouveau la question de l'exercice de l'autorité. L'évolution conduirait à « *diluer* »^[15] le lien de subordination juridique. Le modèle évolue vers une initiative plus poussée du salarié, s'accompagnant en parallèle d'un contrôle qui s'opère « *continûment et parfaitement à des attentes* »^[16]. On assiste à un certain brouillage des limites spatio-temporelles impliquant la nécessité d'une évolution du critère de la subordination.

La question qui est alors légitime de se poser est de savoir comment les NTIC modifient elles la relation contractuelle de travail ?

Il est possible de voir dans les NTIC la possibilité pour l'humain de s'affranchir des contraintes physiques. L'introduction de l'informatique n'a-t-elle pas diminué le nombre de salariés soumis à une forte pénibilité au travail ? Le développement du télétravail n'est-il pas une chance de réduire l'impact écologique des déplacements quotidiens de millions de salariés ? N'est-il pas la chance pour l'homme de concilier plus facilement vie privée et vie professionnelle ? Les TIC interviennent avant même l'exécution du contrat de travail. D'une part, leur émergence a modifié la recherche d'emploi, en offrant un panel de supports bien plus important que par le passé. D'autre part, les méthodes de recrutement ont été étoffées par de nouveaux moyens offerts au recruteur. Par ailleurs, d'autres éléments fondamentaux du contrat peuvent être impactés. Le Droit du travail s'est construit sur le modèle de l'unicité de temps et de lieu de travail. On a tous en tête l'image des manufactures du XIX^{ème} siècle. Le travail s'exécutait alors à un même endroit sur des horaires déterminés. Aujourd'hui, ces critères sont de moins en moins pertinents en raison de l'apparition d'autres modes d'organisation du travail, tel que le télétravail, qui viennent battre en brèche les notions de temps et de lieu de travail. Les NTIC sont aussi source d'une évolution rapide des moyens de production. Par conséquent, la notion de qualification et d'employabilité des salariés sont au cœur de cette problématique. Au vu des impacts importants engendrés par les NTIC sur la conclusion et l'exécution de la relation contractuelle, il est possible d'affirmer qu'elles sont devenues un instrument de gestion du contrat (Titre 1). On constatera qu'en matière de conclusion et d'exécution du contrat, le Droit tend à être perméable aux évolutions technologiques. Il n'en va pas de même en matière de contrôle du salarié.

En la matière, l'employeur se voit *a priori* renforcer ses prérogatives par un important arsenal de moyens technologiques permettant de tracer le salarié dans l'exécution de ses tâches. Partant de ce constat, le renforcement du pouvoir de l'employeur ne se fait-il pas au détriment de l'équilibre de la relation contractuelle, que la jurisprudence et le Code du travail s'affairent à réaliser en faveur de la partie économiquement plus faible ? « *L'utilisation du concept de bonne foi dans les relations individuelles de travail, en tant que fondement à la sanction de certaines attitudes manifestement déloyales, puis en tant que fondement à la reconnaissance d'obligations encore plus riches et plus novatrices à l'égard tant de l'employeur que du salarié permet non seulement*

de moraliser une relation par essence inégalitaire, mais ce recours à la bonne foi a également pour effet de revaloriser la relation de travail, voire de l'humaniser [17] ». L'introduction même de certaines technologies visant à encadrer et à surveiller les salariés n'est-elle pas en elle-même une certaine atteinte à la bonne foi ? Comment instaurer une relation de confiance, lorsqu'aujourd'hui les relations salariés-employeurs se bâtissent sur la méfiance ? L'ouvrier dans la manufacture française du XVIIIème siècle bénéficiait d'une grande autonomie dans l'exécution de ses tâches. La révolution industrielle a conduit à une certaine déqualification de la main d'œuvre, de sorte que le contremaître est lentement passé d'un rôle de coordination, à un rôle de surveillance. Puis ce fût le retour de la valorisation du travail de groupe, et de l'autonomie, avec l'apparition du Toyotisme[18] dans les années 1990. Aujourd'hui, si les NTIC permettent indéniablement de favoriser l'accomplissement du travail pour les salariés, elles sont également un facteur de soumission.

Les nouvelles doctrines de management venant du Japon tel que le « lean management », vont de pair avec la volonté d'encadrer et de contrôler l'ensemble du processus productif. On assiste au développement du « management par le stress ». D'après Daniel Cohen, « *hier l'emploi était intégrateur. Les grandes entreprises industrielles offraient la promesse d'une promotion à tous les niveaux de la hiérarchie. Les ouvriers pouvaient espérer devenir contremaîtres, les contremaîtres cadres... Aujourd'hui, les firmes cherchent à être lean [...] Elles externalisent les emplois vers leurs sous-traitants, vidant ceux-ci des protections implicites qu'elles donnaient auparavant à leurs travailleurs* [19] ». On peut s'interroger sur le maintien de telles pratiques, à l'heure où la volonté de lutter contre les risques psychosociaux est omniprésente, et où la Cour de cassation se montre de plus en plus encline à retenir le harcèlement moral. Par ailleurs, là où le contrôle de l'employeur s'arrêtait auparavant aux portes de l'entreprise, il s'exerce aujourd'hui en dehors de l'entreprise, avec une certaine immixtion dans la vie privée du salarié. Les NTIC peuvent alors être apparentées à un véritable instrument de contrôle du salarié (Titre 2).

Titre 1. Les NTIC instruments de gestion du contrat de travail

On entend par outil de gestion la possibilité pour l'employeur de faire varier ses possibilités tant au niveau de la conclusion du contrat, qu'au niveau de son exécution. Ces domaines apparaissent particulièrement perméables aux NTIC, et subissent d'importantes évolutions. La conclusion du contrat de travail (Chapitre 1) se trouve modifiée par de nouveaux supports de recrutement permis par l'émergence des nouvelles technologies, mais également par de nouvelles formes d'organisation du travail. Si les TIC peuvent intervenir dès la conclusion du contrat, elles peuvent également intervenir au cours de l'exécution du contrat. En cela, elles sont une source importante d'évolution du contrat de travail (Chapitre 2).

Chapitre 1 : Les NTIC et la conclusion du contrat

Les nouvelles technologies impactent le contrat de travail avant même que celui-ci ait été conclu. La toile a permis de mettre les individus en contact beaucoup plus facilement que par le passé. Les employeurs ont saisi cette opportunité afin de mettre en ligne leurs offres d'emplois non pourvues. Les technologies de l'information et de la communication leur permettent de bénéficier de nouveaux supports de recrutement (Section 1). Elles sont aussi la possibilité de proposer un nouveau type d'organisation du travail dès l'embauche, par le biais du recrutement en télétravail (Section 2). Si ce mode d'organisation reste faiblement utilisé en France, il connaît un développement important.

Section 1. Les NTIC et les nouveaux supports de recrutement

La publication d'offres d'emploi par le biais de supports numériques tend à devenir le principe.

Internet apparaît comme un nouvel espace de rencontre entre l'offre d'emploi, et la demande d'emploi. En témoigne l'éruption d'un certain nombre de réseaux sociaux à but professionnel (Linkedin, Viadeo etc.). Dans ces cas bien précis, on peut aisément parler d'E-réputation contrôlée. En effet, un individu qui s'inscrit sur ces sites va chercher à diffuser une image positive de sa personne, publiant des informations choisies par lui-même. Ces nouveaux espaces de rencontres professionnelles sont rapides, souples, mais ils n'en sont pas moins soumis aux exigences légales qui régissent le recrutement (Paragraphe 1).

Pour autant, l'émergence des réseaux sociaux personnels, où l'on y compte sa vie privée, et la googlisation de l'individu, permettent aux recruteurs de disposer d'informations complémentaires (souvent relevant de la vie privée). On peut ici parler d'E-réputation subie, car s'il est possible de veiller à ce que son compte soit paramétré de telle sorte à ne laisser transparaître aucune information privée, et/ou compromettantes, rien ne permet d'empêcher un « ami » malveillant de publier des photos ou des vidéos auxquelles il aurait eu accès. Par ailleurs, il est particulièrement difficile de contrôler le référencement des sites de recherches (Google par exemple), sur lesquels les individus peuvent se retrouver bien malgré eux. Sur ce point, rien n'interdit formellement à un recruteur de rechercher des informations sur un candidat *via* le web. Les réseaux sociaux, et plus généralement l'internet, semblent être une zone privilégiée pour les « chasseurs de tête » qui bénéficient d'un certain vide juridique (Paragraphe 2) dans un espace volatile et immatériel.

Paragraphe 1. De nouveaux supports de recrutement soumis aux exigences légales

Les nouvelles méthodes de communication - au titre desquelles les réseaux sociaux acquièrent une importance croissante - constituent un espace privilégié de par le nombre important de personnes visée, mais également de par la rapidité de la prise de contact. Cela explique en partie que l'offre d'emploi est de plus en plus diffusée par des moyens électroniques. Ces nouvelles méthodes de publication n'en sont pas moins soumises aux principes régissant la publication d'une offre d'emploi (A). Il en va de même des principes régissant le recrutement (B).

A. Les principes régissant la publication d'une offre d'emploi

Le support numérique d'une offre d'emploi ne peut conduire à déroger aux règles qui régissent la matière. L'article L.5331-1, alinéa 1er, du Code du travail énonce « *qu'il est interdit de vendre des offres ou des demandes d'emploi, quel que soit le support utilisé* ». L'alinéa 2 du même article prévoit cependant que « *cette interdiction ne fait pas obstacle à l'insertion, à titre onéreux, d'offres ou de demandes d'emploi dans une publication ou un autre moyen de communication payant* ». La Commission nationale informatique et liberté (CNIL), sur le fondement de la loi du 1^{er} janvier 1978, prohibe les publications d'offres d'emplois fictifs dans le but de créer un fichier de *curriculum vitae*[\[20\]](#).

Par ailleurs, le contenu d'une offre d'emploi doit respecter un certain nombre de règles impératives, qu'elle soit ou non publiée sur le web. Ainsi, elle ne peut comporter « une mention d'une limite d'âge supérieure exigée^[21] » du candidat, et ne doit pas comporter d'allégations fausses^[22], ou susceptibles d'induire en erreur sur le « caractère gratuit du service^[23] ». D'autre part, « tout employeur qui fait diffuser par tout moyen de communication accessible au public une offre anonyme d'emploi fait connaître son nom ou sa raison sociale et son adresse au directeur de la publication ou au responsable du moyen de communication^[24] ». En outre, l'offre d'emploi électronique ne peut être subordonnée à une condition fondée sur l'un des éléments visés à l'article 225-1 du Code pénal. L'autre interdiction concerne les enchères électroniques inversées. Cela consiste à offrir le poste proposé à celui qui acceptera de diminuer ses conditions d'embauche. Cette procédure est interdite en matière de fixation du salaire. Par conséquent, « tout contrat de travail stipulant un salaire fixé à l'issue d'une telle procédure est nul de plein droit^[25] ».

Si les TIC permettent de diversifier les modes de publication des offres d'emplois, permettant ainsi de faciliter la rencontre entre l'offre et la demande de travail, elles ne peuvent constituer un moyen de contourner les règles légales applicables en la matière. Il en va de même en ce qui concerne le recrutement.

B. Les principes régissant le recrutement

Le recrutement d'un candidat passe par la collecte d'informations sur ce dernier afin d'évaluer s'il correspond ou non au poste pour lequel il postule. Un certain nombre de règles encadrent le recrutement. La première d'entre elle est le principe de finalité. L'article L.1221-6, alinéa 1^{er} pose le principe selon lequel « les informations demandées, sous quelque forme que ce soit, au candidat à un emploi ne peuvent avoir comme finalité que d'apprécier sa capacité à occuper l'emploi proposé ou ses aptitudes professionnelles ». L'alinéa 2 ajoute que ces « informations doivent présenter un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles ». Les méthodes de recrutement et d'évaluation doivent « être pertinentes au regard de la finalité poursuivie^[26] ».

Le second principe essentiel est le principe de transparence. Cela signifie que « le candidat à un emploi est expressément informé, préalablement à leur mise en œuvre, des méthodes et techniques d'aide au recrutement utilisées à son égard^[27] ». D'autre part, aucune information personnelle « ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance^[28] ». En outre, il est important que les informations demandées soient justifiées, et proportionnées au but recherché. On peut donc aisément convenir qu'en vertu de ces principes, la recherche d'informations personnelles sur les réseaux sociaux, ou sur internet, d'un candidat à un emploi est interdite. Les principes de finalité et de proportionnalité n'étant pas respectés. Toutefois, les recherches effectuées sur la « toile » peuvent avoir pour but d'obtenir des informations professionnelles. On ne peut interdire l'accès à des sources qui ont un caractère public de par leur large diffusion. Ce qui est interdit, c'est d'utiliser des informations qui n'auraient aucun lien avec l'emploi afin d'écartier un candidat. On peut ici faire référence à l'article 225-2, 3^o du Code pénal, et L.1132-1 du Code du travail qui prohibent la discrimination à l'embauche. Rappelons que la discrimination est le fait d'opérer une distinction entre des personnes en raison de leurs origines, de leur sexe, de leurs mœurs, de leurs orientations sexuelles, de leurs âges, de leurs situation de famille ou de leur grossesse, de leurs caractéristiques génétiques, de leur appartenance ou de leur non-appartenance, vraie ou supposée, à une ethnie, une nation ou une race, de leurs opinions politiques, de leurs activités syndicales ou mutualistes, de leurs convictions religieuses, de leur apparence physique, de leur nom de famille ou en raison de leur état de santé

ou de leur handicap. Si au cours d'un entretien un candidat soupçonne qu'il a fait l'objet d'une discrimination, il peut actionner le mécanisme du renversement de la charge de la preuve prévu à l'article L.1134-1 du Code du travail. Celui-ci dispose que « *lorsque survient un litige en raison d'une méconnaissance des dispositions [relatives à la discrimination] le candidat à un emploi, à un stage ou à une période de formation en entreprise ou le salarié présente des éléments de fait laissant supposer l'existence d'une discrimination directe ou indirecte (...) Au vu de ces éléments, il incombe à la partie défenderesse de prouver que sa décision est justifiée par des éléments objectifs étrangers à toute discrimination* ». Or, il sera difficile pour un candidat d'apporter de tels éléments s'il n'a pas été reçu à un entretien, en raison d'un des critères précédemment évoqués, dont aurait eu connaissance le recruteur par le biais d'internet.

Paragraphe 2. De nouveaux supports de recrutement profitant de l'existence de vides juridiques

« *Le contrôle des antécédents des futurs employés est la deuxième principale raison du recours aux médias sociaux*^[29] » par les entreprises souhaitant recruter. C'est d'ailleurs la raison pour laquelle très peu de personnes souhaitent se servir de leurs réseaux sociaux « privés » pour rechercher un emploi. D'après l'étude susmentionnée, 60 % des personnes interrogées n'apprécient guère que des employeurs cherchent à avoir accès à des informations relevant de leur vie privée (A). La recherche de telles informations peut aisément faciliter la prise en compte non contrôlée de critères pourtant prohibés par la loi (*op-cit*). Cet état de fait soulève la question du droit à l'oubli numérique (B).

A. L'accès à des informations relevant de la vie privée

Les réseaux sociaux prennent une place croissante dans la vie quotidienne des individus. Ces derniers, notamment les jeunes, n'hésitent pas à rendre public des informations très personnelles. On pense à l'orientation sexuelle, aux convictions religieuses ou politiques. Si cela relève de leur responsabilité, on ne peut pas en dire autant des informations présentes sur internet, et accessibles à tous alors même que la personne en question n'ait fait aucune démarche en ce sens. Cette divulgation d'informations personnelles, parfois compromettantes, combinée au fait que les employeurs prennent l'habitude de « googliser » les candidats, conduisent légitimement à s'interroger sur le respect des principes relatifs au recrutement. Il est aujourd'hui possible de dresser un portrait d'un candidat au vu de ses antécédents, de ses activités, de ses opinions, en violation des principes de transparence et de proportionnalité précédemment mentionnés.

C'est ici toute la question de l'E-réputation qui est posée. Compte tenu de la difficulté à contrôler les informations qui peuvent circuler sur Internet, on ne peut que conseiller de ne pas divulguer d'informations privées, même partagées avec un cercle restreint d'amis tel que sur Facebook. Il est aisé pour quelqu'un qui souhaite nous nuire, d'effectuer des captures d'écran ou de copier les photos publiées et de les divulguer à un plus grand nombre. Une fois que de telles informations circulent sur la toile, il devient alors extrêmement difficile de les supprimer, d'autant que « *la mémoire du Web est infinie et que la question du droit à l'oubli numérique est l'un des enjeux majeurs de la protection des citoyens et du respect du droit à la vie privée, voire même de l'existence d'un droit à l'erreur et de la possibilité de se racheter*^[30] ».

B. Vers un droit à l'oubli numérique ?

« *La Toile est une gigantesque mémoire externe pour l'être humain*^[31] . » Le droit à l'oubli numérique n'est pas encore consacré par les textes à ce jour. Pourtant, les « *empreintes très digitales laissées sur le Net [...] conduisent à pouvoir désigner, par adresse courriel ou IP interposée, une personne physique ou morale parfaitement identifiable*^[32] ».

En l'absence de règles en la matière, il faut se contenter des dispositifs déjà existant. Selon Corinne THIÉRACHE « *si la loi de 1978 modifiée offre déjà les outils nécessaires pour protéger les données à caractère personnel, celle-ci souffre d'une absence d'effectivité en pratique, soit de la part des acteurs de l'internet, pas toujours soucieux de son respect, soit de la part des internautes, pas toujours sensibilisés aux possibilités de paramétrage de leurs données et à la manière dont celles-ci sont diffusées*^[33] ». Face à ce manque d'efficacité, mais en raison de la prise de conscience des dangers que peut représenter la mémoire du web, deux chartes ont été signées. La *Charte du Droit à l'oubli numérique dans la publicité*, signée le 30 septembre 2010, et la *Charte du Droit à l'oubli numérique dans les sites collaboratifs et moteurs de recherche*, signée le 13 octobre 2010. Si on peut se réjouir des avancées effectuées, on ne peut pas considérer qu'elles soient suffisantes. D'une part, les chartes n'ont de réelles influences que lorsqu'elles sont signées par un nombre important d'acteurs, et lorsque ces derniers respectent leurs engagements. D'autre part, ces chartes n'ont qu'une portée géographique limitée à l'Etat français, alors même que l'Internet est un phénomène mondial. La consécration d'un droit à l'oubli numérique semble donc dépendre d'un accord conclu au niveau international. Or, on sait que de tels accords sont souvent conclus *a minima*.

Si comme nous l'avons vu, les TIC permettent aux recruteurs d'obtenir de plus amples informations sur les candidats à un emploi, elles sont aussi un moyen d'envisager un autre mode d'organisation du travail : le télétravail. En rendant l'offre d'emploi plus attractive, et en permettant à des candidats situés loin du centre de production de postuler, le télétravail augmente l'attractivité de l'offre, et facilite ainsi le recrutement.

Section 2 : Le recrutement en télétravail

Le télétravail a tout d'abord fait l'objet d'un accord-cadre européen du 16 juillet 2002, transposé par l'accord national interprofessionnel (ANI) du 19 juillet 2005. Cet accord le définit en son article 1 comme une « *forme d'organisation et/ou de réalisation du travail, utilisant les technologies de l'information dans le cadre d'un contrat de travail et dans laquelle un travail, qui aurait également pu être réalisé dans les locaux de l'employeur, est effectué hors de ces locaux de façon régulière* ». C'est seulement par la loi du 22 mars 2012 que le « Télétravail » fait son entrée dans le Code du travail. Les TIC sont au cœur de la définition du télétravail, elles sont l'une des conditions sans laquelle il ne peut exister. Le fait de travailler à l'extérieur des locaux de l'entreprise ne suffit pas à acquérir la qualité de télétravailleur. A l'inverse, la définition précitée n'implique pas que le travail soit réalisé en totalité hors de l'entreprise. L'article 1^{er} de l'ANI poursuit en affirmant que le télétravail peut s'effectuer « *soit dès l'embauche, soit ultérieurement* ». Le recrutement en télétravail est la première forme possible citée par l'ANI. Pourtant, seul 12 % des salariés français étaient en télétravail en 2012, alors même que la moyenne dans les pays Anglo-Saxons se situe entre 20% et 30 %^[34]. Le recours au télétravail revêt pourtant de nombreux avantages (Paragraphe 1). Qu'il soit mis en place dès l'embauche, ou ultérieurement, le télétravail est un mode d'organisation du travail qui ne peut exister sans confiance (Paragraphe 2).

Paragraphe 1. Les raisons du recours au télétravail

Le télétravail recouvre de nombreux avantages pour l'employeur (A), mais aussi pour les salariés (B).

A. Les avantages du télétravail pour l'employeur

Dans cette conjoncture économique marquée par la recherche accrue de gains de productivité et de réduction des coûts, le télétravail trouve toute sa place. L'un des apports incontestés du télétravail pour les entreprises est l'augmentation de la productivité. « *L'OIT relève que les télétravailleurs ont tendance à être plus productifs et même à travailler davantage que leurs homologues exerçant au bureau. Selon la synthèse d'études sur le télétravail, quelques grandes*

sociétés, notamment Best Buy, British Telecom et Dow Chemical, rapportent que les télétravailleurs sont 35 à 40 % plus productifs^[35] ». L'étude relève également que le télétravail réduit l'absentéisme (de 63 % en moyenne) grâce à la flexibilité des horaires qui permet aux télétravailleurs « de gérer [leurs] obligations familiales, (...) prévoir des rendez-vous sans perdre toute une journée de travail^[36] ». Outre les gains de productivité, le télétravail permet également de réduire les coûts immobiliers, et énergétiques en réduisant l'espace nécessaire. Il apparaît également comme un instrument permettant « de véhiculer une image de souplesse et de modernisation qui peut s'avérer attractive^[37] ».

B. Les avantages du télétravail pour le salarié

Le télétravail est une forme d'organisation du travail laissant une grande part de liberté et d'autonomie au travailleur. Cela s'accompagne d'une responsabilisation du salarié, source de valorisation qui peut être recherchée chez un individu. Parce qu'il ne nécessite aucun déplacement lorsqu'il est effectué à domicile, le télétravail emporte une diminution des coûts de transport, ainsi qu'une diminution des temps de trajet. Le stress et la fatigue en sont ainsi réduits.

D'un point de vue social, deux apports importants ressortent de cette forme d'organisation. D'une part, le télétravail peut permettre une meilleure conciliation entre la vie privée et la vie professionnelle. Le fait de travailler à domicile peut faciliter un contact plus important avec sa famille. D'autre part, il permet d'accroître la diversité dans l'entreprise. L'OIT a également relevé que le travail à domicile offres « des perspectives de travail à des femmes qui rencontrent des problèmes de garde d'enfants (ou de parents) ». La jeune génération, particulièrement sensibilisée à l'utilisation des nouvelles technologies et peu attachée à l'organisation classique du travail, se montre fortement intéressée par cette forme d'organisation. Enfin, pour les travailleurs handicapés, le télétravail peut être synonyme d'une meilleure intégration dans la vie professionnelle grâce à un environnement de travail adapté à leur situation. Il est important de rappeler qu'en vertu de l'article L.5212-2 du Code du travail, les entreprises employant au moins 20 salariés sont soumises à une obligation d'emploi de salariés en situation de handicap à hauteur de 6%. Alors que le handicap peut constituer une entrave à une embauche « classique », le télétravail peut s'avérer être une réelle alternative. L'exemple du handicap montre que ce mode d'organisation peut s'apparenter à une véritable relation « gagnant-gagnant », en plus d'être une certaine consécration du principe de confiance.

Au passage, notons que pour l'Etat, le télétravail peut être un levier intéressant en vue de diminuer l'impact écologique des transports et de désengorger la circulation. Il permet aussi de lutter « contre la « désertification » de certains territoires et [d'aider] au désengorgement des grandes villes^[38] ».

Paragraphe 2. La consécration du principe de confiance

Si la tendance montre une augmentation progressive de nombre de télétravailleur, « un tiers des employeurs affirme préférer voir leur personnel, pour s'assurer qu'il travaille réellement. Cela souligne la nécessité de faire évoluer la culture d'entreprise vers une approche plus moderne qui estime le personnel digne de confiance^[39] ». La confiance dans la relation de travail est au cœur du contrat. Elle l'est d'autant plus lorsque le télétravail est mis en place. Celle-ci se matérialise alors par le double principe de volontarisme et de réversibilité (A), ainsi que par les obligations qui pèsent sur l'une et l'autre des parties (B), qu'elles soient tacites ou implicites.

A. Le principe de volontarisme et de réversibilité

« Le télétravail revêt un caractère volontaire pour le salarié et l'employeur concernés. Le télétravail peut faire partie des conditions d'embauche du salarié ou être mis en place, par la suite, sur la base du volontariat^[40] ».

En aucun cas il ne peut être imposé au salarié. Il en va du respect du principe de protection de la vie privée, dont le domicile constitue le sanctuaire. De plus, comme le souligne Jean-Emmanuel RAY, « *le télétravail au domicile, même à temps partiel, peut se révéler ni bon pour le travail, ni bon pour le domicile (et ses autres habitants : conjoint, enfants). L'entrée comme la sortie doivent faire l'objet d'un total consensus sous peine d'échec* ». Une fois ce principe fondamental rappelé, il convient toutefois de relativiser la portée de cet article dans le cadre d'une offre d'emploi proposant un poste en télétravail. On comprend aisément que dans ce cas, le salarié est tenu d'accepter le télétravail s'il souhaite être embauché. Dans cette période où les taux de chômage atteignent des records^[41], il est probable que des personnes acceptent un télétravail sans forcément le désirer. Dans le cas d'une embauche en télétravail, il n'y a pas de période d'adaptation comme c'est le cas pour le passage en télétravail. Toutefois, il pourra y avoir une période d'essai pendant laquelle chaque partie sera libre de rompre le contrat. Lorsque cette période sera terminée, l'employeur ne pourra plus imposer au salarié de travailler dans les locaux de l'entreprise. Il s'agirait d'une modification unilatérale du contrat^[42]. Réciproquement, le salarié ne pourrait refuser d'exécuter sa prestation de travail à son domicile sans commettre une faute grave. En revanche, l'intérêt qu'une personne aurait à accepter un emploi en télétravail, bien qu'elle ne le souhaitait pas, réside dans le fait que « *si le télétravail fait partie des conditions d'embauche, le salarié peut ultérieurement postuler à tout emploi vacant, s'exerçant dans les locaux de l'entreprise et correspondant à sa qualification* ». Il bénéficiera alors d'une « *priorité sur ce poste*^[43] » lui permettant d'obtenir une place au sein même de l'entreprise.

Il est vrai que si le télétravail recouvre de nombreux avantages, il peut également être un échec s'il n'a pas été préalablement bien étudié. D'autre part, sa réussite dépend en grande partie du respect pour chaque partie des obligations qui sont les siennes.

B. Des obligations spécifiques réciproques

La confiance dans la relation de travail passe avant tout par le respect de ses engagements contractuels. La mise en place du télétravail ne peut être un succès lorsqu'il est perçu par l'une ou l'autre des parties comme la possibilité de déroger à ses obligations respectives. Si le télétravail met à la charge de l'employeur certaines obligations (a), le télétravail n'est pas synonyme de « sous subordination » pour le salarié. Si dans « télétravail » il y a « Télé », il y a aussi « Travail » (b).

a. Les obligations de l'employeur

Outre le principe d'égalité de traitement auquel est soumis tout employeur, c'est l'article L.1222-10 du Code du travail qui précise les obligations spécifiques pesant sur l'employeur ayant recours au télétravail. En premier lieu, il lui revient de « *prendre en charge tous les coûts découlant directement de l'exercice du télétravail, notamment le coût des matériels, logiciels, abonnements, communications et outils, ainsi que de la maintenance de ceux-ci*^[44] ». Lorsqu'une partie des frais est avancée par le salarié, l'employeur doit lui rembourser via l'indemnité de télétravail dont l'objet est de couvrir les coûts engendrés directement par le télétravail. Dans une série d'arrêts rendus le 7 avril 2010, la Cour de cassation a ajouté une nouvelle indemnité, que l'on peut intituler « indemnité d'occupation du domicile ». Les hauts magistrats soutiennent que « *l'occupation, à la demande de l'employeur, du domicile du salarié à des fins professionnelles constitue une immixtion dans la vie privée de celui-ci et n'entre pas dans l'économie générale du contrat de travail ; [...] si le salarié, qui n'est tenu ni d'accepter de travailler à son domicile ni d'y installer ses dossiers et ses instruments de travail, accède à la demande de son employeur, ce dernier doit l'indemniser de cette sujétion particulière ainsi que des frais engendrés par l'occupation à titre professionnel de son domicile*^[45] ». Cette indemnité d'occupation est distincte de l'indemnité liée à

la compensation de dépenses à caractère professionnel. Elle s'explique par le désagrément causé par l'utilisation du logement à titre professionnel. Il est également prévu une priorité de retour à un travail sur le site de l'entreprise (v. *Supra*), ainsi que le contrôle et le suivi de l'activité du salarié. Sur ce point, L'article L.1222-10 prévoit la tenue d'un entretien individuel portant sur « *les conditions d'activité du salarié et sa charge de travail* ». La fixation de plages horaires de disponibilité (v. *Supra*) vise quant à elle à « *protéger [la] vie personnelle et familiale [du salarié] contre toute immixtion intempestive de l'employeur dans la vie quotidienne de son salarié*^[46] ». D'autre part, si la loi de 2012 n'aborde le télétravail que « *sous l'angle du contrat individuel*^[47] », l'employeur a l'obligation de consulter le comité d'entreprise au titre de l'article L.2323-6 et L.2323-27 du Code du travail, ainsi que le CHSCT au titre de l'article L.4612-8 du même code.

De nombreux salariés ont la crainte d'être isolés s'ils acceptent le télétravail, ou encore que leur progression de carrière soit compromise. Dans la majorité des cas, le télétravail ne s'effectue pas en totalité à l'extérieur de l'entreprise. Le salarié conserve un point d'attache au sein des locaux afin de maintenir le lien social avec ses collègues, son supérieur hiérarchique, mais aussi pour ne pas être déconnecté de la culture de l'entreprise. Face à cette crainte, l'OIT « *rappelle que les innovations technologiques dont disposent les entreprises - vidéoconférences, messageries instantanées, courriels, téléphone - associées à des contacts personnels et à des systèmes d'évaluation basés sur la performance, permettent de maintenir les aspects collectifs de la relation de travail*^[48] ». On ne peut cependant pas prétendre que les moyens de communication remplacent le contact humain.

b. Les obligations du télétravailleur

Le télétravailleur est un salarié de l'entreprise à part entière. Toutefois, sa situation implique nécessairement quelques particularités. Le fait de ne pas être sous la surveillance directe de l'employeur peut inciter certains salariés de vaquer à leurs occupations personnelles. Or, le télétravail est une source d'autogestion. Le télétravailleur doit parvenir à faire la part entre ses obligations professionnelles et familiales. En outre, « *le télétravail n'est pas un substitut à la garde d'enfants, même s'il aide les parents actifs à remplir leurs responsabilités familiales*^[49] ». Si le salarié a la possibilité de s'organiser comme il le souhaite, il convient toutefois de rappeler que des plages horaires pendant lesquelles il peut être contacté par l'employeur seront fixées dans la convention de télétravail. Un salarié qui ne serait pas joignable durant ces horaires pourra être sanctionné^[50]. A ces plages horaires s'ajoute un contrôle du nombre d'heures travaillées. Ce contrôle est effectué sur la base d'une méthode que l'employeur aura jugée adaptée. Il peut s'agir d'un décompte horaire, ou sur la base d'un forfait jour (logiciel de pointage, système d'auto déclaration.). Notons que si l'employeur se doit de faire respecter les temps de repos hebdomadaires et quotidiens, cela devient plus compliqué dans une situation de télétravail... Il convient alors d'inscrire par écrit que le salarié s'engage à respecter les temps de repos obligatoires. Enfin, le salarié se doit de respecter les prescriptions édictées par l'employeur en matière d'utilisation des outils informatiques mis à sa disposition. Cela suppose également la maîtrise des technologies de l'information et de la communication, sans lesquelles le télétravail ne peut exister. Sans cette maîtrise, la prestation de travail ne pourra être réalisée.

Si le recrutement en télétravail offre de nouvelles opportunités pour l'employeur, seul 10 % d'entre eux « *privilégient cette solution pour recruter*^[51] ». Dans la grande majorité des cas, le télétravail résulte d'une modification du contrat de travail.

Chapitre 2 : Les NTIC et l'évolution du contrat de travail

Les NTIC modifient la façon dont est conclu le contrat de travail. Les offres d'emplois électroniques et le recrutement en télétravail permettent d'avoir une certaine souplesse et

concourent à la modernisation de la relation de travail. Les TIC vont également intervenir au cours de l'exécution du contrat. Là encore, elles vont permettre de gérer la relation de travail en facilitant de nouveaux modes d'organisation ou en poussant à la modification du contrat. Dans le premier cas, il s'agira de montrer comment le télétravail permet à l'employeur de trouver de nouvelles solutions à des situations devenues difficiles. Si le recrutement en télétravail connaît un certain essor, il reste marginal. Dans la plupart des cas, ce dernier est mis en place par le biais d'un avenant au contrat (Section 1).

Le télétravail n'est pas la seule source de modification du contrat. On voit à quelle vitesse se développent les NTIC. Il n'y a pas un jour sans qu'une technologie soit inventée ou améliorée. Cela a un impact direct sur le contrat de travail dans la mesure où les évolutions supposent un effort de formation. Si chaque salarié a le droit d'être formé, ce droit peut aussi s'apparenter à une obligation. En cela, les NTIC sont une source de modification du contrat (Section 2).

Section 1. Le passage en télétravail

Le télétravail peut être un outil d'évolution du contrat. Dans la plupart des cas, il est mis en place au cours de son exécution et non dès sa conclusion. Il est alors un outil d'adaptation du contrat (Paragraphe 1) afin de satisfaire la volonté commune des deux parties. Au-delà de la simple modification du contrat, le télétravail conduit à s'interroger sur la modification de l'équilibre contractuel (Paragraphe 2).

Paragraphe 1. Un outil d'adaptation du contrat

Le contrat de travail fixe les conditions dans lesquelles s'exécute la prestation de travail. Cette relation peut être amenée à évoluer au cours du contrat. Le passage au télétravail nécessite une relation de confiance qui va se traduire par une mise en place volontaire *via* un avenant au contrat (A). Cette souplesse peut permettre de maintenir la relation contractuelle malgré les difficultés rencontrées par l'une ou l'autre des parties. Le passage en télétravail peut alors être source de sécurité (B).

1. Les conditions du passage au télétravail

L'article 2 alinéa 2 de l'ANI du 19 juillet 2005 énonce que le salarié peut demander à l'employeur le passage au télétravail. Celui-ci est libre d'accepter ou de refuser cette demande. L'employeur a également la possibilité de proposer au salarié le passage au télétravail, mais dans ce cas, le salarié devra également donner son accord. La Cour de Cassation rappelle régulièrement que le domicile est au cœur de l'intimité de la vie privée. Par conséquent, on ne peut imposer le transfert du travail au domicile du salarié. En outre, la Cour affirme que le passage au télétravail n'est pas seulement une modification du contrat de travail, mais une modification du mode d'organisation de l'activité. Il s'agit là d'un élément essentiel du contrat de travail nécessitant l'accord du salarié. L'article L.1222-9 alinéa 3 du Code du Travail énonce que « *le refus d'accepter un poste de télétravailleur n'est pas un motif de rupture du contrat de travail* ». On ne peut se placer sur le terrain disciplinaire. L'accord entre les parties se traduit par la rédaction d'un avenant au contrat de travail^[52]. Ce dernier devra préciser entre autres les conditions du passage en télétravail, le lieu du télétravail, les plages horaires, la charge de travail ou encore les équipements de travail fournis. Ce principe peut être illustré par l'arrêt de la chambre sociale de la Cour de cassation du 31 janvier 2012^[53]. Dans cette affaire, un médecin a pris acte de la rupture de son contrat suite à l'ordre qui lui a été donné de travailler à son domicile. La Cour confirme l'arrêt de la Cour d'appel qui en a déduit « *l'existence d'une modification unilatérale du contrat de travail justifiant la prise d'acte de la rupture* ». A cela, il faut ajouter les conditions de retour à une exécution du contrat de travail sans télétravail. Le passage en télétravail n'est pas irrémédiable. L'article 2 alinéa 5 de

l'ANI prévoit la mise en place obligatoire d'une période d'adaptation. Durant cette période, les deux parties sont libres de revenir sur leur décision moyennant le respect d'un délai de prévenance. On parle ici de réversibilité initiale. Le problème qui se pose pour le salarié est de savoir s'il retrouvera exactement le même poste. Cela n'est pas certain, l'ANI prévoyant qu'il retrouve un poste correspondant à ses qualifications. Lorsque la période d'adaptation est terminée et que l'une des parties veut mettre fin au télétravail, on parle de réversibilité à terme. L'article 3 de l'ANI prévoit que l'initiative revient à l'une ou l'autre des parties. Toutefois, la réversibilité nécessite un accord réciproque qui doit avoir été prévu dans le contrat ou dans un accord collectif. Comme l'affirme Henri GUYOT et Brune FOURNIER, « *passer outre le double accord des parties ne paraît envisageable que dans l'hypothèse où un avenant à durée déterminée, sans tacite reconduction, serait conclu* »^[54]. Dans ce cas, l'absence de volonté des parties de renouveler l'expérience mettrait fin au télétravail.

La rigidité qui entoure le passage au télétravail est la condition d'accès à une source de sécurité importante.

2. Le télétravail, source de sécurité

Comme nous l'avons précédemment évoqué, le télétravail peut être une solution d'embauche directe de salarié en situation de handicap. Mais il peut également être une solution de reclassement d'un salarié devenu inapte. Pour l'employeur, le télétravail est une solution de plus en vue d'accomplir ses obligations légales. Pour le salarié, il devient une source de sécurité grâce au maintien dans l'emploi. « *Au Royaume-Uni, le principe du télétravail s'impose peu à peu en cas d'inaptitude liée, par exemple, à une agoraphobie ou à un handicap consécutif à une maladie grave. Il pourrait alors être soutenu que constitue un manquement de l'employeur à son obligation de reclassement l'absence de recherche de proposition de poste en télétravail*^[55] ». Au-delà du reclassement, le télétravail permet aussi de maintenir l'activité en cas de circonstances exceptionnelles. On pense notamment aux risques de pandémies auxquels les salariés en télétravail seraient moins exposés^[56]. L'accord Renault S.A.S du 22 juin 2010 relatif au télétravail à domicile prévoit également le recours au télétravail exceptionnel « *en cas d'une grève des transports publics, de dégradation des conditions climatiques ou d'indisponibilité temporaire du véhicule personnel*^[57] ». Il est important de préciser que dans de telles situations, les dispositions relatives à la modification du contrat de travail ne s'appliquent pas. Le retour dans les locaux de l'entreprise ne nécessite pas l'accord du salarié, ni la rédaction d'un avenant au contrat.

Si le télétravailleur est un salarié comme les autres, il convient toutefois de s'interroger sur les modifications de l'équilibre contractuel qu'il implique.

Paragraphe 2. Le télétravail et la modification de l'équilibre contractuel

Le travail salarié est caractérisé par la réalisation d'une prestation de travail sous la subordination de l'employeur en échange d'une rémunération. Le télétravail entraîne un brouillage du temps et du lieu de travail, de sorte que la frontière entre vie professionnelle et vie privée semble être de plus en plus floue (A). Il apparaît que le travail loin du centre de production assouplit le lien de subordination, certains parlent alors de « sub/organisation^[58] » (B).

1. Le télétravail source de brouillage du temps et de l'espace de travail

Si la mise en place du télétravail nécessite de fixer des plages horaires de travail sur lesquelles le salarié est tenu d'être disponible, qu'est ce qui permet d'affirmer que le salarié anxieux et ayant la volonté de bien faire s'arrête de travailler afin de respecter les temps de repos journaliers ? Certes des moyens permettent de comptabiliser le temps travaillé *via* le matériel mis à disposition du

télétravailleur. Mais il est aujourd'hui facile de transférer les travaux effectués sur son ordinateur professionnel vers son ordinateur personnel. Le salarié pourra alors continuer de travailler à l'insu de son employeur. Dans une telle situation, se pose la question du brouillage du temps de travail induite par les NTIC. Une étude a démontré que de nombreux salariés continuaient à travailler en dehors même de leur temps de travail^[59]. Or, il est acquis que le Droit au repos est un impératif de la Cour de Justice de l'Union Européenne^[60] et de la Cour de Cassation^[61]. L'espace de travail est également brouillé par les NTIC. Le télétravailleur à domicile voit l'endroit le plus sacré de sa vie privée être mis au profit de l'exécution de tâches professionnelles. Loin de l'unité de lieu qui caractérisait la relation de travail, celui-ci est aujourd'hui nulle part et partout. En réalité, si le travail s'immisce dans la vie privée, il ne faut pas oublier que la vie privée a également tendance à s'installer sur le temps et le lieu de travail. Au-delà du télétravail, l'exécution de tâches professionnelles et la disponibilité, sont largement favorisées par la multiplication des points de connexion internet et par l'amélioration des moyens de communication. Il s'en suit un brouillage du temps et du lieu de travail qui peut conduire à atténuer la frontière entre vie professionnelle et vie privée, alors même que le télétravail était censé mieux les concilier.

2. Le télétravail source de « sub/organisation »

Le droit du travail s'est construit sur le modèle de l'unité de temps et de lieu de travail illustré parfaitement par l'organisation scientifique du travail. Il avait alors pour but de protéger les salariés soumis à leur employeur par le lien de subordination, celui-ci étant défini dès 1931 par la Chambre Civile de la Cour de Cassation comme une dépendance juridique du salarié placé « *sous la direction, la surveillance et l'autorité*^[62] » de l'employeur. La notion de lien de subordination a par la suite évolué, puisque la fourniture d'un travail « *dans le cadre d'un service organisé* ». Les NTIC et le télétravail contribuent à l'évolution du lien de subordination. Le salarié s'émancipe de la surveillance directe de l'employeur et semble gagner en autonomie. Toutefois, c'est sans compter sur les moyens dont dispose aujourd'hui l'employeur pour contrôler le travail effectué par le salarié. Les Smartphones, les PC portables contribuent à la portabilité de la subordination. Le travailleur devient alors télé disponible, à tel point que J.E RAY évoque l'image de la « *laisse électronique*^[63] ». On est ici bien loin de l'image du salarié autonome et émancipé. La distance avec l'employeur ne serait alors pas une source de liberté, mais une source de modification de la subordination juridique qui deviendrait alors nomade. Face à cette réalité, « *le droit à la déconnexion*^[64] » a clairement été affirmé par la Chambre Sociale de la Cour de Cassation par un arrêt du 17 février 2004. Les magistrats du Quai de l'horloge affirment que le fait de ne pas pouvoir être joint en dehors des horaires de travail sur son téléphone personnel est dépourvu de caractère fautif et ne peut donc pas justifier un licenciement disciplinaire.

Malgré la compétence induite des institutions représentatives du personnel en matière de télétravail, on ne peut que regretter que ces dernières n'aient pas obtenu un rôle à part entière dans la protection du télétravailleur. Cela illustre « *une fois encore les limites des lois « fourre-tout », quel que soit le nom qu'on leur donne, car si le législateur avait eu la volonté de donner au télétravail un régime juridique clairement identifié et cohérent, il aurait sans doute favorisé une approche plus globale du phénomène dans un texte abordant tous les aspects de la relation de travail*^[65] ».

Si le télétravail entraîne une certaine évolution du contrat de travail, il faut toujours avoir à l'esprit qu'il a pour fondement les NTIC. Ce sont ces dernières qui induisent une évolution plus générale du contrat de travail. Ainsi, l'émergence constante de nouveaux moyens de production et leur évolution amènent les salariés à maintenir leur employabilité par un effort de formation indispensable à la poursuite de la relation de travail.

Section 2. Les nouvelles technologies et la modification du contrat de travail

Les nouvelles technologies entraînent d'importantes évolutions des emplois et des postes occupés. L'adaptation et la formation sont deux clés essentielles à la gestion de ces évolutions. « *La formation est tour à tour droit et obligation, pour l'une ou l'autre partie : tantôt obligation pour le salarié de suivre une formation à la demande de l'employeur, tantôt droit, pour ce même salarié, de prendre un congé pour effectuer une formation de son choix. Droit pour l'employeur d'imposer à ses salariés une formation, mais obligation de les adapter aux évolutions de leurs emplois*^[66] ». Le développement de l'employabilité est source d'obligations réciproques. En matière de mutations technologiques, l'obligation d'adaptation de l'employeur (Paragraphe 1), s'accompagne du devoir d'adaptabilité du salarié (Paragraphe 2).

Paragraphe 1. L'obligation d'adaptation de l'employeur

L'obligation d'adaptation à laquelle est soumis l'employeur revêt deux facettes. D'une part, une obligation générale d'adaptation (A) imposant à l'employeur d'adapter ses salariés par le biais d'un effort de formation. D'autre part, une obligation d'adaptation spécifique dans le cadre d'une procédure de licenciement pour motif économique (B).

A. L'obligation générale d'adaptation

Les employeurs sont tenus de participer à la formation des salariés depuis la loi du 16 juillet 1971. La loi du 2 août 1989, impose la gestion prévisionnelle des emplois. Le but étant de prévoir l'adaptation professionnelle des salariés à l'évolution de l'emploi et à leurs qualifications. Afin de maintenir les salariés dans leur emploi, la loi impose un certain nombre d'obligations en matière de formation à la charge de l'employeur. Le CHSCT et le Comité d'Entreprise sont amenés à jouer un rôle important en la matière. Ces derniers doivent être consultés sur le projet d'introduction et lors de l'introduction de nouvelles technologies lorsqu'elles peuvent avoir des conséquences sur « *la qualification, la rémunération, la formation ou les conditions de travail*^[67] ». La mise en œuvre de mutations technologiques rapides et importantes doivent également faire l'objet d'un plan d'adaptation, lui-même soumis au CHSCT et au Comité d'Entreprise^[68]. Il convient de distinguer deux types d'action de formation. Les actions d'adaptation au poste de travail ou liées à l'évolution ou au maintien dans l'emploi prévue à l'article L.6321-2 et les actions de développement des compétences prévues à l'article L.6321-6. Si le premier type d'action peut donner lieu à sanction en cas de refus du salarié, « *le refus du salarié de participer à des actions de formation de développement des compétences (...) ne constitue ni une faute ni un motif de licenciement*^[69] ».

L'article L.6321-1 du Code du travail prévoit que l'employeur est tenu d'assurer « *l'adaptation des salariés à leur poste de travail et veille au maintien de leur capacité à occuper un emploi, au regard notamment de l'évolution des emplois, des technologies et des organisations* ». Ce principe a été rappelé dans un arrêt de la Cour de Cassation du 5 juin 2013. Les magistrats du Quai de l'horloge affirment que « *viole son obligation d'assurer l'adaptation des salariés à leur poste de travail, l'employeur qui ne fait bénéficier le salarié d'aucune formation au cours d'une longue carrière professionnelle au sein de l'entreprise, (...) qu'en considérant que la société n'avait pas failli à son obligation de formation et d'adaptation à l'égard [du salarié] aux motifs inopérants qu'elle lui avait permis d'acquérir une expérience au poste d'opérateur de ligne et que le salarié n'avait pas pris l'initiative d'une formation dans le cadre d'un congé individuel de formation quand il n'était pas contesté [qu'il] n'avait bénéficié d'aucune formation depuis son recrutement et ce, pendant seize ans*^[70] ». L'obligation d'adaptation résulte de la nécessité d'exécuter de bonne foi le contrat le travail.

B. L'obligation d'adaptation dans le cadre d'un licenciement pour motif économique

Pour être justifié, le licenciement doit être consécutif « *notamment à des difficultés économiques ou à des mutations technologiques*^[71] ». Cette dernière est caractérisée en cas d'introduction d'une nouvelle technologie dans l'entreprise. Selon la Cour de Cassation, l'introduction de nouvelles technologies peut constituer une cause de suppression ou de transformation d'emploi ou de modification de contrat de travail^[72]. Cela se justifie par le fait que l'introduction d'une nouvelle technologie peut rendre obsolète telle ou telle activité de l'entreprise et entraîner des suppressions, transformations ou des modifications du contrat de travail. L'introduction de nouvelles technologies peut intervenir en-dehors de toute difficulté économique rencontrée par l'entreprise. En effet, « *l'informatisation de l'entreprise peut constituer une mutation technologique justifiant un licenciement économique, peu important l'existence de difficultés économiques*^[73] ». L'introduction de nouvelles technologies peut parfaitement être destinée à rendre l'entreprise plus compétitive, à lui faire faire davantage de profits. Les licenciements seront justifiés. Ce motif de licenciement a été critiqué par une partie de la doctrine. Le législateur a tenté de restreindre en 2002 ce motif, aux mutations technologiques mettant en cause la pérennité de l'entreprise, sans succès. On précisera qu'en pratique, l'existence de mutations technologiques est rarement invoquée comme cause de licenciement. Cela tient au fait que cela est parfois la conséquence de difficultés économiques, auquel cas l'employeur invoquera de préférence ces difficultés économiques pour justifier ces licenciements. Cela s'explique également par le fait que les mutations technologiques recouvrent une autre cause de licenciement : la réorganisation de l'entreprise. Cette cause de licenciement a été érigée par la jurisprudence, dans le célèbre arrêt videocolor du 5 avril 1995^[74]. La Cour de Cassation affirme que « *lorsqu'elle n'est pas liée à des difficultés économiques ou à des mutations technologiques, une réorganisation ne peut justifier un licenciement pour motif économique que si elle est effectuée pour sauvegarder la compétitivité du secteur d'activité* ». Les arrêts Pages Jaunes du 11 janvier 2006^[75] autorisent à mener une réorganisation de l'entreprise dans le but de prévenir des difficultés économiques.

Depuis le 25 février 1992^[76], « *l'employeur tenu d'exécuter de bonne foi le contrat de travail a le devoir d'assurer l'adaptation des salariés à l'évolution de leur emploi* ». Ce principe a ensuite été inscrit dans le Code du Travail qui dispose que « *le licenciement pour motif économique d'un salarié ne peut intervenir que lorsque tous les efforts de formation et d'adaptation ont été réalisés*^[77] [...] ». Lorsque le salarié refuse, l'employeur doit rechercher et proposer au salarié concerné des emplois disponibles de même catégorie, avec une rémunération équivalente. A défaut, l'employeur pourra proposer un emploi de catégorie inférieure, « *fût-ce par voie de modification du contrat de travail, au besoin en assurant au salarié une adaptation à l'évolution de son emploi*^[78] ». Notons que la Cour de Cassation se refuse à accorder le droit aux salariés d'obtenir une « reconversion ». Ainsi, « *si l'employeur a l'obligation d'assurer l'adaptation des salariés à l'évolution de leur emploi, au besoin en leur assurant une formation complémentaire, il ne peut lui être imposé d'assurer la formation initiale qui leur fait défaut*^[79] ». Elle limite l'obligation de l'employeur à un effort d'adaptation et non de requalification.

L'obligation d'adaptation de l'employeur résulte de la nécessité d'exécuter de bonne foi le contrat de travail. Celle-ci étant exigée de chaque partie, le salarié est lui-même tenu à une obligation d'adaptabilité.

Paragraphe 2. Le devoir d'adaptabilité du salarié

L'introduction de nouvelles technologies peut justifier la mise en place d'une formation destinée aux salariés impactés par les modifications de leurs postes ou de leur emploi. Si le salarié a le droit d'être adapté, c'est également un devoir qui lui incombe. Il se doit ainsi d'accepter les

formations proposées par l'employeur ayant pour but de l'adapter aux évolutions (A). S'il accepte la modification du contrat, le salarié n'est pas pour autant certain de conserver son emploi.

« *Le problème peut rebondir ultérieurement : encore faut-il qu'il puisse l'occuper durablement et normalement*^[80] » (B).

A. L'obligation d'accepter les actions d'adaptation

Les actions de formation ayant pour objet le développement des compétences du salarié, qui se déroule en tout ou en partie hors du temps de travail, nécessite l'accord du salarié. L'article L.6321-7 du Code du Travail précise que « *le refus du salarié de participer à des actions de formation de développement des compétences [...] ne constitue ni une faute ni un motif de licenciement* ». Dans ce cas, l'employeur ne peut que prendre acte du refus du salarié. Il en va tout autrement des actions d'adaptation au poste de travail, celle liées à l'évolution, au maintien dans l'emploi, ou des actions de développement des compétences se déroulant entièrement pendant le temps de travail. Dans ce cas de figure, le refus du salarié constitue en principe une faute, qui pourra conduire au licenciement du salarié lorsque le refus est dépourvu de « *motif valable* »^[81]. La jurisprudence soutient que cela relève de la bonne foi dans l'exécution du contrat ^[82]. Pour l'employeur il conviendra alors de prendre en considération la situation familiale du salarié, mais également la volonté du salarié de ne pas accepter la modification du contrat de travail induite par la formation. Par ailleurs, le refus d'un salarié d'accepter une formation visant à faciliter son adaptation aux modifications de son poste pourra lui être reproché et justifier son licenciement pour inaptitude professionnelle en cas d'incapacité à tenir le poste.

B. L'acceptation de la modification du contrat

Afin de mieux comprendre ce que l'employeur peut imposer ou pas au salarié, il faut distinguer la modification du contrat de travail du changement des conditions de travail. Si le salarié peut refuser la modification de son contrat de travail, il ne peut pas refuser le changement des conditions de travail, sauf s'il est protégé, sous peine de commettre une faute^[83]. La modification du contrat recouvre la rémunération, la durée du travail, le lieu de travail et la qualification professionnelle. Ainsi, un simple changement de tâche correspondant à la qualification du salarié s'apparente à un changement des conditions de travail et non à une modification du contrat^[84]. A *contrario*, les nouvelles technologies peuvent avoir un impact important sur la qualification des travailleurs et conduire à la modification du contrat. Dans cette hypothèse, l'employeur ne pourra pas imposer la modification du contrat au salarié. Notons que le refus du salarié ne peut constituer en soi une cause réelle et sérieuse de licenciement^[85]. Par conséquent, soit l'employeur renonce à la modification du contrat, soit il engage une procédure de licenciement qui devra être fondée non pas sur le refus du salarié, mais sur le motif l'ayant poussé à proposer la modification. Ainsi, en cas de modification du contrat de travail consécutive à un motif économique. L'employeur devra faire la proposition de modification au salarié par lettre recommandée avec accusé de réception, lequel aura alors un mois pour répondre. A défaut de réponse, il sera réputé avoir accepté la modification proposée^[86]. S'il refuse, soit l'employeur renonce à la modification du contrat, soit il engage une procédure de licenciement pour motif économique en précisant la nature de ce dernier^[87]. L'accord exprès du salarié doit être recueilli avant de procéder à la modification. A défaut, le salarié pourra prendre acte de la rupture de son contrat ou engager une procédure de résiliation judiciaire. Quand bien même le salarié refuserait la modification du contrat, il se verra à la merci d'un éventuel licenciement. En cela, les nouvelles technologies conduisent l'homme à s'adapter aux évolutions.

Alors qu'elles peuvent être de véritables outils de libération des travailleurs, en permettant le télétravail, en allégeant la charge de travail, les NTIC peuvent également être des outils de soumission de la main d'œuvre. En réalité elles ne sont ni un ennemi du travail, ni un allié. Leur

caractère de neutralité dépend de la façon dont elles sont utilisées. Si en matière économique, l'entreprise se doit de maintenir sa compétitivité par le biais de l'innovation, et par conséquent d'intégrer les NTIC et d'adapter ses salariés, il n'en va de même en ce qui concerne les nouvelles formes de surveillance permises par celles-ci. Se pose ici la question de la place de la bonne foi dans l'exécution du contrat. En effet, le pouvoir de subordination se trouve *a priori* renforcé par l'existence de ces nouveaux moyens de contrôle. Les NTIC conduisent les employeurs à utiliser des moyens de contrôle de plus en plus sophistiqués.

TITRE 2. Les NTIC, instrument de contrôle des salariés

Dans son rapport sur les libertés publiques et l'emploi de 1991, Gerard LYON CAEN affirme « *qu'il existe un nouvel espace public 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* ». La surveillance du salarié s'entend de la surveillance opérée par un employeur soit directement par lui ou alors par l'intermédiaire d'un supérieur hiérarchique, ou par le biais de procédés techniques particuliers. La surveillance des salariés est différemment envisagée avec l'intervention des TIC. Finalement elle soulève de nombreuses questions notamment celle de la frontière entre vie privée et vie professionnelle. La possibilité pour un employeur de surveiller son salarié est liée à l'existence d'un lien de subordination. La Cour de cassation affirme cette possibilité depuis un arrêt du 20 novembre 1991 dans lequel elle affirme que l'employeur a le droit de surveiller l'activité de ses salariés pendant le temps de travail.

Le lien de subordination fait naître pour l'employeur des prérogatives de contrôle et de sanction des comportements considérés comme fautifs. Les NTIC vont lui offrir des moyens nouveaux, et variés de contrôle et de surveillance. Toutefois, ce pouvoir est limité par certaines conditions érigées par le Code du travail, et par la jurisprudence. Ces gardes fous visent à garantir au salarié le respect de ses droits fondamentaux, et à tendre vers l'équilibre de la relation contractuelle. Cela passe en premier lieu par la proportionnalité des moyens de surveillance mis en œuvre. En effet, au terme de l'article L.1121-1 « *nul ne peut 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* ». Si la simple surveillance d'un salarié faite sur les lieux de travail par son supérieur hiérarchique ne constitue pas en soi un mode de preuve illicite - même en l'absence d'information préalable de l'intéressé^[88] - la mise en place de dispositifs spécifiques implique le respect du principe de transparence. Ce principe est posé à l'article L.1222-4 du Code du travail qui énonce qu'« *aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance* ». Cette disposition a en partie pour but de veiller à ce que « *le contrat de travail [soit] exécuté de bonne foi*^[89] ». Les articles L.1121-1 et L.1222-4 ont débouché sur la jurisprudence Neocel^[90], au terme de laquelle les juges du Quai de l'horloge estime que si l'employeur a le droit de contrôler l'activité des salariés, il ne peut mettre en œuvre un dispositif de contrôle qui n'a pas été porté préalablement à la connaissance des salariés. Outre l'information individuelle, les IRP peuvent être amenées à être consultées. L'article L.2323-32 dispose que le comité d'entreprise doit être informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens et les techniques permettant un contrôle de l'activité des salariés. Tant qu'aux délégués du personnel, l'article L2313-2 du Code du travail leur confère un droit d'alerte, en cas d'atteinte aux droits des personnes ou aux libertés individuelles. Enfin, rappelons que la CNIL doit en principe être saisie préalablement à la mise en place d'un traitement automatisé d'informations nominatives.

Traditionnellement, le contrôle des salariés s'effectue principalement sur le temps et le lieu de

travail. Les NTIC permettent à l'employeur de disposer de moyens plus importants de contrôle au sein même de l'entreprise (Chapitre1). Le lien de subordination apparait en théorie renforcé. Les TIC ne sont pas uniquement des moyens de renforcement du contrôle interne. Elles sont aussi la possibilité pour l'employeur d'étendre ce pouvoir en dehors même de l'entreprise (Chapitre 2). En effet, les systèmes de connexion permanents tels que la géolocalisation, ou encore les conséquences des réseaux sociaux sur l'affaiblissement de la sphère privée l'amène à être de plus en plus omniprésent.

Chapitre 1. Un contrôle opéré au sein de l'entreprise

L'entreprise est le lieu où l'employeur dispose du pouvoir de contrôle le plus important. Sur les temps et lieux de travail la légitimité de son pouvoir est à son paroxysme. Les salariés doivent accomplir les tâches pour lesquelles ils ont été embauchés. Dès lors, les contrôles opérés par un supérieur hiérarchique ne nécessitent aucune formalité préalable. Un salarié ne peut se prévaloir du fait qu'il n'avait pas été informé de la surveillance effectuée par son supérieur. Cette surveillance ressort naturellement du contrat de travail. La seule limite en la matière ressort en réalité de la bonne foi contractuelle : si le salarié doit exécuter loyalement ses tâches, l'employeur ne doit pas utiliser de stratagèmes pour le surveiller. Toutefois, cette surveillance est différemment envisagée avec l'intervention des TIC. Quand bien même l'employeur dispose de moyens lui permettant d'accroître théoriquement son pouvoir de contrôle de l'activité, on pense à la surveillance opérée par le biais de l'outil informatique (Section1), de nombreuses conditions doivent être respectées. Outre le poste informatique, de nouveaux moyens divers et variés subsistent, ou ont vu le jour. Là encore, si le contrôle de l'activité des salariés (section 2) semble plus simple à effectuer, c'est sans compter les règles de droit qui viennent s'ériger face à l'accroissement des possibilités de surveillance.

Section 1. La surveillance de l'outil informatique

L'utilisation de l'ordinateur professionnel du salarié doit se borner à l'exécution des tâches pour lesquelles il a été embauché. Si une utilisation personnelle de l'ordinateur est souvent tolérée, celle-ci doit d'être raisonnable. Dans le cas contraire, cela ferait apparaître un manquement du salarié à ses obligations contractuelles. Dans le cadre de son pouvoir de surveillance, l'employeur est en droit de contrôler, dans des conditions bien déterminées, le contenu de l'ordinateur (paragraphe 1). La surveillance de l'ordinateur passe également par le contrôle de son utilisation (Paragraphe 2).

Paragraphe 1. La surveillance du contenu de l'ordinateur

Si l'employeur peut avoir accès au contenu de l'ordinateur, il doit respecter un certain nombre de conditions (A). Le respect de ces conditions conditionnera l'utilisation qu'il pourra en faire (B).

A. Les conditions d'accès au contenu de l'ordinateur du salarié

L'arrêt NIKON du 2 octobre 2001 pose le principe selon lequel il existe une sphère de vie privée même au temps et au lieu de travail. Par conséquent les salariés ont droit à l'intimité de leur vie privée même lorsqu'ils sont sous la subordination de l'employeur. De ce principe découle le secret des correspondances. C'est ainsi que « *l'employeur ne peut 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* »^[91]. Cet attendu de la Cour de cassation était particulièrement protecteur. S'il protégeait bel et bien la vie privée du salarié, il ne permettait pas à l'employeur d'exercer les prérogatives qui sont les siennes, à savoir

les pouvoirs de contrôle et de sanction. C'est pour cette raison que la protection accordée aux salariés s'est par la suite fortement atténuée.

Aujourd'hui, « *sauf risque ou événement particulier, l'employeur ne peut ouvrir les messages identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé* »^[92]. Les fichiers et dossiers présents sur l'ordinateur professionnel du salarié relèvent du même régime juridique. Dans un arrêt du 18 octobre 2006, la Cour de cassation énonce 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* »^[93]. Par conséquent, si un salarié ne souhaite pas que l'employeur ouvre en dehors de sa présence un fichier ou un courriel, il se doit de préciser la mention « personnel ». Dans le cas contraire, l'employeur bénéficie d'une présomption de professionnalité du contenu de l'ordinateur. Quand est-il lorsque le courrier ou le fichier comporte la mention « personnel » ? Il faut considérer que « *dans une telle hypothèse, dès lors que la formulation utilisée confère au courrier ou au fichier un caractère privé, même s'il n'est pas formellement identifié comme personnel, l'employeur ne devrait pas être autorisé à l'ouvrir en dehors de la présence du salarié* »^[94]. L'arrêt « société Nova régie » du 18 octobre 2011 semble apporter un nouvel élément en mentionnant la notion de « signe distinctif ». La Cour énonce que l'employeur avait pu légalement avoir accès au contenu des messages car ils « *n'étaient pas identifiés par le salarié comme étant personnels et qu'ils étaient sans signe distinctif dans sa messagerie professionnelle* ». Notons que la mention par défaut « Mes documents » du logiciel Windows, ne confère pas au fichier « *un caractère personnel, et l'employeur peut valablement y accéder en dehors de la présence du salarié* »^[95]. Par ailleurs le 21 octobre 2009, la Cour de cassation affirme que la simple mention des initiales du salarié ne suffit pas à donner un caractère personnel au fichier^[96]. Il en va de même pour le fichier ou le courrier qui ne ferait que mentionner le prénom du salarié^[97], ou qui indiquerait « *essais divers, essais divers B, essais divers restaurés* »^[98]. Enfin, le 4 juillet 2012, la même cour précise que « *la dénomination donnée au disque dur lui-même ne peut conférer un caractère personnel à l'intégralité des données qu'il contient* »^[99]. En l'espèce un salarié avait stocké sur le disque dur de son ordinateur professionnel une grande quantité de fichiers à caractère pornographique ayant conduit à son licenciement pour faute grave. L'argumentation de la défense s'appuyait sur le fait que l'employeur ne pouvait se fonder sur le contenu du fichier en raison de sa dénomination « personnel ». De plus, quand bien même il aurait pu y avoir accès, l'employeur ne pouvait se fonder sur un motif tiré de la vie privée pour fonder un licenciement pour faute grave. Ce qu'il faut retenir, c'est que ce n'est pas le contenu pornographique en lui-même des fichiers qui fonde le licenciement, mais le manquement aux obligations contractuelles du salarié. Dans cet arrêt, le nombre important de fichiers et les fausses attestations ont caractérisé l'abus de droit.

La CNIL recommande dans sa fiche pratique « *le contrôle de l'utilisation d'internet et de la messagerie* »^[100] d'informer les salariés sur le principe retenu pour différencier les e-mails professionnels des e-mails personnels. Cette information peut par exemple prendre la forme d'une charte. Assez récemment, la Cour de cassation est venue étoffer sa jurisprudence en matière de fichiers informatiques à propos du contenu d'une clé USB. Dans un arrêt du 12 février 2013, la Haute juridiction énonce que « *qu'une clé USB, dès lors qu'elle est connectée à un outil informatique mis à la disposition du salarié par l'employeur pour l'exécution du contrat de travail, étant présumée utilisée à des fins professionnelles, l'employeur peut avoir accès aux fichiers non identifiés comme personnels qu'elle contient, hors la présence du salarié* »^[101]. La clé USB en question était pourtant la propriété du salarié sanctionné. C'est le fait qu'elle soit connectée à l'ordinateur professionnel qui est venu justifier la décision. Par conséquent, la clé USB personnelle d'un salarié qui serait simplement posée sur son poste de travail ne pourrait faire l'objet d'une

ouverture licite par l'employeur. *A contrario*, la clé USB professionnelle remise par l'employeur suivrait le même régime que celui de l'ordinateur précédemment évoqué. Si cette jurisprudence peut se justifier techniquement, elle ouvre cependant la voie à de possibles débordements. On sait aujourd'hui que la faible autonomie des Smartphones pousse nombre de leur propriétaire à les recharger sur le lieu de travail, notamment par le biais des supports USB. Est-ce à dire que dans ce cas de figure l'employeur serait en droit d'accéder aux téléphones de ses salariés ? Le mobile pouvant être de surcroît personnel, et étant donné son caractère extrêmement privé, on doute que la Cour de cassation aille jusqu'au bout de la logique.

B. Les conditions d'utilisation du contenu de l'ordinateur

Le 18 mai 2007 la chambre mixte de la Cour de cassation pose le principe selon lequel l'employeur ne peut, « *sans méconnaître le respect dû à la vie privée du salarié, se fonder sur le contenu d'une correspondance privée pour sanctionner son destinataire*^[102] ». Cette protection ne s'applique pas lorsqu'un courriel privé a été transmis par inadvertance à l'employeur^[103]. En 2011, les magistrats réaffirment ce principe. Selon eux, « *si l'employeur peut toujours consulter les fichiers qui n'ont pas été identifiés comme personnels par le salarié, il ne peut les utiliser pour le sanctionner s'ils s'avèrent relever de sa vie privée*^[104] ». En revanche, s'il s'avère que le contenu du fichier ou du courriel en question est en rapport avec l'activité professionnelle du salarié, il pourra être retenu pour fonder une sanction disciplinaire^[105]. Cela sera notamment le cas lorsque le contenu en question illustre un manquement de l'intéressé à ses obligations contractuelles^[106]. Il en sera ainsi lorsque le salarié aura tenu des propos injurieux ou excessifs^[107]. Cette solution vaut également lorsque le salarié se sera risqué à mener des activités illicites en utilisant le matériel de l'entreprise. Dans l'arrêt « société Nova Régie » (*op-cit*), les courriels litigieux montraient que le salarié vendait de la drogue à des tiers. La Cour de cassation juge son licenciement pour faute grave justifié pour « *commerce illicite en utilisant son ordinateur professionnel et les services d'accueil de la société*^[108] ».

Paragraphe 2. La surveillance de l'utilisation de l'ordinateur

Deux grandes problématiques sont posées par la surveillance de l'utilisation de l'ordinateur. D'une part la nécessité de protéger le système informatique et la sécurité de l'entreprise. Cette mission revient la plus part du temps à l'administrateur réseau (A) qui se trouve dans une position délicate. D'autre part, l'outil informatique dont dispose le salarié est souvent mis à sa disposition par l'employeur. Pour ce dernier il est donc légitime d'attendre que cet outil soit mis au profit de l'activité professionnelle, et non au service des occupations privées. Pour autant, toutes les formes de surveillance ne sont pas permises

A. La position délicate de l'administrateur réseau

En matière de cyber surveillance, les administrateurs réseaux occupent un rôle central. Ces derniers sont chargés de la sécurité informatique de l'entreprise. A ce titre, ils peuvent par le biais des moyens dont ils disposent accéder à des informations personnelles des salariés. Afin d'illustrer cette problématique, il convient de faire référence à un arrêt rendu par la chambre sociale de la Cour de cassation le 17 juin 2009. En l'espèce, un employeur soupçonnait dix-sept salariés d'avoir eu connaissance de données confidentielles (l'entreprise en question était classée Seveso). Il demande alors à l'administrateur réseau de surveiller leurs postes de travail, et de lui transmettre les informations obtenues. La Cour de cassation s'est demandée si les messages « *qualifiés de personnels ou pouvant, de par leur classement, être considérés comme tels avaient été ouverts dans le seul cadre de la mission confiée à l'administrateur réseaux ou s'ils l'avaient été par l'employeur*^[109] ». Pour Sandrine Maillard, ce raisonnement sous-tend le fait que « *si l'employeur ne peut pas accéder aux messages qualifiés de personnel ou pouvant, de par leur classement, être considérés comme tel, l'administrateur réseaux qui est tenu d'une obligation de*

confidentialité peut ouvrir ces messages personnels dans le cadre de sa mission de sécurité des réseaux informatiques^[110] ». En raison de son obligation de sécurité, l'administrateur ne peut en aucun cas transférer les messages « personnels » à l'employeur quand bien même il lui demanderait. La possibilité d'ouvrir les messages des salariés s'inscrit uniquement dans le cadre de ses missions. Autrement dit, cela doit être justifié par un impératif de sécurité. Toutefois, si « *la préoccupation de la sécurité du réseau [justifie] que les administrateurs de systèmes et de réseaux fassent usage de leurs positions et des possibilités techniques dont ils [disposent] pour mener les investigations et prendre les mesures que cette sécurité [impose], la divulgation du contenu des messages (...) ne [relève] pas de ces objectifs*^[111] ». En outre, l'administrateur se doit de garantir la sécurité du système, et prendre les mesures qui s'imposent. Ce dernier peut alors se trouver dans une situation délicate. Car s'il doit détecter et sécuriser la faille, les moyens dont il dispose peuvent se trouver limiter. Il peut par exemple décider de restreindre l'accès au web des salariés concernés, mais « *s'agit-il d'une mesure de sécurité relevant du pouvoir de l'administrateur réseaux ou d'une mesure disciplinaire relevant du pouvoir de l'employeur ?*^[112] ». D'un autre côté, les informations qu'il peut communiquer à l'employeur sont limitées. A noter également que s'il vient à ouvrir des messages personnels sans raison, il risque des poursuites pénales au titre de la violation du secret des correspondances^[113]. En tout état de cause, l'administrateur réseau ne pourra sanctionner des utilisations abusives, ce pouvoir étant exclusivement réservé à l'employeur.

2. L'employeur et la surveillance de l'utilisation de l'ordinateur

Si l'employeur a toute la légitimité pour exiger une utilisation professionnelle de l'ordinateur, les moyens dont il dispose pour s'en assurer ne sont pas illimités. Ainsi, proportionnalité des moyens et loyauté sont à nouveau exigés. On peut comprendre qu'un employeur puisse être tenté de mettre en place des logiciels espions sur les postes informatiques des salariés afin de s'assurer qu'ils sont bien entrain de travailler. A titre d'exemple, on peut citer les "keyloggers". Ces logiciels sont des dispositifs de surveillance qui se lancent automatiquement à chaque démarrage du poste informatique, et ce à l'insu de son utilisateur. Ce type de dispositif doit faire l'objet d'une information préalable des IRP au titre de l'article L.2323-32 du Code du travail, et d'une information individuelle des salariés concernés^[114]. De tels dispositifs doivent être déclarés auprès de la CNIL, pour laquelle ces derniers ne peuvent se justifier que pour de forts impératifs de sécurité. A défaut, les preuves obtenues par l'employeur seraient irrecevables dans un litige l'opposant à un salarié. En outre, depuis la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011, la CNIL a rappelé que le fait d'utiliser des « *dispositifs de captation de données informatiques à l'insu des personnes concernées* » est puni de 5 ans d'emprisonnement et de 300 000 euros d'amendes^[115].

Si l'employeur ne peut contrôler par n'importe quel moyen l'utilisation qui est faite de l'ordinateur, il peut être légitime à le faire en raison des abus susceptibles d'être commis. S'il est déconseillé d'interdire totalement l'utilisation à titre personnel de l'outil professionnel - au risque de voir cette décision condamnée pour non-respect du principe de proportionnalité^[116] - il semble important, au vu des nombreuses tentations que suscite le web, d'en limiter l'accès. Cela pourra ainsi éviter à certains de se voir licencier pour faute grave. En effet, il est acquis que l'utilisation personnelle et abusive d'internet à partir de l'ordinateur professionnel est un cas de licenciement pour faute grave^[117]. Cette sanction trouve son fondement dans la violation des obligations contractuelles du salarié. Ainsi, dans un arrêt du 18 mars 2009 la Cour de cassation a considéré qu'un salarié pouvait être licencié pour faute car il avait usé de la connexion internet de l'entreprise à des fins non professionnelles pour une durée d'environ 41 heures sur un mois^[118].

Section 2. Le contrôle de l'activité des salariés

La surveillance des faits et gestes des salariés au sein de l'entreprise s'explique par le lien de subordination. Les salariés étant sur le temps et le lieu de travail, l'employeur dispose d'un pouvoir de contrôle afin de s'assurer qu'ils exécutent leurs obligations contractuelles. Cela passe par le contrôle de l'activité des salariés (Paragraphe 1), et par le contrôle des accès au sein même de l'entreprise (Paragraphe 2). Si les moyens utilisés peuvent être légitimement justifiés par un objectif économique, ils peuvent aussi démontrer une certaine crise de confiance entre les parties dans la relation contractuelle.

Paragraphe 1. Les écoutes téléphoniques et les enregistrements sonores

Outre l'ordinateur que le salarié peut être amené à utiliser dans le cadre de son activité professionnelle, d'autres moyens de communication peuvent lui être confiés telle qu'une ligne téléphonique (A). Par ailleurs, l'employeur peut être amené à utiliser un dispositif d'écoute qui fait l'objet d'un encadrement très strict (B).

A. Le contrôle des communications téléphoniques

Il est établi que l'utilisation abusive des moyens de communication de l'entreprise à des fins personnelles est un motif valable de licenciement pour faute grave^[119]. Le juge est le seul à pouvoir apprécier si la sanction est justifiée. Il tiendra compte des pratiques de l'entreprise, mais encore du salarié en question (ancienneté etc.). Pour pouvoir sanctionner, encore faut-il détenir des preuves licites. Le contrôle des communications téléphoniques peut être opéré par deux moyens que sont l'autocommutateur (a), et les factures détaillées (b).

a. Le contrôle des communications par le biais des autocommutateurs

La mise en place d'un autocommutateur permet à l'employeur d'enregistrer les numéros appelés à partir des postes téléphoniques. Il lui devient alors possible de connaître la date, l'heure, la durée, et le coût de la communication. Etant donné qu'il est possible d'identifier les interlocuteurs, l'employeur a la possibilité de vérifier si le temps passé relève ou non d'un usage professionnel. En raison du caractère intrusif de ce dispositif, plusieurs conditions doivent être respectées.

La première d'entre elle consiste à en déclarer l'existence auprès de la CNIL. Notons que depuis le 3 février 2005, les traitements de données à caractère personnel mis en place par le biais des moyens de communication, qu'ils soient fixes ou mobiles, bénéficient de la procédure de déclaration simplifiée^[120]. La norme simplifiée n°47 précise un certain nombre de modalités. C'est ainsi que les finalités de ce contrôle sont limitées à la gestion des moyens de communication et à la maîtrise des dépenses liées à l'utilisation des services de téléphonie. Il en découle une interdiction expresse d'utiliser l'autocommutateur dans le but d'écouter, d'enregistrer des conversations, ou de localiser un salarié à partir de son téléphone portable. Notons que des mesures particulières doivent être prises au bénéfice des salariés protégés. En la matière, la CNIL et la Cour de cassation exigent que « *pour l'accomplissement de leurs missions légales et la préservation de la confidentialité qui s'y attache les salariés investis d'un mandat électif ou syndical dans l'entreprise doivent pouvoir y disposer d'un matériel ou procédé excluant l'interception de leurs communications téléphoniques et l'identification de leurs correspondants* »^[121]. Cette exigence a été étendue à tous les salariés protégés, qu'ils aient un mandat à l'intérieur ou à l'extérieur de l'entreprise^[122]. Toutefois, la Cour de cassation a précisé que « *la simple vérification des relevés de la durée, du coût et des numéros des appels téléphoniques passés à partir de chaque poste édités au moyen de l'autocommutateur téléphonique de l'entreprise ne constitue pas un procédé de surveillance illicite pour n'avoir pas été préalablement porté à la connaissance du salarié* »^[123].

Le régime juridique de l'autocommutateur est différent lorsqu'il s'agit des salariés protégés. Ces derniers ont droit à la confidentialité de leurs communications, et doivent donc disposer d'une ligne non dotée d'un dispositif permettant d'intercepter leurs communications, et d'identifier leurs correspondants^[124]. Dans un arrêt du 4 avril 2012, la Cour de cassation précise que ce régime s'applique pour tous les salariés protégés, qu'ils exercent ou non leurs mandats au sein de l'entreprise^[125]. Le secret des communications « *s'applique aux lignes de téléphone fixes ce qui suppose qu'elles ne soient pas reliées à un autocommutateur, ainsi qu'aux portables professionnels, ce qui interdit à l'employeur d'examiner les relevés détaillés des correspondances* »^[126]. Un autre type de contrôle moins intrusif, mais qui peut se révéler tout aussi efficace consiste à vérifier les factures détaillées.

b. Le contrôle des communications par le biais des factures détaillées

Le contrôle des communications par le biais des factures détaillées fait l'objet d'une appréciation plus souple par la Cour de cassation. Celle-ci refuse de considérer que leur utilisation constitue un moyen de contrôle. Par conséquent elle n'exige pas que les salariés soient préalablement informés de ce type de vérification^[127]. La production par l'employeur des relevés de facturation téléphonique constitue donc un mode de preuve licite. Il convient cependant d'être vigilant en raison de la position de la CNIL qui se montre beaucoup plus réticente sur le sujet. Cette dernière estime que lorsque l'employeur contrôle les communications du personnel à l'aide d'une facture détaillée, il doit en informer les salariés concernés dès lors que le contrôle poursuit la même finalité que celle de l'utilisation d'un autocommutateur^[128]. La position de la Cour de cassation est donc susceptible d'évoluer.

B. L'encadrement strict des enregistrements sonores

Les écoutes et les enregistrements sont susceptibles de constituer un délit. L'article 226-15 du Code pénal incrimine le fait 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 de façon

intentionnelle. De tels procédés constituent une atteinte à la vie privée lorsque la personne n'en a pas été informée. Il ne suffit pas d'aviser à l'avance un salarié que ses communications téléphoniques sont susceptibles d'être écoutées. Il faut avant tout recueillir son consentement. Plusieurs conditions cumulatives sont nécessaires à l'utilisation de tels dispositifs. Tout d'abord, aucune écoute ou enregistrement permanent des conversations des salariés ne peut être mis en œuvre de façon permanente. Ceux-ci doivent être justifiés et proportionnés au but recherché. Par conséquent, on ne peut y recourir que de façon sporadique. Cela recouvre des possibilités très limitées, tels que les enregistrements effectués pour la formation du personnel afin d'améliorer l'accueil téléphonique. Ils ne peuvent nullement être utilisés à des fins de surveillance. Les autres conditions sont celles rencontrées précédemment, à savoir la déclaration préalable auprès de la CNIL (lorsque les écoutes donnent lieu à enregistrement et à conservation), l'information et la consultation des institutions représentatives du personnel, et l'information des salariés. Ces derniers doivent être informés des objectifs poursuivis par la mise en place du dispositif d'écoutes, des destinataires des enregistrements, et de leur droit d'accès à ces derniers.

Outre les sanctions pénales, l'employeur ne pourra nullement se prévaloir de moyens de preuves obtenus par le biais d'un dispositif d'écoutes ou d'enregistrements dès lors que les conditions sus-évoquées n'auraient pas été respectées. Ainsi, l'enregistrement d'une conversation téléphonique privée à l'insu de l'auteur est un procédé déloyal ayant pour conséquence de rendre irrecevable la preuve obtenue^[129].

Paragraphe 2. Le contrôle de l'activité par la vidéosurveillance

Durant l'année 2011, la CNIL a eu à traiter plus de 360 plaintes concernant la vidéosurveillance, soit une augmentation de 32 % par rapport à l'année 2010. 60 % de ces plaintes concernaient la vidéosurveillance au travail^[130]. La mise en place d'un tel système nécessite le respect de certaines conditions très strictes (A) posées par la loi, la CNIL, et par la jurisprudence. Le non-respect de ces conditions conduira *de facto* à de possibles sanctions (B).

A. Les conditions du recours à la vidéosurveillance

Le recours à la vidéosurveillance est limité par les principes généraux posés par le Code du travail (a), et par le contrôle préalable opéré par la CNIL (b).

a. Les conditions posées par le Code du travail

Une caméra implantée sur le lieu de travail ne peut poursuivre qu'un seul but : la sécurisation des personnes et des biens. Les caméras peuvent être installées aux entrées et aux sorties des bâtiments, dans les axes de circulation, de stockage et les issues de secours. En aucun cas, elles ne doivent par principe filmer un salarié sur son poste de travail. Une zone de repos ou de pause ne doit pas être filmée. Il en va de même du local réservé aux représentants du personnel. L'article L.1221-1 du Code du travail énonce que « *nul ne peut 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* ». De ce principe général découle le fait que la vidéosurveillance ne peut être mise en place de n'importe quelle façon. En outre, il ne peut être procédé à la surveillance permanente des salariés sur leur poste de travail. La CNIL veille à ce que ce principe de proportionnalité soit respecté. A titre d'illustration, elle a récemment sanctionné un dispositif de surveillance dont il se trouvait que la finalité première était de contrôler l'activité et la présence des agents de sécurité^[131]. La caméra en question était orientée de façon à ce que les salariés soient en permanence filmés. Par conséquent, « *le dispositif a été jugé disproportionné en ce qu'il ne participait pas à la protection des occupants de l'immeuble mais témoignait en réalité de la volonté du responsable de traitement de contrôler le travail du personnel de surveillance* »^[132].

Le principe de proportionnalité conduit à limiter l'usage de la vidéosurveillance.

L'autre principe visant à encadrer le recours à la vidéosurveillance est le principe de la transparence. Celui-ci vise à veiller au maintien de la bonne foi dans la relation contractuelle. C'est ainsi que la mise en place d'un système de vidéosurveillance implique l'information et la consultation des IRP, ainsi que l'information individuelle des salariés. Le comité d'entreprise se voit compétent dès lors que la mise en place d'un système de surveillance vise un but de management. Lorsque c'est le cas, « *le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés* »^[133]. Par ailleurs, « *le fait de savoir que nos gestes et mouvements sont suivis dans le cas de la surveillance généralisée et continue, peut avoir un impact psychologique important qui consiste à ajuster en permanence notre comportement aux attentes de ceux qui nous regardent* »^[134]. Au regard des conséquences possibles sur la santé mentale des salariés, il paraît opportun d'informer et de consulter également le CHSCT malgré le fait qu'aucun texte ne le prévoit. Notons que l'information et la consultation doivent porter sur la mise en place, mais aussi et surtout sur les utilisations éventuelles à des fins de surveillance. Outre l'information préalable des IRP, chaque salarié concerné doit avoir été individuellement informé conformément à l'article L.1222-4 du même code qui dispose qu'« *aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance* ». Cette information doit se faire par courrier (ou courriel) individuel, ou peut figurer dans le contrat de travail. Il est également impératif de les informer par le biais d'un panneau d'affichage précisant l'existence du dispositif, le nom de son responsable, et la procédure à suivre pour demander l'accès aux enregistrements visuels les concernant^[135]. Dans un arrêt du 10 janvier 2012^[136], la chambre sociale de la Cour de cassation vient préciser que cette obligation incombe également à l'employeur lorsque le dispositif est mis en place par un tiers dans ses locaux. Ce qui est intéressant dans ce cas d'espèce, est le fait que l'employeur avait bien averti ses salariés de la présence de vidéosurveillance. La Cour justifie sa décision en affirmant que le chef d'entreprise n'avait pas expressément mentionné « *que le dispositif mis en place [pouvait] servir à surveiller l'activité du personnel intervenant* »^[137]. L'information donnée par l'employeur est une information qui doit être claire et précise. Les salariés doivent connaître les utilisations possibles des enregistrements et les finalités du contrôle ainsi opéré.

b. La déclaration préalable auprès de la CNIL

La CNIL a en la matière un rôle de premier plan à jouer, car « *à moins que les images ne soient ni enregistrées ni conservées dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques, la mise en place de la vidéosurveillance doit faire l'objet d'une déclaration auprès de la Cnil* »^[138]. Deux régimes sont à distinguer. Lorsque les caméras filment un lieu ouvert au public le dispositif doit être déclaré à la CNIL pour chaque site ou établissement équipé. Toutefois, lorsqu'au sein de l'entité concernée, il existe un Correspondant informatique et liberté (CIL), aucune formalité ne doit être réalisée par l'employeur. En revanche, lorsque les caméras filment un lieu ouvert au public (espaces d'entrée et de sortie du public, caisses), le dispositif doit être autorisé par le préfet du département. La CNIL peut être amenée à effectuer des contrôles au sein des établissements et dispose d'un pouvoir de sanction. Elle s'assure le cas échéant, du respect du droit du travail, de la finalité légitime du dispositif, et que la visualisation des images soit limitée aux seuls destinataires habilités. Notons qu'en matière de vidéosurveillance, les images ne peuvent être conservées plus d'un mois^[139].

Dès lors que la mise en place d'un dispositif de surveillance vidéo ne respecte les conditions précitées, l'employeur ne pourra s'appuyer sur les preuves qu'il aura obtenues. Par ailleurs, il s'expose à des sanctions pécuniaires, et à de lourdes sanctions pénales.

B. Les sanctions du non-respect des conditions de recours à la vidéo surveillance

L'application des conditions de recours à la vidéosurveillance vont venir conditionner l'utilisation que l'on peut en faire. Sur la question, il existe une divergence jurisprudentielle entre la Chambre sociale et la Chambre criminelle de la Cour de cassation. En droit du travail, le non-respect des conditions de mise en place conduit à l'illicéité des preuves obtenues (a). Outre le fait que la preuve devient inopposable, des sanctions prononcées par la CNIL et par les juridictions pénales peuvent être encourues (b).

a. L'illicéité des preuves obtenue de façon déloyale

L'application des conditions de recours à la vidéosurveillance vont venir conditionner l'utilisation que l'on peut en faire. En effet, dès lors que les salariés, les IRP, ou encore la CNIL n'ont pas été informés de la mise en place du dispositif, toute preuve apportée par le biais de la vidéosurveillance serait inopposable au salarié. La preuve obtenue serait alors irrecevable et ne pourrait venir à l'appui d'une sanction disciplinaire ou d'un licenciement. Ce principe a été posé à l'occasion d'une affaire dans laquelle un employeur avait installé une caméra dans une caisse afin de surveiller le comportement d'une salariée à son insu. La Cour de cassation a alors refusé de retenir le moyen de preuve obtenue en raison de l'absence de transparence du dispositif mis en place^[140]. En 2006, sous le visa l'article L.2323-32, la Cour de cassation a rappelé que « *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* »^[141]. En l'espèce il s'agissait d'un salarié licencié pour faute grave pour avoir commis un vol. L'employeur rapportait la preuve de sa prétention *via* les enregistrements vidéo des caméras de surveillance du magasin. La Cour d'appel avait retenu le mode de preuve en se justifiant par le fait que le salarié ne pouvait ignorer l'existence du dispositif. Toutefois, le comité d'entreprise n'avait pas été consulté car le dispositif avait pour finalité la surveillance des clients du magasin et non des salariés. Dès lors, l'absence d'information et de consultation du CE avait pour conséquence de rendre le mode de preuve illicite. Il faut savoir que les délégués du personnel ont un rôle important à jouer en la matière. En effet, en vertu de l'article L. 2313-2 du Code du travail, ils ont le pouvoir d'agir en justice pour demander le retrait d'éléments de preuve obtenus par des moyens frauduleux lorsque ceux-ci portent atteinte aux droits des personnes et aux libertés individuelles^[142].

A ce principe bien fondé de transparence et de loyauté dans l'administration de la preuve, la Cour de cassation est venue apporter quelques nuances. Dans un arrêt du 2 février 2011, la Haute juridiction affirme que « *lorsque l'ensemble du personnel de la brasserie et du bar d'un casino avait été avisé de la présence de caméras de vidéosurveillance fonctionnant en permanence conformément aux prescriptions réglementaires en la matière, les enregistrements vidéo constituent un mode de preuve licite* ». Résumés, les faits sont les suivants. Un barman avait omis d'encaisser des consommations. Il est licencié pour faute grave, avec preuve vidéo à l'appui. Il soutient que les salariés n'avaient pas été informés du fait que le système qui avait été mis en place pouvait avoir pour finalité de surveiller leurs activités. C'est sans compter le raisonnement de la Cour de cassation qui valide le mode de preuve étant donné que les salariés avaient connaissance de l'existence du dispositif. En ce qui concerne les locaux qui ne sont pas des lieux

de travail, la position jurisprudentielle semble également s'écarter du principe. Dans ces lieux, la Chambre sociale est venue préciser que les enregistrements vidéo sont recevables, quand bien même les IRP et les salariés n'en n'avaient pas eu connaissance. Ce principe est posé par l'arrêt rendu le 31 janvier 2001^[143]. En l'espèce un salarié a été licencié pour faute lourde pour avoir commis des détournements de marchandises. Les preuves rapportées provenaient des caméras installées dans l'entrepôt. Etant donné que le système n'enregistrait pas l'activité de salariés sur un poste de travail, l'employeur n'était pas tenu d'informer les salariés et les IRP. Cette position a été réaffirmée en 2005 à propos de locaux dont les salariés n'avaient pas accès dans le cadre de leurs activités professionnelles. A cette occasion, la Cour de cassation rappelle que « *l'employeur ne peut mettre en œuvre un dispositif de contrôle de l'activité professionnelle qui n'a pas été porté préalablement à la connaissance des salariés* »^[144]. Toutefois, il peut opposer aux salariés des preuves recueillies par les systèmes de surveillance des locaux auxquels les salariés n'ont pas accès dans le cadre de leurs fonctions. Notons que la même solution est retenue concernant la surveillance opérée par une personne. Si l'employeur a la possibilité de surveiller à tout instant ses salariés, il n'en va pas de même de la surveillance opérée par des salariés de l'entreprise. Cependant, lorsque la surveillance est opérée par un salarié au sein de zones non affectées au travail du personnel, les modes de preuves recueillis sont licites^[145].

Enfin, il convient de souligner que sur ces questions de recevabilité de la preuve, la position de la Chambre criminelle est divergente. Ainsi, dans un arrêt 6 avril 1994, elle admet que des enregistrements qui seraient jugés irrecevables devant la Chambre sociale puissent être retenus comme preuve valable en cas de vol commis par un employé. Ceci est justifié par le fait qu'« *aucune disposition légale [en matière pénale] ne permet aux juges répressifs d'écarter les moyens produits au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale* »^[146]. Autrement dit, si un salarié peut voir sa sanction annulée ou son licenciement requalifié comme étant sans cause réelle et sérieuse, il n'est pas à l'abri d'éventuelles sanctions pénales. Outre cette divergence entre la chambre criminelle et la chambre sociale de la Cour de cassation, un débat doctrinal s'est ouvert sur ce principe de loyauté de la preuve. L'existence de ce principe s'explique par le lien contractuel qui unit le salarié et l'employeur. Leur obligation de bonne foi les oblige à avoir un comportement loyal. Toutefois, dans certains cas, il peut paraître choquant de voir un juge écarter un mode de preuve alors même que le fait commis par l'une ou l'autre des parties est incontestable. Ces situations ne servent pas le Droit et la justice, et peuvent aisément caractériser des abus de droits. Il serait alors intéressant que le juge apprécie la preuve qui lui est soumise au regard de la faute commise afin de rendre son jugement.

b. Les sanctions érigées par la CNIL et par le Code pénal

En raison de son statut d'autorité administrative, la CNIL a non seulement la possibilité de mener des enquêtes sur le terrain, mais également de prononcer des sanctions à l'encontre des entreprises qui ne respecteraient pas les prescriptions établies. Dans la plupart des cas, la CNIL met en demeure avant de prononcer une sanction pécuniaire. Lorsque malgré les avertissements, il n'y a aucune mise en conformité, de lourdes sanctions pécuniaires peuvent être prononcées.

Outre les sanctions de la CNIL, le non-respect des dispositions légales sont susceptibles d'entraîner des sanctions pénales. Tout d'abord, l'absence d'information des IRP préalablement à la mise en place de dispositif peut conduire à la qualification du délit d'entrave sanctionné par une peine d'un an d'emprisonnement et de d'une amende de 3750 euros. D'autre part, la captation de l'image d'autrui sans son consentement « *est puni d'un an d'emprisonnement et de 45000 euros d'amende* »^[147]. L'article R.625-10 du Code pénal impose la réalisation d'une information complète comprenant notamment : l'identité du responsable du traitement, de la finalité poursuivie par le traitement, ou encore de ses droits d'opposition, d'interrogation, d'accès et de rectification.

Le non-respect de cette disposition peut être sanctionné d'une contravention de cinquième classe. Notons également que « *le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite*^[148] » ou encore le fait de procéder ou de faire procéder même par négligence « *à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi* » est sanctionné de cinq ans d'emprisonnement et de 300 000 euros d'amende^[149]. La conservation des données au-delà du délai d'un mois prévu par la loi est sanctionnée par la même peine^[150].

Paragraphe 3. Le contrôle des accès de l'entreprise

De nouvelles technologies se sont développées dans ce domaine visant à sécuriser certains lieux sensibles de l'entreprise. Ces moyens visent à limiter les accès aux salariés habilités. Il est possible de distinguer deux grands types de moyen. Les contrôles d'accès par biométrie (A), et par le biais des badges électroniques et des cartes à puce magnétiques (B).

A. Le contrôle des accès par système biométrique

La biométrie recouvre l'ensemble des procédés tendant à identifier un individu à partir de la mesure de l'une ou de plusieurs de ses caractéristiques physiques, physiologiques ou comportementales. Il peut s'agir des empreintes digitales, de l'iris de l'œil, du contour de la main, de l'ADN ou d'éléments comportementaux. La mise en place de ces procédés nécessite l'autorisation préalable de la CNIL, qui exige un impératif de sécurité. Cette exigence s'explique par le danger que fait courir la collecte de telle donnée sur les libertés fondamentales des individus. Néanmoins, il existe une procédure allégée dite de « déclaration de conformité ». Cette procédure permet aux entreprises entrant dans le cadre de l'autorisation unique, de bénéficier d'une procédure de simple déclaration. Seuls deux types de dispositif biométrique font l'objet d'une procédure simplifiée. Il s'agit de ceux ayant pour objectif la reconnaissance du contour de la main, et la reconnaissance de l'empreinte digitale. Toutefois, encore faut-il respecter les finalités édictées par la Commission. Pour le premier dispositif, seul le contrôle d'accès pouvait en bénéficier^[151] (auparavant la gestion des horaires et de la restauration sur les lieux de travail faisait également l'objet de la procédure simplifiée). Pour le second, il est nécessaire que l'empreinte digitale soit exclusivement enregistrée sur un support individuel détenu par le salarié concerné, et qu'elle ait pour finalité le contrôle de l'accès aux locaux sur les lieux de travail.

Au-delà de ces formalités préalables, il va sans dire que la mise œuvre de ce type de contrôle nécessite l'information et la consultation des IRP, ainsi que l'information des salariés sur les finalités du dispositif, et sur la possibilité d'accéder aux données collectées.

B. Le contrôle des accès par badge et carte à puce magnétique

Les systèmes d'accès par badge et par carte à puce magnétique sont moins intrusifs que les systèmes de biométrie. C'est pour cette raison qu'ils doivent simplement faire l'objet d'une déclaration simplifiée^[152]. Ce type de contrôle peut avoir pour but de contrôler l'accès à l'entrée et à certains locaux de l'entreprise, la gestion des horaires variables et des temps de présence, ou encore la gestion de l'accès au restaurant d'entreprise. L'absence de déclaration simplifiée pourra entraîner des sanctions de la CNIL. De plus, dans une telle hypothèse, le refus d'un salarié d'utiliser son badge ne pourra constituer un motif de sanction disciplinaire^[153].

Les badges et les cartes à puce peuvent indéniablement permettre à l'employeur de suivre les déplacements de ses salariés. Or, dans son 10ème rapport d'activité, la CNIL recommande de prévoir uniquement le contrôle des habilitations, et non l'enregistrement des entrées et sorties^[154].

(sauf impératif de sécurité). Par ailleurs, en vertu de l'article L.2315-5 du Code du travail, les représentants du personnel et les délégués syndicaux bénéficient d'une liberté de déplacement. Cela se traduit par la possibilité qui leur ait donné de « *circuler librement dans l'entreprise et d'y prendre tous contacts nécessaires à l'accomplissement de leur mission, notamment auprès d'un salarié à son poste de travail, sous réserve de ne pas apporter de gêne importante à l'accomplissement du travail des salariés* ». L'employeur doit donc s'assurer que les mesures mises en place n'entravent pas cette liberté. En outre, les badges et les cartes à puce ne doivent avoir pour conséquence d'instaurer un véritable contrôle préalable des déplacements. De tels contrôles sont prohibés par la Cour de cassation^[155].

Chapitre 2. Un contrôle qui se poursuit en dehors de l'entreprise

Dans une certaine mesure, les NTIC ont entraîné un certain affaiblissement du pouvoir de subordination directe de l'employeur, notamment par le biais du télétravail. Le salarié se trouvant plus libre dans l'exécution de sa tâche. Toutefois, son pouvoir de contrôle s'est accru au sein de l'entreprise avec l'arrivée de nouveaux moyens de surveillance. Loin de ne s'opérer que dans le cadre de l'entreprise, de nouvelles possibilités ont été ouvertes leur permettant de contrôler son salarié en dehors même de l'entreprise. On pense tout d'abord à la géolocalisation (Section 1). Ce type de contrôle fait l'objet d'un encadrement très strict. S'il est certes un moyen de surveillance efficace pour l'employeur, la CNIL et la jurisprudence érigent des conditions visant à protéger le salarié d'une intrusion trop importante de l'employeur. L'émergence des réseaux sociaux (Section 2) contribue au développement d'une surveillance extra-entreprise. Le stockage de photos, de vidéos sur la toile sont alors un véritable danger pour le salarié. L'exécution du contrat pourrait se voir remise en cause pour des faits relevant de sa vie privée. La jurisprudence tente d'appliquer les principes établis du droit au respect de la vie privée et à la liberté d'expression à ces réalités nouvelles. Toutefois, outre les divergences jurisprudentielles qui existent sur ce terrain, il semble que de nombreuses questions sont susceptibles de se poser. Le décalage entre la rapidité de développement des nouveaux moyens de communication, et le développement du droit, ne doit avoir pour conséquence de remettre en cause les libertés des salariés. La jurisprudence a en la matière un rôle de premier plan.

Section 1. La géolocalisation

La géolocalisation permet de contrôler l'activité des salariés « itinérants » en suivant leur position géographique grâce à la localisation d'objets dont ils ont l'usage (badge, téléphone mobile) ou à la localisation des véhicules qui leur sont confiés. De nombreux argumentaires de vente de systèmes de géolocalisation insistent sur la possibilité pour les employeurs de contrôler la durée du travail, et d'en tirer toutes conclusions utiles. La jurisprudence a mis fin à ces aspirations. Avant tout propos, rappelons que la géolocalisation doit être distinguée des chronotachygraphes. Ces derniers permettent d'enregistrer la vitesse, les temps de conduite, les temps d'attente, etc. Ils sont obligatoirement mis en place dans les véhicules routiers qui transportent des personnes ou des marchandises. Par conséquent, concernant ces dispositifs la problématique de la validité de la surveillance des chauffeurs routiers ne se posent pas. En raison de leur fonction, les chauffeurs routiers sont en charge d'une prestation directement liée à l'utilisation d'un véhicule. Dès lors, même si un dispositif de géolocalisation vient compléter le chronotachygraphe, cela ne peut être considéré comme pouvant porter atteinte à leur liberté d'aller et venir ou à leur vie privée. En revanche, lorsque ce système est mis en place dans les véhicules des salariés pour lesquels l'utilisation d'un véhicule n'est qu'un moyen d'accomplir leurs missions, il peut facilement dévier en moyen de filature électronique des salariés. Une telle surveillance se justifie par le pouvoir de direction de l'employeur, pour lequel il est impératif de surveiller ses salariés afin de s'assurer qu'ils exécutent leur prestation de travail de bonne foi. Toutefois, ce système étant

particulièrement intrusif, le recours à ce type de dispositifs est encadré par la CNIL (Paragraphe 1) et par la jurisprudence (Paragraphe 2).

Paragraphe 1. L'encadrement de la géolocalisation par la CNIL

Les prescriptions de la CNIL en la matière sont inscrites dans la délibération du 16 mars 2006 « portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public » [\[156\]](#). Il est aisé de relever l'existence de deux grandes conditions. La première consiste à respecter les conditions de mise en place du dispositif (A). La deuxième condition implique le respect de formalités préalables (B).

A. Les conditions de mise en place du dispositif de géolocalisation

En raison du caractère intrusif des dispositifs traitant la donnée de géolocalisation des véhicules et des informations qui peuvent y être associées, la CNIL estime que la mise en œuvre de tels dispositifs n'est admissible que dans le cadre de certaines finalités [\[157\]](#). On y retrouve ainsi des impératifs de sécurité. C'est le cas lorsque le dispositif est mis en place afin de veiller à « la sûreté ou la sécurité de l'employé lui-même ou des marchandises ou véhicules dont il a la charge (travailleurs isolés, transports de fonds et de valeurs, etc.) ». D'autres objectifs permettent d'avoir recours à la géolocalisation. On y retrouve les impératifs d'optimisation de l'entreprise et de suivi. Ainsi, la volonté de trouver « une meilleure allocation des moyens pour des prestations à accomplir en des lieux dispersés, (interventions d'urgence, chauffeurs de taxis, flottes de dépannage, etc.) » est un objectif légitime. C'est aussi le cas pour « le suivi et la facturation d'une prestation de transport de personnes ou de marchandises ou d'une prestation de services directement liée à l'utilisation du véhicule (ramassage scolaire, nettoyage des accotements, déneigement routier, patrouilles de service sur le réseau routier, etc.) ». Le suivi du temps de travail peut également justifier sa mise en œuvre, mais uniquement lorsqu'il ne peut être réalisé par d'autres moyens. En revanche, l'utilisation d'un système de géolocalisation ne saurait être justifiée lorsqu'un employé dispose d'une liberté dans l'organisation de ses déplacements (visiteurs médicaux, VRP, etc.). L'employeur qui déclare à la CNIL la mise en place d'un dispositif de géolocalisation pour telle ou telle finalité doit respecter sa déclaration. D'autre part, l'utilisation d'un dispositif de géolocalisation ne doit pas conduire à un contrôle permanent du salarié concerné. C'est pourquoi la CNIL recommande que les employés aient la possibilité de désactiver cette fonction des véhicules à l'issue de leur temps de travail, notamment lorsque ces derniers peuvent être utilisés à des fins privées. Notons que les salariés investis d'un mandat électif ou syndical ne doivent pas faire l'objet d'une opération de localisation lorsqu'ils agissent dans le cadre de l'exercice de leur mandat. Outre le fait que la mise en place d'un dispositif doit répondre à certaines finalités, il est impératif de respecter certaines formalités préalables.

B. Le respect de formalités préalables

La première formalité consiste pour l'employeur à informer et à consulter les institutions représentatives du personnel. « Le responsable du traitement doit procéder, conformément aux dispositions du code du travail et à la législation applicable aux trois fonctions publiques, à l'information et à la consultation des instances représentatives du personnel avant la mise en œuvre d'un dispositif de géolocalisation des employés. » [\[158\]](#). Les salariés concernés devront faire l'objet d'une information individuelle préalable à la mise en œuvre du traitement [\[159\]](#). En outre, il s'agira de leur communiquer « la finalité ou des finalités poursuivie(s) par le traitement de géolocalisation, les catégories de données de localisation traitées, la durée de conservation des données de géolocalisation les concernant, les destinataires ou catégories de destinataires des données » [\[160\]](#)

. L'employeur doit également mentionner l'existence d'un droit d'accès, de rectification et d'opposition des données et les modalités d'exercice de ce droit.

Lorsque la mise en place de la géolocalisation met en œuvre des procédés informatiques, l'employeur doit effectuer une déclaration auprès de la CNIL. Lorsque le traitement des données répond aux conditions définies par la norme n° 06-067 du 16 mars 2006, il s'agira de la procédure de déclaration simplifiée prévue par la loi. L'accomplissement de ces formalités doit être effectué par l'employeur ou le responsable de l'organisme qui met en œuvre le système de géolocalisation. Lorsqu'elle ne répond pas aux normes précédemment édictées, il reviendra à l'employeur d'effectuer une déclaration dite « normale » conformément à l'article 23 de la loi du 6 janvier 1978.

Les informations obtenues par le biais de ce système doivent faire l'objet d'un tri. Il s'agit de ne collecter qu'un certain type de données. En outre, « *les données collectées dans le cadre de la mise en œuvre d'un dispositif de géolocalisation des véhicules doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles le traitement est mis en œuvre* ». L'article 2 de la directive 2002/58/CE du 12 juillet 2002 dite "Vie privée et communications électroniques" définit les "données de localisation" comme « *toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public* ». La directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 dit "Paquet Télécom" [\[161\]](#) est venue élargir la définition des "données de localisation". Il s'agit désormais de « *toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public* ».

Les données collectées ne peuvent être stockées *ad vitam aeternam*. « *Les données relatives à la localisation d'un employé ne peuvent être conservées que pour une durée pertinente au regard de la finalité du traitement qui a justifié cette géolocalisation* ». A ce titre, la CNIL estime qu'une durée de conservation de deux mois paraît proportionnée. Néanmoins il est possible que les données soient conservées pour une période supérieure « *si cela est rendue nécessaire soit dans un objectif d'historique des déplacements à des fins d'optimisation des tournées, soit à des fins de preuve des interventions effectuées lorsqu'il n'est pas possible de rapporter la preuve de cette intervention par un autre moyen* ». A noter que dans le cadre du suivi du temps de travail, seules les données relatives aux horaires effectués peuvent être conservées pour une durée de cinq ans.

L'accès aux données de géolocalisation doit être limité aux seules personnes qui, dans le cadre de leur fonction, peuvent légitimement en avoir connaissance au regard de la finalité du dispositif (telles que les personnes en charge de coordonner, de planifier ou de suivre les interventions, personnes en charge de la sécurité des biens transportés ou des personnes ou le responsable des ressources humaines). Le responsable du traitement doit dès lors prendre toutes les précautions utiles pour préserver la sécurité de ces données et empêcher, notamment en mettant en place des mesures de contrôle et d'identification, que des employés non autorisés y aient accès. Les accès individuels aux données de géolocalisation doivent s'effectuer par un identifiant et un mot de passe individuel, régulièrement renouvelés, ou par tout autre moyen d'authentification. La Commission rappelle que chaque employé doit pouvoir avoir accès aux données issues du dispositif de géolocalisation le concernant en s'adressant au service ou à la personne qui lui aura été préalablement indiqué. Outre le fait que le traitement de données à caractère personnel fasse l'objet du consentement du salarié, en vertu de l'article 7 de la loi du 6 août 2004. La loi Informatique et libertés du 6 janvier 1978 reconnaît aux personnes physiques le droit d'accès aux données informatisées à caractère personnel les concernant [\[162\]](#). Le non-respect de ce droit conduit la CNIL à prendre de lourdes sanctions. On peut citer une affaire dans laquelle

la commission prononce une sanction pécuniaire de 10 000 euros à l'encontre d'une société qui n'avait pas rempli son obligation envers un salarié. Ce dernier désirait avoir connaissances des données de géolocalisation afin de faire reconnaître l'origine professionnelle de l'accident dont il avait été victime^[163].

Les mesures d'encadrement de la CNIL ne doivent pas être prises à la légère. Comme le souligne Marie Hautefort, « *on a trop souvent tendance à parler de la déclaration à la CNIL comme d'une formalité. On peut facilement lire des exposés sur les sanctions encourues en cas de défaut de déclaration (...) mais il est rare de trouver des commentaires sur la portée de cette déclaration* »^[164].

Paragraphe 2. L'encadrement jurisprudentiel de la géolocalisation

Une fois la déclaration effectuée à la CNIL, l'employeur se doit de respecter les finalités déclarées à celle-ci. Lorsqu'il met en place un dispositif de géolocalisation, l'employeur se doit d'être transparent. Il s'agit là d'une retranscription de l'obligation de loyauté (A). Par ailleurs, la Haute juridiction est particulièrement attentive au respect des droits fondamentaux du salarié. C'est ainsi qu'elle exige que la mise en place d'un tel dispositif soit proportionné au but recherché (B).

A. L'obligation de loyauté de l'employeur

La déclaration de l'employeur effectuée à la CNIL a des conséquences dans le contentieux qui peut opposer un salarié à son employeur. L'absence de déclaration auprès de la CNIL, ou son non-respect entraîne *de facto* l'absence de transparence. Notons par ailleurs que selon l'article L.1222-4 du Code du travail, « *aucune information concernant personnellement un salarié ne peut être collectée, par un dispositif qui n'a pas été porté préalablement à sa connaissance* ».

Dans un arrêt du 3 novembre 2011, la chambre sociale de la Cour de cassation affirme, sur le fondement de l'article L.1121-1 du Code du travail, selon lequel « *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* », que le système de géolocalisation ne peut être utilisé par l'employeur pour d'autres finalités que celles qui ont été déclarées auprès de la CNIL et portées à la connaissance des salariés. En l'espèce, la mise en place d'un système de géolocalisation avait été notifiée à un vendeur salarié. Il était tenu d'exécuter un horaire de 35 heures par semaine, mais était libre de s'organiser comme il le souhaitait. La raison avancée par l'employeur pour justifier la mise en place de ce système était de « *permettre l'amélioration du processus de production par une étude a posteriori de ses déplacements et analyser les temps nécessaires à ses déplacements pour une meilleure optimisation des visites effectuées* ». Quelques mois plus tard, le salarié prend acte de la rupture de son contrat de travail aux torts de l'employeur. Il lui reproche d'avoir calculé sa rémunération, en l'espèce de l'avoir diminué, en se basant sur le système de géolocalisation du véhicule. La Cour de cassation justifie la prise d'acte, qui doit par conséquent produire les effets d'un licenciement sans cause réelle et sérieuse. Une utilisation illicite du système de géolocalisation peut constituer un manquement suffisamment grave de l'employeur pour justifier la prise d'acte de la rupture du contrat de travail par le salarié aux torts de l'employeur^[165]. D'autre part, elle se justifie du fait que l'employeur a modifié la rémunération du salarié sur la base de critères déloyaux. Cela s'apparente à une modification unilatérale du contrat de travail. Selon Laetitia DIVOL, « *si l'employeur avait avoué le véritable but dans lequel il mettait en œuvre ce système de contrôle (c'est-à-dire non seulement optimiser le travail, mais calculer le temps de travail réellement effectué, et par suite, la rémunération due), il se situait hors du cadre tracé par la CNIL en 2006. En détournant le dispositif de géolocalisation pour contrôler l'activité de ses employés alors que la finalité déclarée à la CNIL était toute autre, l'employeur s'expose ici à 5 ans d'emprisonnement et à 300.000 euros d'amende* ^[166] »^[167].

Dans l'arrêt précédemment évoqué, il s'agissait d'une rupture à l'initiative du salarié. Que se passe-t-il si l'employeur est à l'origine de la rupture, qu'il souhaite licencier un salarié pour faute en raison du non-respect de ses obligations contractuelles, en se fondant sur des éléments de preuve obtenus grâce au système de géolocalisation ? Dans ce cas, le licenciement ne pourra être justifié uniquement si le dispositif a fait l'objet d'une déclaration à la CNIL, et que le salarié ait été informé. Ici c'est toujours la loyauté qui est visée, et plus particulièrement le principe de loyauté de la preuve. Dans un arrêt du 14 septembre 2010 rendu par la Cour d'appel de Dijon, un salarié avait été licencié pour avoir utilisé son véhicule pour son usage personnel, et pour ne pas avoir respecté le Code de la route. L'employeur se prévalait de preuves obtenues par le biais du système de géolocalisation dont était équipé son véhicule professionnel. Etant donné que l'employeur ne pouvait apporter un justificatif de déclaration à la CNIL, et que l'information du salarié n'était pas avérée, les juges du fond affirment que « *les informations relatives à la conduite et à l'utilisation de son véhicule par l'intimé ayant été obtenues par l'employeur par des procédés dont la licéité n'est pas établie, les griefs qui en découlent ne sauraient être considérés comme avérés* »^[168]. Par conséquent, le licenciement était sans cause réelle et sérieuse.

B. Le principe de subsidiarité

La Cour européenne des droits de l'Homme (CEDH) rappelle que « *l'ingérence du dispositif de géolocalisation dans la vie privée du salarié doit correspondre à un besoin social impérieux et qu'elle doit être proportionnée au but légitime* »^[169]. Au niveau national, ce principe est inscrit à l'article L.1221-1 du Code du travail^[170]. C'est d'ailleurs sur cet article que la Cour de cassation s'est appuyée pour rendre sa décision dans l'arrêt du 3 novembre 2011 (*op-cit*). Le principe de

subsidiarité peut se traduire par le fait que l'utilisation de la géolocalisation ne doit être employée qu'en cas d'absence d'autres moyens « *plus respectueux de la liberté d'aller et venir et du droit au respect de la vie privée* »^[171]. En vertu de ce principe, la géolocalisation ne peut être mise en place dès lors que le salarié dispose d'une autonomie dans l'organisation de son travail. Lorsqu'un employeur reconnaît une autonomie à des salariés dans l'organisation de leur travail, les « *seuls contrôles qui sont admis - et même indispensables - sont ceux qui ont pour but de s'assurer que le salarié dispose bien de son temps de repos quotidien et hebdomadaire* »^[172]. Par ailleurs, notons que la reconnaissance de l'autonomie du salarié exclut l'utilisation de la géolocalisation dans le but de calculer le temps de travail. En effet, « *l'utilisation dans de telles circonstances est antinomique avec l'indépendance d'organisation du salarié* »^[173]. Un tel objet ne peut se justifier que lorsqu'il n'existe aucun autre moyen pour le chef d'entreprise.

L'autre droit qui découle de cette exigence de proportionnalité est le droit à la désactivation du système de géolocalisation. La surveillance d'un salarié par le biais d'un tel système se justifie par le pouvoir de direction de l'employeur. Dès lors qu'il n'est plus dans le cadre de son temps de travail, le salarié n'est plus sous l'autorité de l'employeur. Dès lors, cela vient justifier la « *la nécessité d'une désactivation complète* »^[174].

La possibilité pour l'employeur de surveiller ses salariés par le biais de la géolocalisation fait l'objet d'un encadrement strict. L'objectif de la CNIL et de la Cour de cassation étant clairement la protection des libertés individuelles des personnes concernées. La surveillance de l'employeur en dehors de l'entreprise ne s'arrête pas à la géolocalisation. Celle-ci peut également mettre à profit les réseaux sociaux afin de surveiller les salariés en dehors même de leur temps de travail.

Section 2. Les réseaux sociaux et le pouvoir de contrôle et de sanction de l'employeur

La notion de réseau social est difficile à cerner, en raison de sa polysémie. Force est d'ailleurs de constater que la notion a radicalement changé de sens en l'espace de quelques années. Selon Ludovic BOURSIN et Laetitia PUYFAUCHER^[175], le terme de « réseau social » a été inventé par le sociologue John A. BARNES en 1954, et désignait « *des liens d'amitié et de connaissance entre des individus qui se reconnaissent mutuellement un statut social à peu près égal* ». Cette définition ne brille pas par sa clarté, mais donne des indices sur ce qu'est un réseau social : un ensemble de contacts humains liés par des intérêts communs. Une définition de la notion, telle qu'entendue aujourd'hui, a été récemment donnée par un groupe de travail constitué de représentants des « CNIL européennes ». Ces derniers définissent les réseaux sociaux comme « *des plateformes de communication en ligne qui permettent à tout internaute de rejoindre ou de créer des réseaux d'utilisateurs ayant des opinions similaires et des intérêts communs* »^[176].

Ces réseaux sociaux sont, pour la plupart, bien connus. Facebook, Twitter, Copains d'Avant, MySpace, LinkedIn... Tous présentent des points communs. Ce sont des sites internet – parfois déclinés en “applications” pour les appareils mobiles – permettant à un utilisateur inscrit d'accéder à une plateforme d'échange d'informations avec ses contacts. Cet accès est soumis à la production d'un certain nombre de renseignements, tels que le nom de l'utilisateur, son âge voire son sexe. Une fois connecté, l'utilisateur dispose d'un certain nombre d'outils pour communiquer. Il peut publier des statuts, des photos, discuter avec des amis en public, tenir des discussions privées... De cet usage - parfois addictif pour certaines personnes^[177] - peut découler un certain nombre de problèmes. Les réseaux sociaux étant, pour certains utilisateurs, des journaux intimes en ligne, l'on comprendra aisément quels peuvent être les conflits qui sont susceptibles de naître. Un utilisateur peut porter atteinte à l'image ou à la réputation d'une autre personne physique ou morale, en publiant des “statuts” ou des photos compromettantes. De la même manière, cet utilisateur peut être victime de ce procédé. Un employeur peut également tenter de surveiller ses salariés, afin de s'assurer qu'ils ne portent pas atteinte à l'image de la hiérarchie ou de

l'entreprise. Il est certain que la liberté d'entreprendre est un droit constitutionnel, mais le respect à la vie privée et la liberté d'expression en sont également... Les nouveaux espaces de liberté que constituent les réseaux sociaux sont sources d'un épilogue jurisprudentiel (Paragraphe 1). Quand bien même le salarié serait protégé par les principes du droit à la liberté d'expression et du droit au respect de sa vie privée, il n'en va pas moins que l'employeur conserve un pouvoir de sanction et de contrôle (Paragraphe 2).

Paragraphe 1. De nouveaux espaces de liberté sources d'un épilogue jurisprudentiel

Les réseaux sociaux sont des espaces nouveaux, où trouve à s'appliquer des principes fondamentaux tels que le droit à la liberté d'expression, et le droit au respect de la vie privée (A). Pour autant, ces principes relativement anciens et bien établis, se trouvent confrontés à une nouvelle forme de support encore inconnu il y a quelques années. Dès lors, il semble logique que nos juridictions soient confrontées à de nouvelles problématiques. En l'absence de positionnement de la chambre sociale de la Cour de cassation - à ce jour - sur ces sujets, des divergences jurisprudentielles sont apparues (B).

A. De nouveaux espaces de liberté pour les travailleurs

« *Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit* »^[178]. Le développement des réseaux sociaux offre aux individus de nouveaux moyens d'expression. Les blogs, Facebook, Twitter permettent à chacun de s'exprimer librement et facilement. Au niveau international, la liberté d'expression est consacrée à l'article 19 de la Déclaration Universelle des Droits de l'Homme (DUDH) et par l'article 10 de la Convention Européenne de Sauvegarde des Droits de l'Homme (CESDH) et des Libertés Fondamentales. Celle-ci dispose que « *toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière* ». L'article énonce également que « *l'exercice de ces libertés [comporte] des devoirs et des responsabilités* » pouvant faire l'objet de restrictions notamment pour protéger « *la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles* ». En France, c'est l'article 10 et 11 de la Déclaration des Droits de l'Homme et du Citoyen (DDHC) qui érige cette liberté. Elle fait par conséquent partie intégrante du bloc de constitutionalité. En tant qu'individus, les salariés ont également le droit à la liberté d'expression. Leur subordination à l'égard de leur employeur ne doit pas avoir pour conséquence de leur ôter cette liberté. La liberté d'expression ne doit pas se confondre avec le droit d'expression direct et collectif des salariés sur leurs conditions de travail, applicable sur le temps et sur le lieu de travail, consacré à l'article L. 2281-1 du Code du travail. Depuis 1988, la jurisprudence a étendu le droit d'expression en considérant qu'il pouvait également être utilisé en dehors du temps et du lieu de travail dès lors qu'il ne donne pas lieu à abus^[179]. C'est d'ailleurs ce même arrêt qui consacre la liberté d'expression en tant que liberté fondamentale. Par conséquent, un licenciement portant atteinte à cette liberté sera nul. C'est ainsi que la création d'un site Internet externe à l'entreprise est licite car « *il n'existe aucune raison d'interdire aux salariés d'utiliser les techniques nouvelles pour l'exercice de leur droit d'expression direct et collective* »^[180]. Cette possibilité leur est également donnée par l'intermédiaire des blogs^[181]. En outre, les salariés ont droit à la liberté d'expression et à la critique dans et hors de l'entreprise, à condition de respecter leurs obligations de discrétion et de loyauté. La liberté d'expression des salariés peut donc s'exercer à l'intérieur et en dehors de l'entreprise. Notons qu'elle n'est pas limitée au propos ayant trait au fonctionnement de l'entreprise. Les propos étrangers à l'entreprise tel que les discussions religieuses, politiques sont également protégées par la liberté d'expression.

La problématique de la liberté d'expression des salariés par le biais des réseaux sociaux est particulièrement liée à la question de la vie privée du salarié. Selon Le Doyen Jean CARBONNIER, la vie privée est la revendication d'une « *sphère secrète de vie d'où [l'individu] aura le pouvoir d'écarter les tiers (...)* »^[182]. Des propos tenus en public auront des conséquences différentes de ceux tenus en privé et inversement. Par ailleurs, en stockant des photos ou des vidéos de leur vie privée sur les réseaux, les individus s'exposent à des répercussions sur leur vie professionnelle. Le salarié doit pouvoir jouir pleinement de ses droits sans que cela puisse interférer sur sa sphère professionnelle. Le droit à la vie privée est mentionné à l'article 8 de la CEDH qui dispose que « *toute personne a le droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ». Au niveau interne, c'est l'article 9, alinéa 1 du Code civil dispose que « *chacun a droit au respect de sa vie privée* ». La Chambre sociale de la Cour de cassation a consacré la plupart des composantes de la vie privée et ce, au profit du salarié. L'employeur ne peut s'immiscer dans la vie privée du salarié. Une fois qu'il n'est plus sous son autorité, le salarié retrouve sa pleine liberté. De plus, si la vie professionnelle de l'individu implique qu'il doit remplir des obligations contractuelles. Cependant, cela ne saurait aboutir à ce que sa vie privée soit suspendue pendant l'accomplissement de ses fonctions. Il existe donc une sphère de vie privée au sein de la sphère professionnelle. En Droit du travail, le principe est qu'un fait

relevant de la vie privée ne peut caractériser une faute du salarié^[183].

La protection de la vie privée implique la protection de la correspondance privée. Dans le fameux arrêt Nikon du 2 octobre 2001^[184], la Cour de cassation rappelle « *que le salarié à droit même au temps et au lieu de travail, au respect de l'intimité de sa vie privée* », et ajoute que cela implique « *le secret des correspondances* ». Depuis cet arrêt il est admis qu'un salarié puisse se servir de la messagerie mise à sa disposition par son employeur à des fins personnelles. Par conséquent, ce dernier ne peut dans le cadre de son pouvoir de sanction, se fonder sur le contenu d'une correspondance privée pour sanctionner son destinataire^[185]. Si cet arrêt reste symbolique du fait qu'il est l'un des rares à faire référence à l'article 8 de la CEDH, il a été fortement amoindri par les positions postérieures de la Haute Juridiction. Aujourd'hui, les juges retiennent que « *sauf risque ou événement particulier, l'employeur ne peut ouvrir les messages identifiés par le salarié comme personnels sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé* »^[186]. Parallèlement, la Cour de cassation affirme que tout message non-identifié comme personnel est présumé professionnel^[187], ce qui implique l'accès de l'employeur hors la présence du subordonné. Ce rappel est nécessaire pour comprendre les nouveaux enjeux qui se posent du fait de l'utilisation des réseaux sociaux par le salarié. Les différents positionnements ont permis d'identifier une ligne jurisprudentielle claire, mais qui ne s'applique qu'aux messageries électroniques.

S'agissant des réseaux sociaux, la question devient plus complexe. Si l'utilisation de Twitter ne pose aucun problème, (toutes les publications sont considérées comme publiques étant donné qu'elles peuvent être vues par tous les contacts de l'utilisateur), il n'en va pas de même pour Facebook. Ce réseau social permet d'utiliser deux types de communication. Celles publiées sur le « mur » (avec des paramétrages de confidentialité pouvant varier), et les messages envoyés en privé sur le même modèle que les courriels électroniques. C'est d'ailleurs Facebook, qui engendre aujourd'hui le plus de contentieux. Dans certains arrêts, les juges considèrent que les écrits diffusés sur le « mur » d'un titulaire d'un compte Facebook, relèvent de la protection de la correspondance privée. Dans deux affaires jugées fin 2011, la Cour d'appel de Rouen a considéré Facebook comme un espace privé^[188], puisqu'il « *ne peut être affirmé de manière absolue que la jurisprudence actuelle nie à Facebook le caractère d'espace privé, alors que ce réseau peut constituer soit un espace privé, soit un espace public, en fonction des paramétrages effectués par son utilisateur* ».

L'utilisation de nouveaux moyens d'expression et d'espaces de vie de privée nécessite une adaptation rapide du Droit. Cette adaptation est d'autant plus difficile que les évolutions en matière de réseaux sociaux sont particulièrement rapides. L'objectif est de maintenir les droits à la liberté d'expression et au respect de la vie privée des salariés. Toutefois, au vu des intérêts de l'entreprise, la jurisprudence et la loi viennent poser des nuances. La notion de vie personnelle est beaucoup plus perméable au pouvoir de sanction de l'employeur que la notion de vie privée. Il va sans dire que malgré les efforts de la jurisprudence pour maintenir un espace de liberté, l'utilisation de certains réseaux exclus de fait le caractère privé. Un réseau social est un espace sur lequel « *on mène une vie sociale, et il est somme toute illusoire de pouvoir y mener une "vie privée"* »^[189]. Il est certain que les réseaux sociaux ont un impact direct sur les relations de travail. De nouvelles problématiques sont posées auxquelles il convient d'y apporter une réponse rapide. La jurisprudence devra concilier les droits fondamentaux des salariés, et les intérêts légitimes de l'entreprise.

La frontière entre espace public et privé semble être l'enjeu central de la problématique de l'utilisation des réseaux sociaux par les salariés. Lorsqu'ils s'expriment à propos de leur entreprise, c'est de la sphère dans laquelle seront tenus les propos dont dépendront les

éventuelles sanctions de l'employeur. Sur cette question, la jurisprudence reste divergente.

B. La source d'un épilogue jurisprudentiel

Jean-Emmanuel RAY résume la problématique dans une interview accordée à Libération en novembre 2010. Selon lui, « *Facebook ne ressemble à rien d'existant. Jusqu'ici, la situation était simple : un espace public est accessible à tout le monde. Donc, sur Facebook, un profil ouvert aux amis d'amis, c'est moins privé tout en le restant a priori. Mais avec la chasse aux amis sur Facebook – les « amis » ne sont que de vagues connaissances- et l'aspect privé devient discutable* »^[190].

La notion d'ami est essentielle pour définir si une publication est privée ou publique. Si l'on s'intéresse à la définition d'ami, « *être lié d'amitié avec quelqu'un* »^[191], cela sous-entend l'idée d'un lien entre les personnes, d'une relation forte entre ces personnes, d'une histoire commune. L'ami de Facebook semble renvoyer à une toute autre réalité, selon Jean-Emmanuel RAY, il faut l'entendre comme de simple « contact »^[192]. L'ami de « Facebook » peut être un membre de la famille, des amis proches mais également des connaissances, des connaissances de connaissances pour lesquelles aucune relation réelle n'existe. Il s'agit en réalité d'un tiers, d'un « étranger », d'une connaissance professionnelle. Il est par conséquent évident que Facebook n'est pas un espace de vie privée mais un lieu public où se rencontre un ensemble de personnes ayant des liens plus ou moins existant. C'est l'importance du droit d'accès que l'on accorde à ses amis qui permet de définir si une conversation est publique ou privée, et si cette conversation peut être utilisée contre son auteur. Une notion d'ami vague, une intrusion de la vie professionnelle dans la sphère privée et l'incapacité de définir le périmètre de visibilité d'une conversation sont autant de problématiques ayant nécessité l'intervention des juges. Cette délicate question se retrouve dans le contentieux relatif aux propos tenus sur Facebook. Des divergences jurisprudentielles sont apparues. Si la chambre civile de la Cour de cassation s'est prononcée sur le sujet en mars 2013, il faudra attendre une réponse de sa chambre sociale pour connaître une ligne claire sur cette question.

Dans un premier temps la Cour d'appel de Reims le 9 juin 2010, confirme le jugement du Conseil de Prud'hommes (CPH) de Troyes du 16 décembre 2009 et estime que Facebook est un espace public^[193]. En l'espèce il s'agissait d'un journaliste qui avait été sanctionné pour avoir écrit, sur le « mur » Facebook d'une amie des propos considérés comme injurieux et diffamatoires. Elle rappelle que « *nul ne peut ignorer que Facebook, qui est un réseau accessible par connexion internet, ne garantit pas toujours la confidentialité nécessaire (...). Que le mur s'apparente à un forum de discussion qui peut être limité à certaines personnes ou non (...)* » ; « *(...) en mettant un message sur le mur d'une autre personne dénommée «ami», il s'expose à ce que cette personne ait des centaines d'«amis» ou n'ait pas bloqué les accès à son profil et que tout individu inscrit sur Facebook puisse accéder librement à ces informations* ». Selon la cour d'appel, le fait de mettre un message sur le « mur » d'une autre personne revient à exposer la publication à l'ensemble des amis de cette personne. Cette démarche rend la publication ouverte puisqu'il n'est pas possible de contrôler le nombre de personnes qui y auront accès. De plus la Cour d'appel de Reims précise que si le salarié « *voulait envoyer un message privé non-accessible à d'autres personnes que le destinataire ou quelques amis choisis, il pouvait utiliser la boîte mail individuelle de Facebook* ». Les juges précisent ici qu'il est possible d'échapper aux sanctions disciplinaires si la publication reste dans un cadre purement privé à travers l'utilisation de mails privés ou de conversations privées.

Toujours en 2010, le CPH de Boulogne-Billancourt^[194] a validé le licenciement pour faute grave

d'une salariée, pour avoir « porté atteinte à l'autorité et à la réputation de sa supérieure hiérarchique ». La salariée avait choisie dans le paramétrage de son compte, la possibilité de partager sa page avec « les amis de leurs amis ». Ce choix rend l'ensemble de ces publications publiques, puisqu'elle n'avait pas la capacité de contrôler l'accès au contenu de ses publications. Le Conseil considère à juste titre que « ce mode d'accès à Facebook dépasse la sphère privée ». La CNIL, le 10 janvier 2011 est venue confirmer cette position en affirmant que « les propos tenus ont perdu leur caractère privé du fait qu'ils étaient accessibles à des personnes non concernées par la discussion ». La CNIL reprend donc l'idée d'un nécessaire paramétrage du compte pour définir le caractère privé d'une conversation en refusant la consultation par « les amis des amis ».

La Cour d'appel de Besançon, le 15 novembre 2011^[195] fait observer que Facebook « doit être nécessairement considéré, au regard de sa finalité et de son organisation, comme un espace public ». Une fois encore, il appartenait à la salariée d'utiliser la fonction appropriée si elle souhaitait avoir une discussion privée. Toutefois il faut noter que certains arrêts sont beaucoup plus frileux à considérer le « mur » comme étant public. Dans une affaire du 15 novembre 2011 la cour d'appel de Rouen a été amenée à se prononcer sur le sort de deux salariées qui échangeaient avec quatre autres collègues des propos relatifs à leur entreprise et leur hiérarchie. Elles sont licenciées pour faute grave, pour propos injurieux et calomnieux, tenus ou soutenus sur le site Facebook, vis-à-vis de la société, et de leurs supérieurs hiérarchiques. Lors de cette discussion, elles invitent leurs collègues à « cracher [leur] haine sur certaine pouf de Leclerc et contre Leclerc tout court ». Une salariée indique : « marre de cette ambiance de merde, des pétasses qui parlent sur notre gueule (...) fait chier, Leclerc ». L'autre s'exprime dans les termes suivants : « des réflexions de bâtards (...), des papias d'enfants de certaines grosses connes, (...) marre de cette semi responsable qui se permet des vanes de merde (...) sale morue ». La cour d'appel de Rouen juge que les licenciements sont dépourvus de cause réelle et sérieuse, leurs propos ayant un « caractère de correspondance privée ». Elle ajoute qu'ici « aucun élément ne permet de dire » que le compte Facebook était paramétré de façon à autoriser le partage avec les « amis » de ses « amis » ou tout autre forme de partage à des personnes indéterminées, « de nature à faire perdre aux échanges litigieux leur caractère de correspondance privée ». Elle estime « qu'il ne peut être affirmé de manière absolue que la jurisprudence actuelle nie à Facebook le caractère d'espace privé, alors que ce réseau peut constituer soit un espace privé, soit un espace public, en fonction des paramétrages effectués par son utilisateur ». De plus, les propos ont été tenus « en dehors du temps et du lieu de travail, et en usant de moyens techniques dont il n'est pas allégué qu'ils auraient été mis à leur disposition par l'employeur ». Elle semble considérer que Facebook doit être présumé comme étant un espace privé, sauf à justifier du contraire. Dès lors que le compte est paramétré de façon à autoriser l'accès au « mur » que pour les « amis », Facebook est un espace privé. Cette décision remet en cause la qualification d'espace public de Facebook et rappelle que c'est à l'utilisateur d'en définir la visibilité grâce au paramétrage. C'est l'utilisateur qui définit la frontière entre le privé et le public. La nature du « mur » pose jusqu'à aujourd'hui le plus grand nombre de problèmes.

Une première réponse a été apportée à ces interrogations dans un cas d'injures publiques par la Chambre civile de la Cour de cassation. Le 10 avril 2013, s'attachant au critère du paramétrage, la Cour énonce « qu'après avoir constaté que les propos litigieux avaient été diffusés sur les comptes ouverts, tant sur le site Facebook que sur le site MSN, lesquels n'étaient en l'espèce accessibles qu'aux seules personnes agréées par l'intéressée, en nombre très restreint, la cour d'appel a retenu, par un motif adopté exempt de caractère hypothétique, que celles-ci formaient une communauté d'intérêts ; qu'elle en a exactement déduit que ces propos ne constituaient pas des injures publiques »^[196]. Le paramétrage semble donc être bel et bien le critère déterminant. Toutefois, on peut s'interroger sur sa pertinence. A partir de quand un compte devient-il public ? Le critère reste particulièrement subjectif et pourra donc évoluer à l'avenir. Ajoutons qu'en

l'espèce, il s'agissait d'un cas d'injures publiques, où il était par conséquent nécessaire de qualifier l'espace sur lequel s'étaient tenus les propos de public. Pour autant, il n'est pas certain que cette solution soit celle retenue en cas de violation de l'obligation de loyauté sur un mur Facebook. Comme nous le verrons, il semble bien plus pertinent de prendre en considération la violation, ou non, de l'obligation de bonne foi, qui va permettre à l'employeur de retrouver son pouvoir de sanction indépendamment de l'existence d'une sphère publique ou privée. En effet, qu'elle soit publique ou non, des propos injurieux, diffamatoires ou excessifs^[197] pourraient fonder une sanction disciplinaire en raison du manquement à l'obligation de loyauté.

Paragraphe 2. Des espaces de liberté soumis à un pouvoir de surveillance et de sanction

Les réseaux sociaux ont pour conséquence de brouiller les frontières entre vie privée et vie professionnelle. Le support virtuel des réseaux est propre à atténuer le principe selon lequel on considère que des photos de famille, de soirée, ou encore des propos tenus sur un journal intime soient privés. Comment considérer que de tels éléments restent privés lorsque des centaines de personnes voir des milliers peuvent les voir ? L'employeur peut alors être tenté de surveiller les activités de ses salariés sur la toile afin de vérifier que ces derniers ne tiennent pas des propos qui lui seraient préjudiciables, ou qu'ils n'aient pas de comportement qui seraient incompatibles avec leurs fonctions. Si on ne peut empêcher un employeur de naviguer sur les réseaux, il lui sera interdit de prendre en compte certains éléments, ou de prendre certaines décisions au nom du droit au respect de la vie privée.

A. Un pouvoir de surveillance et de sanction encadré

La surveillance par l'employeur de ses salariés *via* les réseaux sociaux n'est pas sans limite. D'une part il doit veiller à respecter l'article 9 du Code civil qui énonce le droit au respect de la vie privée. D'autre part, il doit respecter le principe de loyauté de la preuve.

Si les réseaux sociaux sont susceptibles d'être de véritables sources d'informations pour l'employeur, cette surveillance est limitée par le principe du droit au respect de la vie privée. Outre les textes précédemment cités, il faut ajouter que toute collecte de données à caractère personnel doit faire l'objet d'une déclaration à la CNIL. La loi du 6 janvier 1978 dite « informatique et liberté », définit la donnée ayant un caractère personnel comme « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* »^[198]. Par ailleurs, le Code pénal vient sanctionner « *le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende* »^[199].

Le 10 septembre 2012 la CNIL a énoncé qu'il était important que les réseaux sociaux mettent en place les mesures essentielles afin de protéger les données de leurs utilisateurs^[200]. Elle reprend ainsi les recommandations émises par les 29 CNIL européennes (G29), le 12 juin 2009. Celles-ci préconisaient certaines pratiques au titre desquelles on peut citer : la définition des paramètres par défaut limitant la diffusion des données, la suppression des comptes restés inactifs pendant une longue période, la possibilité ouverte aux personnes non-membres des réseaux sociaux de supprimer des données les concernant ou encore proposer aux internautes d'utiliser un pseudonyme plutôt que leur réelle identité. La CNIL est particulièrement attentive à cette problématique des réseaux sociaux et de la surveillance des employeurs. Elle prodigue d'ailleurs de nombreux conseils sur son site internet. Le dernier date du 12 décembre 2012 et explique

comment partager des photos notamment sur les réseaux sociaux sans se surexposer^[201].

En vertu du principe de l'immunité disciplinaire pour les faits relevant de la vie privée, le chef d'entreprise ne peut utiliser des photos ou des commentaires publiés sur les réseaux sociaux, s'ils relèvent de la vie privée. Toutefois, s'il ne peut pas prendre de mesures disciplinaires à l'encontre d'un salarié en se fondant sur des éléments relevant de sa vie privée, « *il peut être procédé à un licenciement dont la cause objective est fondée sur le comportement du salarié qui, compte tenu de la nature de ses fonctions et de la finalité propre de l'entreprise, a créé un trouble caractérisé au sein de l'entreprise*^[202] ». Le trouble causé à l'entreprise est apprécié *in concreto*. Il s'agit « *d'une situation de désordre, d'indignation dont la cause semble sans incidence*^[203] ». Les juges prennent en compte les fonctions du salarié, la nature de l'entreprise, mais aussi sa notoriété ou sa finalité. L'employeur n'a pas à établir un préjudice subi étant donné que le trouble relève plus de la menace que du dommage. Il doit présenter un risque de perte de clientèle, ou de démissions massives par exemple. On peut se réjouir que la Cour de Cassation exige une certaine intensité du trouble, dans la mesure où celui-ci est souvent caractérisé par une réaction vive des tiers, ce qui peut s'avérer dangereux sur le terrain des droits et libertés de la personne. A cet égard, le simple désagrément ou la désapprobation modérée constituent des motifs de licenciement insuffisants. Si en principe, ce type de licenciement n'est pas disciplinaire, quelques arrêts de la Cour de Cassation ont été à l'origine d'inquiétudes^[204] en retenant la faute dans le cadre d'un licenciement pour trouble objectif caractérisé. Fort heureusement, elle a réaffirmé le caractère non-disciplinaire de ce type de licenciement en 2007^[205].

En outre, le problème central en la matière semble être le paramétrage du compte de l'utilisateur. Le 15 novembre 2011, la Cour d'appel de Rouen nous dit que le réseau peut constituer soit un espace privé, soit un espace public en fonction du paramétrage. La CNIL a suivi cette logique considérant que les propos tenus sur Facebook ont perdu leur caractère privé dans la mesure où ils sont ouverts à des personnes qui ne sont pas intéressées par la discussion. Afin d'éviter des contentieux qui sont désormais de plus en plus médiatisés, les entreprises ont tendance à insérer des clauses dans les contrats de travail prévoyant la surveillance des salariés *via* les réseaux sociaux mais également l'interdiction pour eux de publier des commentaires sur l'entreprise ou même ses clients. Par ailleurs, le chef d'entreprise peut également mettre en place une charte informatique qui aurait pour but de réguler l'usage d'internet^[206]. A ces chartes informatiques générales, d'autres prônent l'instauration de charte spécifique. L'utilisation « *massive des réseaux sociaux par les salariés doit inciter les entreprises à encadrer ce type de pratique, notamment par la rédaction d'une charte spécifique*^[207] ». Elle doit également sensibiliser les salariés à leurs responsabilités notamment lorsqu'ils publient des commentaires ou des photos et que ces données sont à la vue de tous. Cette charte peut faire l'objet d'une déclaration à la CNIL.

B. La réaffirmation du pouvoir disciplinaire de l'employeur

Dès lors que les faits commis par un salarié sont publics, l'employeur retrouve son pouvoir de sanction. Par conséquent, il s'agira de savoir si la preuve sur laquelle se fonde l'employeur a été loyalement obtenue. Par ailleurs, la distinction publique-privée ne semble pas véritablement pertinente pour appréhender la logique juridique de la Cour de cassation. S'il est vrai que les réseaux sociaux sont des espaces particuliers, il est tout à fait possible d'y appliquer des principes bien établis. En effet, « *Il résulte de la position de la juridiction suprême que le critère à prendre en compte pour savoir si l'employeur peut valablement exercer son pouvoir de direction ou de sanction est moins celui de la distinction entre espace privé et espace public que celui du manquement du salarié à ses obligations contractuelles, notamment de bonne foi*^[208]. Le pouvoir disciplinaire de l'employeur retrouvera sa plénitude en cas d'abus. Dans un tel cas, « *le salarié ne peut s'abriter derrière ses « intérêts juridiquement protégés » pour proférer à l'encontre de son chef de service des propos outrageants*^[209].

En effet, si on considère que les propos ne sont pas privés, on va ici glisser sur le terrain de la liberté d'expression. Si la Cour de cassation veille à ce que le salarié dispose d'une véritable liberté d'expression dans et hors de l'entreprise, dès l'instant où une page Facebook comportant des propos litigieux a été portée à la connaissance de l'employeur, on doit se placer sur le terrain de l'abus.

Tel était la position retenue par le CPH de Boulogne Billancourt le 19 novembre 2010. Comme *sus* évoqué, le conseil valide le licenciement pour faute grave d'une salariée, pour avoir « *porté atteinte à l'autorité et à la réputation de sa supérieure hiérarchique* ». Le 17 janvier 2012, la Chambre correctionnelle du Tribunal de Grande Instance de Paris condamne un représentant du personnel et délégué syndical pour injure publique. En l'espèce une militante syndicale poste sur le mur Facebook de son syndicat : « *journee de merde, temps de merde, boulot de merde, chefs de merde...* ». Pour se défendre la militante invoque la liberté d'expression syndicale. Cependant, le tribunal explique que « *les expressions incriminées excèdent les limites de la critique admissible, y compris lorsqu'elle s'exerce dans un cadre syndical, par l'utilisation de mots ou de termes insultants ou injurieux voir vexatoires démontrant en eux-mêmes l'intention de nuire et portant clairement atteinte à la dignité des personnes* ». Le TGI déclare donc la militante coupable d'injure publique puisqu'en publiant sur le mur, elle s'est inscrite dans une démarche de publication justifiant l'incrimination. En effet, la militante ne pouvait pas contrôler l'accès à la page rendue visible pour tous.

Que les propos soient tenus dans la sphère publique ou privée, le salarié peut être tenu à une obligation de confidentialité. Cela s'explique par l'importance du secret dans certaines activités économiques. Cette restriction à la liberté d'expression n'est valable que si elle est nécessaire et proportionnée. Lorsque l'employeur invoque un « abus » de liberté d'expression pour sanctionner un salarié sur le fondement de cette obligation, le juge devra connaître l'étendue de l'obligation de confidentialité. De manière générale, on peut estimer qu'une exigence de non-divulgence couvre les « *méthodes de travail de l'entreprise* »^[210], et les caractéristiques des biens ou services produits par le salarié^[211]. Il en va de même des questions relatives à la situation financière de l'entreprise^[212]. En l'espèce, le salarié avait communiqué à une banque des « *renseignements sur les difficultés de l'entreprise et une demande d'aide financière* ». Au final, l'obligation de non-divulgence s'impose donc aux salariés pour toutes les informations qui portent sur un aspect technique ou financier de l'entreprise et qui n'ont pas encore été rendues publiques par l'employeur. Le fait de divulguer de telles informations sur des réseaux sociaux pourra donc avoir comme conséquence non seulement de le soumettre à des sanctions disciplinaires, mais également à engager sa responsabilité civile voir pénale.

Finalement, le seul moyen pour le salarié de se prémunir contre toute mesure de licenciement est, d'une part, de rester extrêmement vigilant quant aux informations qu'il publie, ainsi que celles que d'autres personnes sont susceptibles de publier à son égard. D'autre part, il ne peut que lui être conseillé de respecter son obligation de loyauté, et d'éviter au maximum de commenter ses conditions de travail, son entreprise ou ses supérieurs hiérarchiques, d'autant que l'appréciation des juges du fond quant à ce type de contentieux apparaît très casuistique.

Conclusion

Si la matière ne fait pas l'objet d'une réglementation écrite importante, soulignons le fait que le 9 juillet 2013, les partenaires sociaux ont signé l'ANI sur la qualité de vie au travail. Une partie de cet accord a pour but d'inciter les entreprises à rechercher des solutions afin d'éviter l'intrusion du travail dans la vie privée par le biais des TIC. Il prévoit notamment un droit à la déconnexion.

Les nouvelles technologies de l'information et de la communication ont un impact important sur le

contrat de travail, cela n'est plus à prouver. Elles sont à la fois un instrument permettant de gérer le contrat, mais également un outil de renforcement du pouvoir de contrôle. Cela intervient avant même la conclusion du contrat, et se poursuit lors de son exécution. Si elles poussent l'Homme à s'adapter à de nouvelles contraintes, elles sont aussi la possibilité de l'en dégager. Si elles renforcent le pouvoir de contrôle de l'employeur, elles sont également susceptibles de lui nuire. Ainsi, les NTIC ne sont ni un outil de libération ni un outil de soumission du salarié au sens strict. Elles sont tout à la fois, mais sont avant tout un phénomène neutre. Elles n'ont pas pour dessein de servir l'employeur ou le salarié. Les conséquences qui peuvent en découler sur le contrat ne sont pas la conséquence de l'existence des TIC, mais bel et bien des utilisations qui en sont faites.

On remarquera qu'en matière de conclusion du contrat de travail, le Droit est perméable aux NTIC. On entend par là qu'il ne fait pas obstacle à leur utilisation, à tel point que certains domaines il existe un réel vide juridique. D'une part, cela peut s'expliquer par le fait qu'à cet instant le contrat n'est pas encore conclu. Certes l'employeur est tenu à des obligations, mais il est facile d'utiliser les TIC comme un citoyen lambda au profit du statut d'employeur sans que rien ni personne ne puisse contrôler ces pratiques. D'autre part, les TIC permettent d'avoir recours à de nouveaux modes d'organisation du travail profitables aux deux parties. La chose est bien différente lorsque les TIC sont utilisés pour contrôler le salarié. Dans ce domaine, le Droit apparaît assez hermétique. De nouvelles formes de surveillance sont apparues grâce ou à cause de ces technologies, mais leur utilisation est soumise au respect de règles bien précises.

Au-delà de ces aspects, les TIC viennent remettre en cause le fondement même du contrat de travail : la subordination. On peut même aller plus loin, et considérer qu'elles viennent tout simplement modifier ce sur quoi le Droit du travail s'est fondé : l'unité de temps et de lieu de travail. Ces évolutions conduiront indéniablement certains salariés à être plus proches du statut de « travailleur indépendant » que du salariat.

Bibliographie

Revue juridique

- A. BELLO « Le licenciement pour motif tiré de Facebook : un changement... dans la continuité » *La Semaine Juridique Social* n° 26, 26 Juin 2012, 128
- B. BOSSU « Ouverture d'un courriel par l'employeur et utilisation de son contenu » *La Semaine Juridique Social* n° 5, 31 Janvier 2012, 1041
- B. FOURNIER ; H.GUYOT « Le télétravail » *La Semaine Juridique Social* n° 7, 15 Février 2011, 1072
- C. MAHIEU- GENIAUT « l'immunité disciplinaire de la vie personnelle du salarié en question » *Droit social septembre octobre 2006*
- C. PARLANT ; C. BONAITI « De l'obligation de se former à un droit à être formé » *Semaine sociale lamy 2001 n°1051*
- « CNIL : sanction de la surveillance permanente de salariés au travail » *La Semaine Juridique Social* n° 5, 29 Janvier 2013, act. 52
- C. THIÉRACHE « Retour sur le rapport « L'oubli numérique est-il de droit face à une mémoire numérique illimitée ? » du 25 mai 2010, rédigé par le groupe « Droit à l'oubli » de Cyberlex » *Revue Lamy Droit de l'Immatériel 2011*
- « Des réseaux sociaux plus protecteurs de la vie privée », *Revue Lamy Droit civil 2012 n°97*
- D. GARDES « Le télétravail : Une bonne idée ? » *Les Cahiers Lamy du CE - 2009 n°81*
- E. WALLE « De nouvelles règles issues du Contrôleur européen de la protection des données pour encadrer la vidéosurveillance » *Gazette du Palais, 24 avril 2010 n° 114, P. 21*
- E.WALLE S.SAVAÏDES « L'e-réputation sous le prisme du droit du travail » *Gazette du Palais, 15 octobre 2011 n° 288, P. 26*

- F. PERROTIN « Se préparer à la reprise » *Gérer- Le magazine du Responsable comptable administratif financier – 2011 n°25*
- J-E. RAY « Actualité des TIC : savoir gérer son identité numérique » *Dr. soc. 2010, p. 269*
- J.E. RAY, « De la sub/ordination à la sub/organisation » *Droit social 2002 p.5*
- J.E RAY, « Il y a une porosité croissante entre vie privée et vie professionnelle », *Libération, 20 novembre 2010*
- J.E RAY, « Little Brothers are watching you » *Semaine sociale Lamy*
- J.E RAY, « Mise en place du télétravail » *Les Cahiers du DRH - 2007 n°128*
- L. BOURSIN et L. PUYFAUCHER, « Le média humain - dangers et opportunités des réseaux sociaux pour l'entreprise », *Eyrolles, 2011*
- L. DIVOL, « Contrôle des salariés par géolocalisation : le « oui mais » de la jurisprudence » *Dictionnaire permanent de Sécurité et condition de travail 15 novembre 2011*
- M. CANAPLE, R. FRIEDERICH, « Dynamiser le télétravail : un enjeu décisif pour la croissance et l'emploi » *Semaine Sociale Lamy - 2011 n°1510.*
- M.-J. GOMEZ-MUSTE, « Formation et adaptation dans la jurisprudence sociale », *Dr. soc. sept./oct. 1999, n° 9/10, p. 805*
- M. POTTIE, « Charte d'utilisation des réseaux et moyens informatiques : mode d'emploi », *Revue Lamy Collectivités territoriales 2012, n°84 novembre 2012*
- M. HAUTEFORT, « Géolocalisation : un système de contrôle à n'utiliser qu'à bon escient » *Jurisprudence Sociale Lamy - 2011 311/312*
- O. DUFOUR « La CNIL s'empare du dossier de la vidéosurveillance » *Petites affiches, 27 juin 2012 n° 128, P.3*
- OIT, 25 mars 2013, communiqué « L'OIT présente les atouts du travail à domicile ». *La Semaine Juridique Social n° 14, 2 Avril 2013, act. 164*
- P-H d'ORNANO, « Tout salarié protégé a droit à la confidentialité de ses communications téléphoniques. » *La Semaine Juridique Social n° 24, 12 Juin 2012, 1263*
- Ph. FLORES, « La géolocalisation et le contrôle de la durée du travail : l'état des cartes », *Semaine sociale Lamy n° 1518, p. 7*
- P.Y VERKINDT, « À propos du télétravail et du télétravailleur... après la loi du 22 mars 2012 » *Les Cahiers du DRH - 2012 n°187*
- S. BONNAMY, « Le grisage insuffisamment protecteur de la vie privée et de la liberté syndicale » *Semaine Sociale Lamy - 2013 1566*
- S. MAILLARD, « L'administrateur réseaux peut ouvrir les messages personnels des salariés dans le cadre de sa mission » *La Semaine Juridique Edition Générale n° 39, 21 Septembre 2009, 263*
- S.MILLET, « Les transformation d'emploi, du licenciement à la gestion prévisionnelle » *La semaine juridique et social n°31, 31 juillet 2007, 1598*
- V. STULZ, « Vidéosurveillance des salariés : Oui, mais pas n'importe comment ! La Cnil et la Cour de cassation continuent de poser des limites pour protéger les salariés d'une intrusion massive de l'employeur », *Semaine Sociale Lamy - 2012*
- Willy DUHENATER, « L'utilisation des données de géolocalisation du véhicule d'entreprise pour le suivi du temps de travail d'un salarié » *Revue Lamy droit de l'immatériel*

Rapports et délibération de la CNIL

- Délibération CNIL n° 84-31, 18 sept. 1984
- Délibération CNIL n° 2002-17, 21 mars 2002
- Délibération CNIL n°2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public.
- Délibération CNIL n°2012-213, 22 juin 2012 « Le salarié doit avoir accès aux données de

géolocalisation le concernant ».

- ÉCONOMIE ET STATISTIQUES N° 339-340, 2000 - 9/10. INSEE « Nouvelles technologies, nouvelle économie et nouvelles organisations »
- Rapport du Conseil d'analyse stratégique « L'impact des TIC sur les conditions de travail » 29 fev. 2012
- Rapport Commission des questions sociales, de la santé et de la famille 6 juin 2000
- Rapport stepstone 2010 « Réseaux sociaux et recrutement. Qu'en est-il de leur utilisation et de leur rentabilité ? »
- Synthèse remise au ministre chargé de l'industrie, de l'énergie et de l'économie numérique – Mai 2012 « Le télétravail dans les grandes entreprises françaises Comment la distance transforme nos modes de travail »

Sites internet

- <http://sante.lefigaro.fr/actualite/2012/10/16/19304-plus-4-utilisateurs-sont-addicts-facebook>
- <http://bugbrother.blog.lemonde.fr> J-M MANACH « Facebook et le « paradoxe de la vie privée » » 25 septembre 2012
- <http://www.cnil.fr/la-cnil/actualite/article/article/publication-des-photos-sur-internet-comment-partager-sans-se-sur-exposer/>
- www.cnil.fr/la-cnil/actualite/article/article/keylogger-des-dispositifs-de-cybersurveillance-particulierement-intrusifs/ 2/2. 25 févr. 2013 « Keylogger : des dispositifs de cybersurveillance particulièrement intrusifs - CNIL - Commission nationale de l'informatique et des libertés »

Ouvrages généraux

- D.COHEN Homo Economicus prophète (égaré) des temps nouveaux *Edition Albin Michel* 2012
- J. CARBONNIER, Introduction. *Les personnes. La famille, l'enfant, le couple*, PUF, 2004, n° 278, p. 518

[1] Albert Einstein

[2] Dictionnaire de français Larousse

[3] Economiste du XVIIIème siècle

[4] Dictionnaire de français Larousse

[5] Circulaire DRT n° 12 du 30 novembre 1984

[7] A. MADDISON (1926-2010)

[8] INSEE « Nouvelles technologies, nouvelle économie et nouvelles organisations »
ÉCONOMIE ET STATISTIQUE N° 339-340, 2000 - 9/10

[9] Assemblée parlementaire du Conseil de l'Europe « Impact des nouvelles technologies sur la législation du travail » Rapport Commission des questions sociales, de la santé et de la famille 6 juin 2000

[10] Karl MARX

[11] A. REYMANN « Moderniser la gestion des hommes dans l'entreprise » *Les Cahiers du DRH - 2005*

[12] DP 1931, Tome I, p. 131, note P. Pic ; « Les grands arrêts » n° 1.

[13] Cass. soc., 20 janv. 2010, n° 08-42.207, Bull. V, n° 15.

[14] Cass.soc n° 94-13.187, « Les grands arrêts »°2 ; Dr. soc. 1996, p. 1067, note J.-J. Dupeyrou

[15] A.SUPIOT, « Les nouveaux visages de la subordination » *Dr.soc. 2000, p.131*

[16] C. NICOD ; J-F PAULIN « La subordination en cause » *Semaine sociale Lamy 2011 N°1494*

[17] F. VASSEUR-LAMBRY « La bonne foi dans les relations individuelles de travail. » *Petites affiches, 17*

mars 2000 n° 55, P. 4

[18] Forme d'[organisation du travail](#) inventée par l'ingénieur japonais [Taiichi ?no](#)

[19] D. COHEN *Homo Economicus, Prophète (égaré) des temps nouveaux* Edition Albin Michel 2012

[20] Délib. CNIL n° 2002-17, 21 mars 2002 : JO, 16 juillet

[21] Art. L. 5331-2 du Code du travail

[22] Art. L. 5331-3 du Code du travail

[23] Art. L. 5331-4 du Code du travail

[24] Art. L. 5332-2 du Code du travail

[25] Art. L. 1221-4 du Code du travail

[26] Art. L. 1221-8, al. 3 du Code du travail

[27] Art. L. 1221-8, al. 1^{er} du Code du travail

[28] Art. L. 1221-9 du Code du travail

[29] « Réseaux sociaux et recrutement Qu'en est-il de leur utilisation et de leur rentabilité ? »
Rapport stepstone 2010

[30] E.WALLE, S.SAVAÏDES « L'e-réputation sous le prisme du droit du travail Gazette du Palais », 15 octobre 2011 n° 288, P. 26

[31] Michel SERRE

[32] J-E. RAY, « Actualité des TIC : savoir gérer son identité numérique » *Dr. soc. 2010*, p. 269

[33] C. THIÉRACHE « Retour sur le rapport « L'oubli numérique est-il de droit face à une mémoire numérique illimitée ? » du 25 mai 2010, rédigé par le groupe « Droit à l'oubli » de Cyberlex »
Revue Lamy Droit de l'Immatériel 2011.

[34] « Le télétravail dans les grandes entreprises françaises Comment la distance transforme nos modes de travail » Synthèse remise au ministre chargé de l'industrie de l'énergie et de l'économie numérique mai 2012.

[35] OIT, 25 mars 2013, communiqué « L'OIT présente les atouts du travail à domicile ». *La Semaine Juridique Social n° 14, 2 Avril 2013, act. 164*

[36] *Ibid.*

[37] D. GARDES « Le télétravail : Une bonne idée ? » *Les Cahiers Lamy du CE - 2009 n°81*

[38] M. CANAPLE, R. FRIEDERICH « Dynamiser le télétravail : un enjeu décisif pour la croissance et l'emploi » *Semaine Sociale Lamy - 2011 n°1510*.

[39] OIT, 25 mars 2013, communiqué *op-cit*

[40] Article 2 de l'ANI du 19 juillet 2005

- [41] En avr. 2013, la France comptait selon Pôle emploi 4 800 000 demandeurs d'emplois (toutes catégories confondues).
- [42] Cass.soc., 28 fev. 2001, n°99-40.600 : JurisData n°2001-008512
- [43] ANI 19 juill. 2005, art. 3.
- [44] Article L.1222-10 du Code du travail
- [45] Cass. soc., 7 avril 2010, n° 08-44.865, 08-44.866, 08-44.867, 08-44.868 et 08-44.869.
- [46] P.Y VERKINDT « À propos du télétravail et du télétravailleur... après la loi du 22 mars 2012 » *Les Cahiers du DRH - 2012 n°187*
- [47] « À propos du télétravail et du télétravailleur... après la loi du 22 mars 2012 » *op-cit*
- [48] OIT, 25 mars 2013, communiqué *op-cit*
- [49] Cass.soc 17 fev.2004, n°04-45.889
- [50] *Ibid.*
- [51] F. PERROTIN « Se préparer à la reprise » *Gérer- Le magazine du Responsable comptable administratif financier – 2011 n°25.*
- [52] Article L.1222-9 du Code du travail
- [53] Cass.,soc 31 jan. 2012 n° 10-25.367
- [54] B.FOURNIER ; H.GUYOT « Le télétravail » *La Semaine Juridique Social n° 7, 15 Février 2011, 1072*
- [55] B.FOURNIER, H.GUYOT « Le télétravail » *op-cit*
- [56] Circ. DGT n° 2007/18, 18 déc. 2007 relative à la continuité de l'activité des entreprises et aux conditions de travail et d'emploi des salariés du secteur privé en cas de pandémie grippale.
- [57] Avenant à l'accord Renault SAS relatif au télétravail à domicile, 22 juin 2010, art. 5.

- [58] J.-E. RAY, « De la sub/ordination à la sub/organisation » *Droit social* 2002 p.5
- [59] Rapport du Conseil d'analyse stratégique « L'impact des TIC sur les conditions de travail » 29 fev. 2012
- [60] CJCE, 1er décembre 2005, af. C-14/04 : REC CJCE 2005, I, p.10253
- [61] Cass.soc., 1^{er} juillet 2009, n°08-41.217
- [62] Cass.civ., 6 juillet 1931 Rec. Dalloz. 1931, 1ère partie, p.121.
- [63] J.E RAY « Mise en place du télétravail » *Les Cahiers du DRH - 2007 n°128*
- [64] J.-E. RAY, « De la sub/ordination à la sub/organisation » *op-cit*
- [65] P.Y VERKINDT « À propos du télétravail et du télétravailleur... après la loi du 22 mars 2012 » *Les Cahiers du DRH - 2012 187*
- [66] C.PARLANT ; C. BONAÏTI « De l'obligation de se former à un droit à être formé » *Semaine sociale lamy 2001 n°1051*
- [67] Article L.2323-13 et L.4612-9 du Code du travail
- [68] Article L.2323-14 et L.4612-10 du Code du travail
- [69] Article L.6321-7 du Code du travail
- [70] Cass. soc., 5 juin 2013, n° 11-21.255, F-P+B, M. D. c/ SA Numec : [JurisData n° 2013-011322](#)
- [71] Article L1233-3 du Code du travail
- [72] Cass.soc., 2 juin 1993, Bull. 5ème partie n° 155.
- [73] Cass.soc., 9 décembre 2003, RDS 2004, p. 210
- [74] Cass.soc., 5 avril 1995 n° 93-42.690
- [75] Cass. soc., 11 janvier 2006, n° 04-46.201

[76] Cass. soc., 25 févr. 1992, Expovit, Bull. V, n° 122 ; Dr. soc. 1992, p. 922

[77] Article L. 1233-4 du Code du travail

[78] Cass. soc., 22 janv. 1992, Bull. civ. V, n° 31 ; 9 nov. 2004, n°02-44.202 ; 6 juill. 2006, Bull. civ. V, n° 333.

[79] Cass.soc 3 avril 2001 n° 99-42.188 à n° 99-42.190

[80] S.Millet « Les transformation d'emploi, du licenciement à la gestion prévisionnelle » *La semaine juridique et social n°31, 31 juillet 2007, 1598*

[81] Cass. soc., 3 mai 1990, n° 88-41.900.

[82] M.-J. GOMEZ-MUSTE, « Formation et adaptation dans la jurisprudence sociale », Dr. soc. sept./oct. 1999, n° 9/10, p. 805

[83] Cass. soc., 23 févr. 2005, n° 04-45.463

[84] Cass. soc., 10 oct. 2000, n° 98-41.358

[85] Cass. soc. 28 janv. 2005, n° 03-40.639

[86] Article L. 1222-6 du Code du travail

[87] Article L. 1233-3 du Code du travail

[88] Cass. soc., 26 avr. 2006, n° 04-43.582, n° 1050 F - P + B, Sté Argedis c/ Audin

[89] Art. L.1222-1

[90] Cass. soc., 20 nov. 1991, n° 88-43.120, n° 4080 P + F, Neocel c/ Spaeter

[91] JCP E 2001, p. 1918, note C. Puigelier

[92] Cass.soc., 17 juin 2009, n° 08-40.274 : JurisData n° 2009-048669 JCP S 2009, 1362, note E. Jeansen

[93] Cass. soc., 18 oct. 2006, n° 04-48.025: JurisData n° 2006-035418 et Cass. soc., 18 oct. 2006,

n° 04-47.400 : JurisData n° 2006-035412

[94] B.Bossu « Ouverture d'un courriel par l'employeur et utilisation de son contenu » *La Semaine Juridique Social* n° 5, 31 Janvier 2012, 1041

[95] Cass.soc., 10 mai 2012, n°11-13-884, F-P+B JurisData n°2012-009432

[96] Cass. soc., 21 oct. 2009, n° 07-43.877: JurisData n° 2009-049999; Bull. civ. 2009, V, n° 226 ; JCP S 2010, 1026, note B. Bossu

[97] Cass. soc., 8 déc. 2009, n° 08-44.840 : JurisData n° 2009-050763 ; RJS 2010, n° 144

[98] Cass. soc., 15 déc. 2009, préc

[99] Cass.soc., 4 juill.2012, n°11-12.502, F-D : JurisData n°2012-015858

[100] Disponible sur www.cnil.fr

[101] Cass. soc., 12 février 2013, pourvoi n° 11-28.649

[102] Cass. ch. mixte, 18 mai 2007, n° 05-40.803 : JurisData n° 2007-038898 JCP E 2007, 1844, note C. Puigelier

[103] Cass. soc., 2 févr. 2011, n° 09-72.313

[104] Cass. soc., 5 juill. 2011, n° 10-17.284 : JurisData n° 2011-013754 ; JCP S 2011, 1501, note B. Bossu

[105] Cass. soc., 2 févr. 2011 : JCP S 2011, 1274, note A. Martinon

[106] Cass. soc., 8 déc. 2009, n° 08-42.097 : JurisData n° 2009-050761 ; RDT 2010, p. 215, note Y. Leroy

[107] Cass. soc., 15 déc. 2009, n° 07-44.264 : JurisData n° 2009-050802

[108] Cass. soc., 18 oct. 2011, n° 10-26.782, F-D, M. C. c/ SARL Nova régie : JurisData n° 2011-022346

[109] Cass. soc., 17 juin 2009, n° 08-40.274, FS P+B, Sté Sanofi Chimie c/ M. Guzzi et a. : JurisData n° 2009-048669

[110] S. MAILLARD « L'administrateur réseaux peut ouvrir les messages personnels des salariés dans le cadre de sa mission » *La Semaine Juridique Edition Générale n° 39, 21 Septembre 2009*, 263

[111] CA Paris, 11e ch., sect. A, 17 déc. 2001 : JurisData n° 2001-166690 ; JCP G 2002, II, 10087, note M. Vivant et J. Devèze

[112] S.MAILLARD (*op-cit*)

[113] Art. 226-15 du Code pénal

[114] Art. L.1222-4 du Code du travail

[115] 25 févr. 2013 « Keylogger : des dispositifs de cybersurveillance particulièrement intrusifs - CNIL - Commission nationale de l'informatique et des libertés »
www.cnil.fr/la-cnil/actualite/article/article/keylogger-des-dispositifs-de-cybersurveillance-particulierement-intrusifs/ 2/2

[116] Art. L.1221-1 du Code du travail

[117] Cass. soc., 9 juill. 2008, n° 06- 45.800

[118] Cass. soc., 18 mars 2009, n° 07-44.247 : JurisData n° 2009-048024

[119] Cass. soc., 11 juill. 1995, n° 94-40.205

[120] Délib. CNIL n° 2005-019, 3 févr. 2005 : JO, 1er mars

[121] Cass. soc., 6 avr. 2004, n° 02-40.498, n° 938 FS - P + B + R + I, Gonzales c/ Sté BDI constructions.

[122] Cass. soc., 4 avr. 2012, n° 10-20.845, n° 999 F - P + B, Gauvignon c/ Sté Groupe Progrès

[123] Cass. soc., 29 janv. 2008, n° 06-45.279, Touati c/ Sté Canon France

[124] Délib. CNIL n° 84-31, 18 sept. 1984 ; Cass. soc., 6 avr. 2004, n° 02-40.498 : JurisData n° 2004-023266 ; Bull civ. 2004, V, n° 104

[125] Cass. soc., 4 avr. 2012, n° 10-20.845, F-P+B, M. G. c/ SA Groupe Progrès : JurisData n° 2012-006380

[126] P-H d'Ornano « Tout salarié protégé a droit à la confidentialité de ses communications téléphoniques. » *La Semaine Juridique Social n° 24, 12 Juin 2012, 1263.*

[127] Cass. soc., 15 mai 2001, n° 99-42.937, n° 2086 FS - P + B, Aymard c/ Cabinet Regimbeau

[128] CNIL, 11ème rapport d'activité, p. 322

[129] Cass. soc., 16 mars 2011, n° 09-43.204, Sté Caisse d'épargne et de prévoyance de Normandie c/ Pontais

[130] O.DUFOUR « La CNIL s'empare du dossier de la vidéosurveillance » *Petites affiches, 27 juin 2012 n° 128, P.3*

[131] Délib. CNIL n° 2012-475, 3 janv. 2013, Synd. des copropriétaires « Arcade Champs-Élysées »

[132] « CNIL : sanction de la surveillance permanente de salariés au travail » *La Semaine Juridique Social n° 5, 29 Janvier 2013, act. 52*

[133] Art. L. 2323-32 du Code du travail

[134] E. WALLE « De nouvelles règles issues du Contrôleur européen de la protection des données pour encadrer la vidéosurveillance » *Gazette du Palais, 24 avril 2010 n° 114, P. 21*

[135] Loi « informatique et liberté », art. 32, 6 janv. 1978, modifiée par la loi du 29 mars 2011 et décision Cnil n° 2009-201, 16 avr. 2009

[136] Cass. soc., 10 janv. 2012, n° 10-23.482

[137] V. STULZ « Vidéosurveillance des salariés : Oui, mais pas n'importe comment ! La Cnil et la Cour de cassation continuent de poser des limites pour protéger les salariés d'une intrusion massive de l'employeur ». *Semaine Sociale Lamy - 2012*

[138] V. STULZ (*op-cit*)

[139] CNIL vidéosurveillance — *vidéoprotection Fiche pratique Edition juin 2012*

[140] Cass. soc., 20 nov. 1991, n° 88-43.120, n° 4080 P + F, Neocel c/ Spaeter

[141] Cass. soc., 7 juin 2006, n° 04-43.866, n° 1459 FS - P + B, Girouard c/ Sté Continent France

groupe Carrefour et a.

[142] Cass. soc., 10 déc. 1997, n° 95-42.661, n° 4739 P + B + R, Aubin c/ Sté Euromarché Carrefour

[143] Cass. soc., 31 janv. 2001, n° 98-44.290, n° 380 FS - P, Alaimo c/ Sté Italexpress transports

[144] Cass. soc., 19 avr. 2005, n° 02-46.295, n° 942 F - P + B, Lemberet et a. c/ Sté Immodéf

[145] Cass. soc., 19 janv. 2010, n° 08-45.092, Cabrol c/ Sté Nestlé Waters Supply Sud

[146] Cass. crim., 6 avr. 1994, n° 93-82.717

[147] Art. 226-1 du Code pénal

[148] Art. 226-18 du Code pénal

[149] Art. 226-16 du Code pénal

[150] Art. 226-20 du Code pénal

[151] Délib. CNIL n° 2012-322, 20 sept. 2012 : JO, 12 oct

[152] Délib. CNIL n° 02-001, 8 janv. 2002

[153] Cass. soc., 6 avr. 2004, n° 01-45.227, n° 944 FS - P + B + R + I

[154] 10ème rapport d'activité, p. 261-262

[155] Cass. crim. 4 oct.1977 : Bull. crim. N°287 ; D.1977. IR 491

[156] Délib. n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés (du privé ou du public.)

[157] Délib.n°2006-066 du 16 mars 2006 *op-cit.*

[158] Délib.n°2006-066 du 16 mars 2006 *op-cit*

[159] Article 32 de la loi du 6 janvier 1978 et article 34-1 IV du code des postes et des

communications électroniques

[160] Article 32 de la loi du 6 janvier 1978 *op-cit*

[161] J.O de l'union européenne 18 Décembre 2009

[162] Article 39 de la loi du 6 janvier 1978

[163] CNIL, Délib. n°2012-213, 22 juin 2012

[164] M.HAUTEFORT, « Géolocalisation : un système de contrôle à n'utiliser qu'à bon escient » *Jurisprudence Sociale Lamy - 2011 311/312*. Commentaire de l'arrêt de la Cour de cassation du 3 novembre 2011 (Pourvoi n°10-18.036).

[165] Cass.soc., 03 novembre 2011 n°10-18.036 Juris-Data n° 2011-023703

[166] **Article 226-21 du Code pénal**

[167] L. DIVOL « Contrôle des salariés par géolocalisation : le « oui mais » de la jurisprudence » *Dictionnaire permanent de Sécurité et condition de travail 15 novembre 2011*.

[168] CA Dijon, chbre. soc., 14 septembre 2010, Sté Mille Services c/ Rémi X.

[169] CEDH, 2 septembre. 2010, Uzun c./Allemagne, n°35623/05

[170] *Op-cit*

[171] Ph. FLORES, « La géolocalisation et le contrôle de la durée du travail : l'état des cartes », *Semaine sociale Lamy n° 1518, p. 7*

[172] M. HAUTEFORT « Géolocalisation : un système de contrôle à n'utiliser qu'à bon escient » (*op-cit*)

[173] Ph.FLORES (*op-cit*)

[174] S. BONNAMY « Le grisage insuffisamment protecteur de la vie privée et de la liberté syndicale » *Semaine Sociale Lamy - 2013 1566*

[175] L. BOURSIB et L. PUYFAUCHER ; *Le média humain - dangers et opportunités des réseaux sociaux pour l'entreprise*, Eyrolles, 2011

- [176] Définition proposée dans un avis référencé 5/2009 du 12 juin 2009
- [177] <http://sante.lefigaro.fr/actualite/2012/10/16/19304-plus-4-utilisateurs-sont-addicts-facebook>
- [178] Article 19 de la Déclaration universelle des droits de l'Homme
- [179] Cass.soc., 28 avr. 1988 : Bull. civ. 1988, V, n° 257 ; Dr. ouvrier 1988, p. 252,
- [180] TGI Paris, ord. Référé, 17 nov. 1997 : TPS 1998, comm. 204
- [181] TGI Paris, 16 oct. 2006, n° 06-8820
- [182] J. CARBONNIER, Introduction Les personnes. La famille, l'enfant, le couple, PUF, 2004, n° 278, p. 518
- [183] Cass.soc, 17 avril 1991, n° 90-42.636 Bull. civ. 1991, V, n° 201
- [184] Cass.soc, 2 octobre. 2001, n° 99-42.942 Bull. civ. 2001, V, n° 291, p. 233
- [185] Cass.ch. mixte, 18 mai 2007, n° 05-40.803, P+B+R+I. Juris-Data n° 2007-038898
- [186] Cass.soc. 17 juin 2009, n° 08-40.274, JCP G 2009, n° 39, 263
- [187] Cass.soc. 18 octobre 2006, n° 04-48.025, J CP S 2006, n° 48, 1946
- [188] CA Rouen, 15 novembre 2011, n°11.01827 et n°11.01830
- [189] J-M MANACH « Facebook et le « paradoxe de la vie privée » » 25 septembre 2012
<http://bugbrother.blog.lemonde.fr>
- [190] J-E RAY, « Il y a une porosité croissante entre vie privée et vie professionnelle », Libération, 20 nov. 2010
- [191] Dictionnaire LAROUSSE
- [192] J-E RAY. "Little Brothers are watching you" *Semaine sociale Lamy*
- [193] CA Reims, 9 juin 2010, n° 09-3205.

[194] CPH Boulogne-billancourt. 19 nov.2010, n° 10.853

[195] CA Besançon, 15 nov. 2011, n° 10/02642

[196] Cass. Soc., 10 avril 2013 n°11-19.530

[197] Cass.soc., 27 mars 2013 n°11-19.734 JurisData n°2013-005587

[198] Article 2 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[199] Art. 226-18 du Code pénal

[200] « Des réseaux sociaux plus protecteurs de la vie privée », *Revue Lamy Droit civil 2012 n°97*

[201] <http://www.CNIL.fr/la-CNIL/actualite/article/article/publication-des-photos-sur-internet-comment-partager-sans-se-sur-exposer/>

[202] Cass.soc, 17 avr. 1991 : Dr. soc. 1991, p. 485, note J. SAVATIER

[203] C. MAHIEU- GENIAUT « *l'immunité disciplinaire de la vie personnelle du salarié en question* » Dr.soc septembre octobre 2006.

[204] Cass.soc 3 décembre 2002; Cass.soc 25 janvier 2006

[205] Cass.chbre mixte 18 mai 2007

[206] M. POTTIE, « Charte d'utilisation des réseaux et moyens informatiques : mode d'emploi », *Revue Lamy Collectivités territoriales 2012, n°84 novembre 2012*

[207] « Réseaux sociaux : la rédaction d'une charte spécifique s'impose » *Semaine sociale Lamy*

[208] Ahmed BELLO « Le licenciement pour motif tiré de Facebook : un changement... dans la continuité » *La Semaine Juridique Social n° 26, 26 Juin 2012, 1280*

[209] *Ibid.*

[210] Soc. 19 mars 2008, n° 06-45.322, RJS 6/2008 n° 631

[211] Art. L. 1227-1

[\[212\]](#) Soc. 8 oct. 1992, n° 91-41.515, inédit