Association d'Etude et de suivi de L'aménagement du Temps de Travail Dans les métiers du savoir

ADESATT

Les organisations virtuelles du travail. Pilotage et cybersurveillance.

Synthèse des études et enquêtes réalisées
du 11 mai 2010 au 15 décembre 2010

Sommaire

1/
VERS UNE ORGANISATION VIRTUELLE DE L'ENTREPRISE

1/ VERS UNE ORGANISATION VIRTUELLE DE L'ENTREPRISE *

* Selon présentation Akting/Gide Loyrette Novel du 1er Juillet 2010

LE CONSTAT

Pour s'adapter à la globalisation économique, les entreprises ont mis en place des organisations virtuelles grâce aux nouvelles technologies de l'information et de la communication (voir chapitre 5 : La cybersurveillance et les outils TIC). Ce nouveau mode d'organisation engendre une remise en cause des cadres de travail traditionnels : définition de la durée de travail, séparation vie privée/vie professionnelle, procédures d'encadrement, de contrôle et de surveillance… Qu'en est-il des organisations des entreprises ?

LES DIFFÉRENTES TYPOLOGIES D'ORGANISATIONS DES ENTREPRISES

Organisation classique :

dans ce cadre, les équipes disposent d'un management à la fois hiérarchique et de proximité. Ainsi, la règle des trois unités (lieu, temps, action) est respectée. La proximité spatio-temporelle permet de s'affranchir de processus, procédures et outils spécifiques et sophistiqués pour assurer « l'unité et la permanence du commandement ».

Dans ce cas, l'existence d'outils collaboratifs, de management et de cybersurveillance est rare.

Organisation matricielle :

de plus en plus de salariés exercent leur activité en dehors des locaux de leur entreprise (notamment les sociétés de services, d'ingénierie et de conseil). Dans ce cas, les procédures et les outils sont nécessaires pour garantir le travail collaboratif et le management (relevé d'activité, grille d'évaluation…) mais aussi pour garantir les droits et devoirs des salariés.

Dans ce cas, l'existence d'outils collaboratifs, de management et de cybersurveillance est fréquente.

Télétravail à domicile :

il peut s'exercer de différentes manières, cela dépend s'il est formalisé ou non (voir chapitre 2 consacré au télétravail). Bien sûr, lorsque le télétravail est reconnu ou encouragé, on constate l'existence d'accords et de chartes mais aussi de procédures (fournitures d'équipements, prise en charge de frais) et de systèmes de contrôle voire de cybersurveillance.

Dans ce cas, l'existence d'outils collaboratifs, de management et de cybersurveillance est rare.

Entreprise en réseau :

le principe de ce modèle est que plusieurs sociétés (fournisseurs, partenaires, clients) travaillent depuis différents lieux en ayant une unité de commandement. Dans ce cas de figure, il est impératif de disposer de solides procédures et outils de collaboration mais aussi de solutions pour assurer un management plus «subtil ».

Dans ce cas, l'existence d'outils collaboratifs, de management et de cybersurveillance est essentielle.

Plateforme collaborative :

la plateforme collaborative permet à différents acteurs de contribuer au même projet en restant sur leur lieu de travail contractuel au contact de leur management de proximité. Les salariés apportent leurs compétences respectives via une plateforme collaborative d'échange.

Dans ce cas, l'existence d'outils collaboratifs, de management et de cybersurveillance est essentielle.

QUELQUES CHIFFRES *

- ***49%*** *des entreprises de plus de 10 salariés ont des salariés travaillant en équipe virtuelle.*
- ***40%*** *des entreprises ont des salariés en déplacement plus de 50% de leur temps.*
- ***40%*** *des entreprises ont des salariés en délégation chez le client.*

Près de la moitié des cadres encadrant ont des membres de leur équipe travaillant à distance.

☐ AVANTAGES ET INCONVÉNIENTS DES ORGANISATIONS VIRTUELLES

Avantages

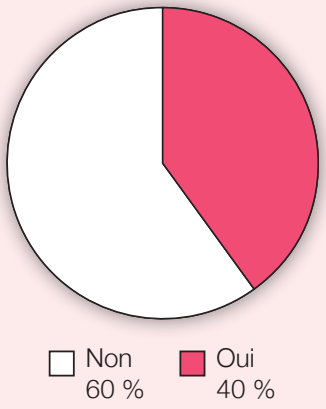
- Flexibilité
- Proximité
- Productivité
- Transparence
- Modernisation de l'organisation du travail
- Développement durable, empreinte carbone

Inconvénients

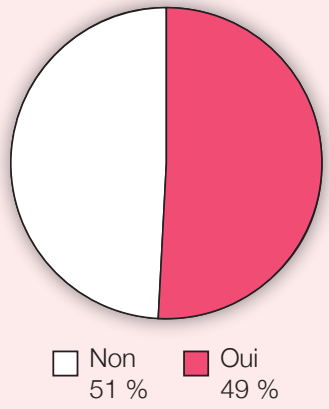
- Cohésion de l'équipe, réduction des échanges informels
- Isolement des salariés
- Manque d'encadrement
- Sécurité informatique
- Respect de la vie privée des salariés
- Respect des conditions de travail
- Problème de liaison arc les IRPs
- Respect des droits des salariés

☐ CARACTÉRISTIQUES DES ORGANISATIONS

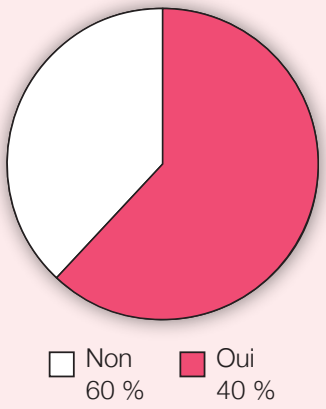
Présence de salariés en déplacement plus de 50% de leur temps et donc éloignés de leur équipe et/ou management.



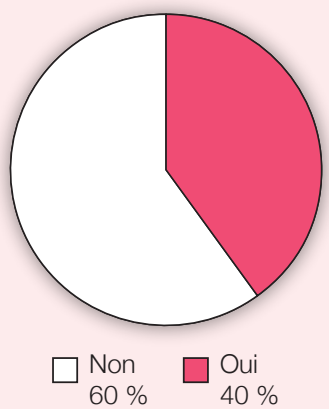
Présence de salariés travaillant en équipe virtuelle, éloignés de leur équipe ou de leur management.



Présence de salariés travaillant en équipe virtuelle, avec des salariés d'autres entreprises.



Présence de salariés en délégation chez le client (régie par exemple).



N = 510 entreprises

2/
LIMITES DE L'ORGANISATION VIRTUELLE DE L'ENTREPRISE

2/ LIMITES DE L'ORGANISATION VIRTUELLE DE L'ENTREPRISE *

* Selon étude IDC/Akting/Gide Loyrette Novel

Après l'enthousiasme suscité par les promesses des nouvelles technologies à la fin du siècle dernier, les organisations virtuelles ont, à l'épreuve de la réalité, montré leurs limites. Quelles sont ces limites ?

Isolement :
ressenti par les salariés isolés de leur équipe, de manière occasionnelle ou prolongée. Le salarié isolé est susceptible de se détacher de son équipe avec les conséquences que cela peut induire en termes de productivité et d'intégration.

Déperdition d'information informelle :
notamment pour ce concerne les discussions et réunions informelles qui se déroulent dans les locaux de l'entreprise et ne sont par portées à la connaissance des télétravailleurs. Il en résulte que le salarié ne peut être averti d'un changement sur un projet pouvant l'affecter et invalider son travail.

Changement majeur dans le rapport au travail :
les organisations virtuelles ont un impact profond sur le mode de travail, limitant les modes de socialisation traditionnels. Il y a une dimension psychologique particulièrement exacerbée en cas de télétravail à domicile puisque le cadre familial n'est pas un cadre habituel de travail.

Frein à la créativité collective :
sur ce point la situation des entreprises est binaire. Les entreprises traditionnelles prônent le regroupement physique des experts pour favoriser les échanges et optimiser la créativité. Les entreprises très orientées vers les nouvelles technologies, fonctionnent en mode totalement virtuel avec des outils de messagerie et de travail collaboratif. Dans un même secteur, on trouve des entreprises aux antipodes, démontrant un écart lié à la culture de l'entreprise.

Perception négative des salariés physiquement éloignés par les autres salariés :
bien que très difficile à mesurer, ce frein existe néanmoins.

Des dérives constatées :
il s'agit soit de salariés consciencieux qui rattrapent leur « retard » le soir ou les weekends (ce qui crée un déséquilibre entre vie professionnelle et vie privée) soit de salariés au contraire peu consciencieux qui abusent de leur « invisibilité ».

3/ RECOMMANDATIONS POUR LA MISE EN PLACE ET LE PILOTAGE D'ORGANISATIONS VIRTUELLES

3/ RECOMMANDATIONS POUR LA MISE EN PLACE ET LE PILOTAGE D'ORGANISATIONS VIRTUELLES *

* Recommandations établies par l'IDC selon son étude.

Promotion et information

- Intégrer plus largement la problématique « Organisations Virtuelles » dans les groupes de travail du SYNTEC Numérique et leurs publications (Green IT, Cloud, mobilité…)

- Créer un observatoire des pratiques pour partager les expérimentations et les expériences au sein du secteur et avec d'autres secteurs car tous les secteurs d'activités sont concernés par l'évolution des modes de travail.

- Améliorer le niveau d'information relatif à la réglementation notamment par le biais d'une meilleure promotion des documents d'information de la CNIL et de l'Assemblée des chambres françaises de commerce et d'industrie.

Encadrement et IRPs

- Proposer une formation spécifique des managers à la gestion d'une équipe virtuelle et aux outils

- Former aux outils et procédures de contrôle les collaborateurs à distance

- Intégrer la gestion des équipes virtuelles dans les référentiels OPIEC

- Favoriser et faciliter l'accès aux IRP

Sécurité et prévention des risques

- Améliorer et préciser les conditions de prise en charge par les assurances des salariés en télétravail qu'il s'agisse de dommage personnel, des équipements personnels ou de l'entreprise pour une simplification de la démarche.

- Prévenir les risques d'isolement par la mise en place d'une réglementation.

Durée du travail

- Définir des horaires de travail afin que le télétravailleur soit joignable lors des horaires bureau (et éviter ainsi tout phénomène de harcèlement).

- Envisager le forfait jour qui semble le plus adapté au travail à domicile ou en organisation virtuelle.

Editer un « Guide des bonnes pratiques »

- Créer un guide qui réunirait -sous la forme de fiches pédagogiques- l'ensemble des préconisations visant à améliorer le pilotage et la mise en place des organisations virtuelles des entreprises dans les domaines de la formation, la gestion des ressources humaines, les outils de gestion des organisations virtuelles, la sécurité, le télétravail.

4/
LE TELETRAVAIL A DOMICILE

4/ LE TELETRAVAIL A DOMICILE

LE CONSTAT

D'une manière générale, il existe très peu de formalisation pour le télétravail, excepté pour le télétravail régulier qui se pratique plusieurs jours par semaine ou pleinement à domicile.

MOTIVATION

On constate que le télétravail formalisé est le plus souvent motivé par des événements affectant l'organisation de l'entreprise (déménagement, rachat, réduction de l'espace de bureau, extension géographique de la société…). Le télétravail peut également être mis en place dans le cadre de la politique RH (recrutement d'une compétence pointue, rétention/fidélisation de certains profils ou comme avantage en remplacement d'augmentations salariales). Il faut noter qu'une majorité d'entreprises choisit d'ignorer le télétravail occasionnel, à faible fréquence ou touchant un faible nombre d'employés. On parle dans ces cas-là de télétravail « gris ».

FORMALISATION

La plupart des entreprises formalisent le télétravail par un avenant au contrat de travail. Actuellement, l'Accord National Interprofessionnel (ANI) de 2005 sert de point de départ pour les entreprises qui souhaitent formaliser le recours au télétravail. Pour les entreprises, les points les plus difficiles à formaliser sont ceux qui concernent la santé et la sécurité des salariés, la protection des données, l'assurance du salarié et le suivi de l'accès aux droits collectifs.

☐ QUELQUES CHIFFRES *

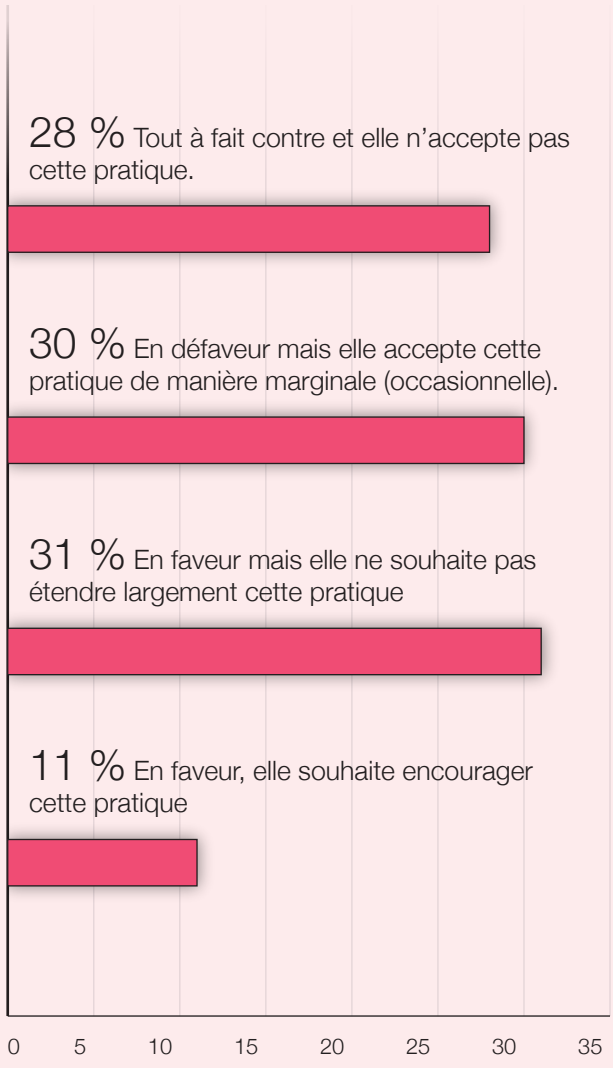
- *Près de **50 000 salariés** travaillent fréquemment à domicile aux horaires de bureau, plusieurs fois par mois. Parmi ceux-ci, environ **10 000** disposent d'un avenant à leur contrat de travail précisant les modalités d'exercice du télétravail à domicile.*

*Le nombre de salariés en télétravail à domicile dans le cadre d'un accord d'entreprises s'élève à près de **2 000** à la mi-juin 2010 et devrait doubler dans les 12 mois.*

* Selon présentation IDC pour ADESATT du 15 décembre 2010

☐ TRAVAIL À DOMICILE AUX HORAIRES DE BUREAU

Question : Quelle est la position de la Direction générale sur le télétravail à domicile ?



Notes :

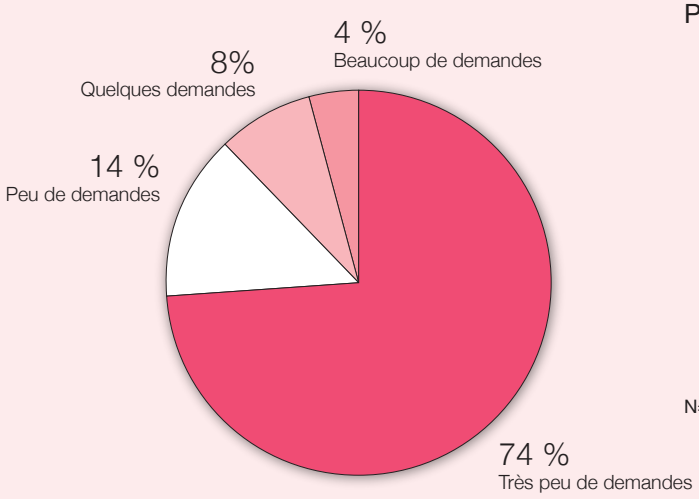
- Les entreprises de l'ingénierie sont tout à fait contre (44%) et le Management dans une moindre mesure (25%)

- Les petites entreprises (10 à 19 salariés) sont tout à fait contre (32%) contre 15% pour les entreprises de plus de 100 salariés.

N= 510 entreprises

☐ DEMANDE DES SALARIÉS POUR LE TÉLÉTRAVAIL À DOMICILE

Demande des salariés pour travailler régulièrement aux horaires de bureau à leur domicile



Principales raisons des demandes

- Temps de transport excessif (42%)
- Besoin de travailler au calme (25%)
- Equilibre de vie (22%)
- Meilleures conditions de travail (22%)
- Peu de différences en fonction des effectifs. Moins de demandes dans les petites structures
- Des différences importantes entre secteur : très peu de demandes dans l'ingénierie (82%) contre 59% dans l'édition.

N= 415 entreprises

■ ACCORDS ENTREPRISES *

Dans le cadre de la mise en place du télétravail, on assiste à une croissance du nombre d'accords d'entreprises dont plusieurs accords conclus dans les grandes entreprises de la Fédération (Microsoft, Oracle, Atos Origin, Accenture et SGS). Quels sont-ils ?

Définition :

organisation en alternance du travail entre le domicile et l'entreprise, distinguée du travail nomade. Le télétravail n'est jamais intégral : le salarié doit revenir travailler sur site à une fréquence variable selon les accords. Le télétravail s'applique à tous les salariés dont l'activité est compatible avec cette organisation.

Caractéristiques :

double volontariat, double réversibilité, période probatoire.

Formalisation :

la plupart des entreprises contractualisent la mise en place du télétravail par un avenant (à durée déterminée ou non) au contrat de travail qui précise le lieu, les horaires, les éléments importants à l'exécution du télétravail.

Conditions d'emploi du télétravailleur :

des dispositions particulières liées au statut de télétravailleur visent à le protéger de l'isolement. Ainsi, le télétravailleur doit bénéficier d'une protection contre l'isolement et maintenir le lien avec l'entreprise grâce notamment au suivi exercé par un responsable hiérarchique et sa participation au sein de l'entreprise à des événements importants.

Horaires :

les télétravailleurs doivent respecter les mêmes horaires que les salariés sur site. Ils peuvent bénéficier d'autres horaires si ceux-ci ont fait l'objet d'un avenant à leur contrat de travail. de travail. A l'exception des accords SNEDA et Michelin, il n'y a pas de réel contrôle.

Droits :

les télétravailleurs ont les mêmes droits individuels et collectifs que les autres salariés ET bénéficient également, au même titre que les autres salariés, à la formation individuelle.

Obligations de l'employeur :

l'employeur s'engage à assurer au télétravailleur la protection des données, de la vie privée, à fournir le matériel informatique ou autre nécessaire à l'exercice de l'activité professionnelle et à appliquer les dispositions légales de même que les contrôles nécessaires en matière de sécurité. A noter que certains accords évoquent la mise en place d'éventuels moyens de contrôle via la cybersurveillance (voir le chapitre 5 consacré à la cybersurveillance et outils TIC).

* Selon modèle des accords d'entreprises mis en place par Atos Origin (accord du 15/04/2010, Oracle France (accord du 29/01/2010), France Telecom SA (accord du 22/06/2009), Michelin (accord du 12/05/2009), SNEDA (accord du 31/12/2008), Renault SAS (accord du 22/01/2007), Tokheim Services France SAS (accord du 07/07/2005)

JURISPRUDENCE

Etat des lieux de la jurisprudence en matière de télétravail

Conditions de mise en place :
nécessaire respect de la procédure d'information de consultation des IRP avant la mise en place du télétravail. L'employeur ne peut exiger du CE qu'il ne rende son avis sans que le CHSCT se soit prononcé (CA Paris, 14e ch., sect. A, 13 mai 2009).

Nécessaire accord du salarié (Cass. Soc., 7 avril 2010) L'absence de formalisation de situations de télétravail par un avenant, si elle n'empêche pas les salariés de les invoquer, doit jouer en leur faveur. En conséquence, un accord est requis pour mettre fin à la situation de télétravail constatée (Cassation. Soc. 29 novembre 2007).

Volontariat et réversibilité du télétravail :
un accord du salarié et de l'entreprise est requis pour exercer la réversibilité et modifier le contrat de travail. En conséquence, le licenciement du salarié ayant refusé qu'il soit mis fin unilatéralement à une situation de télétravail est sans cause réelle et sérieuse.

Jurisprudence en ce sens :
retour au bureau imposé après le congé maternité d'une salariée préalablement en télétravail (Cassation. Soc. 31 mai 2006) – mutation d'un salarié impliquant la fin de son télétravail (Cassation Soc. du 31 octobre 2006) – Directeur commercial tenu de travailler au siège situé à 200 km de son domicile (Cassation Soc. 13 avril 2005).

Conditions de travail :
une indemnité proportionnelle à la contrainte imposée est due au salarié dès lors qu'une partie de son domicile est transformée en bureau (Cassation Soc. 7 avril 2010)

Heures supplémentaires :
la qualité de cadre et l'existence d'une liberté d'organisation liée à l'exécution d'un travail à domicile ne suffisent pas à exclure le droit au paiement d'heures supplémentaires, sauf à constater l'existence d'un salaire forfaitaire compensant les dépassements d'horaire résultant des impératifs de la fonction assurée (Cassation. Soc. 18 octobre 2006).

Le droit commun à vocation à s'appliquer dans le cadre du travail à domicile. Par conséquent, si la charge de la preuve des heures effectivement travaillées par le salarié n'incombe spécialement à aucune des parties, l'employeur doit néanmoins fournir les éléments de nature à justifier les horaires effectivement réalisées par le salarié. Il appartient, cependant, à celui-ci de fournir préalablement des éléments de nature à étayer sa demande et à rendre vraisemblable l'accomplissement d'heures supplémentaires (CA Bordeaux Chambre sociale Section A, 28 septembre 2010).

Accidents du travail :
trois exemples de jurisprudence concernant des accidents survenus à des salariés en télétravail considérés comme accident professionnel :

- Accident dans l'escalier extérieur du domicile d'un salarié qui retournait travailler : accident du travail (Cassation. Soc. 18 novembre 1993)

- Accident d'un salarié au sortir du bureau de poste : l'accident qui s'est produit au temps et au lieu de travail a été considéré comme un accident professionnel, la victime n'ayant pas de bureau extérieur à son domicile et l'accident étant survenu un jour ouvrable, à une heure normale de travail d'un salarié, en un lieu justifié par son activité professionnelle (Cassation Soc. 11 avril 1996)

- Accident d'un vendeur survenu pendant les horaires de travail indiqués par l'employeur alors que le salarié chargeait dans son véhicule les documents et échantillons entreposés dans son garage avant de partir visiter les clients. La présomption d'imputabilité au travail de l'accident est établie ce qui permet de qualifier l'accident de professionnel (CA Pau Chambre sociale 27 septembre 2010).

LES POINTS À RETENIR *

- *38% des entreprises ont au moins un salarié travaillant à domicile aux horaires de bureau. Dans ces entreprises 1,7 salarié travaille de manière régulière à domicile.*
- *11% des entreprises souhaitent développer le télétravail à domicile alors que 58% sont contre (24% des entreprises du secteur Etudes de marché et d'opinion et 16% des SSII sont en faveur – 4% des entreprises de l'ingénierie sont pour le télétravail à domicile).*
- *Des demandes de la part des salariés dans 12% des entreprises*
- *18% des entreprises ont des problèmes d'accès pour certains de leurs sites*
- *Le mode de formalisation préféré est constitué par les avenants (34% des entreprises où le télétravail à domicile est présent).*

* Selon les résultats de l'enquête IDC pour ADESATT réalisée par téléphone auprès de 510 entreprises tous secteurs confondus de plus de 10 salariés durant les mois de juin et juillet 2010, selon la méthode des quotas.

5/
LA CYBERSURVEILLANCE ET LES OUTILS TIC

5/ LA CYBERSURVEILLANCE ET LES OUTILS TIC *

* Selon présentation ADESATT du 11 mai 2010

Définition :
la cybersurveillance est la surveillance par l'employeur de l'activité de ses salariés dans le cadre de leurs activités pour l'employeur, au moyen d'outils TIC.
La cybersurveillance doit être justifiée au regard de la tâche à accomplir et respecter la vie privée des salariés.

Principes :
l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps du travail s'il en a informé ses salariés (la surveillance clandestine est illicite) et procéder au préalable à une déclaration auprès de la CNIL (Commission Nationale Informatique et Libertés).

LES OUTILS DE CONTRÔLE

Plusieurs outils permettent d'exercer une cybersurveillance.

Identification physique :
par cartes et badges, biométrie, vidéosurveillance.
Ces différentes solutions d'identification peuvent être reliées à l'application de gestion du temps de travail ou à d'autres applications de l'entreprise.

Cartes et badges :
ceux-ci permettent la prévention d'intrusions physiques ainsi que le contrôle du temps de travail. La tendance actuelle est à l'utilisation de la carte à puce qui se révèle efficace comme autentifieur, via un code confidentiel ou biométrique.

▸ *Réglementation et jurisprudence :*
selon la norme simplifiée n°42 et le jugement de la Cour de Cassation, ch. Soc. du 6 avril 2004, Allied System Industrial Fibers c.M.X : licéité du dispositif de contrôle électronique d'entrée et de sortie du personnel à condition d'en informer préalablement les salariés concernés. A défaut de déclaration à la CNIL, le refus de déférer à une exigence de son employeur impliquant la mise en œuvre d'un tel traitement ne peut lui être reproché.

Biométrie :
sert à éviter les usurpations d'identité et vérifier les habilitations. La biométrie est basée sur l'analyse morphologique propre à un individu (empreintes digitales, iris, etc.). La tendance actuelle est à la mise à jour dynamique des modèles de reconnaissance par le biais de mesures morphologiques qui prennent en compte le développement naturel de la personne. La reconnaissance veinale est l'une de ces tendances, autre axe de développement également à l'étude : la multimodalité qui consiste à combiner des reconnaisseurs de voix et visages pour améliorer la fiabilité d'un système.

▸ *Réglementation et jurisprudence :*
article 25-8 Loi Informatique et Libertés, autorisation préalable auprès de la CNIL et le jugement du TGI Paris, sect. Soc. du 19 avril 2005 Syndicat Sud Rail c/Efa Service relatif au système de pointage par empreintes digitales qui n'est ni adéquat, ni pertinent, ni justifié au regard de l'objectif de l'établissement des bulletins de paie.

Vidéosurveillance :
prévient les éventuelles intrusions physiques dans les locaux de l'entreprise. La vidéosurveillance est un système de caméras disposées dans un espace privé pour le surveiller le jour comme la nuit qui permet notamment de comptabiliser les entrées et sorties. Les images obtenues grâce à ce système peuvent être visionnées en temps réel ou enregistrées. La tendance actuelle est aux caméras vidéo mobiles contrôlables à distance et les caméras numériques consultables via Internet (caméra IP), ce qui permet un flux vidéo permanent.

▸ *Réglementation et jurisprudence :*
Loi Informatique et Libertés relative à la captation d'images sur un lieu du secteur public ou privé où le public ne peut accéder et Loi du 21 janvier 1995 (article 10) relatif à la captation d'images lieu public ouvert au public si aucune image n'est enregistrée dans des traitements informatisés ou des fichiers structurés permettant d'identifier des personnes. Jurisprudence Cour de Cassation, ch. Soc. 7 juin 2006 Continent France relatif à l'illicéité du dispositif qui na pas été préalablement porté à la connaissance du salarié même si le salarié ne pouvait sérieusement ignorer l'existence des caméras vidéo. Jurisprudence Cour de Cassation, ch. Soc. du 20 novembre 1991 relatif à licéité du système de vidéosurveillance destiné au contrôle des salariés si ce dispositif est justifié par la nature de la tâche à accomplir et proportionné au but recherché. Jurisprudence Cour d'appel de Paris 19 mars 2001 : employeur condamné à une amende de 100 000 Frs 80 000 Frs de dommages et intérêts, et quatre mois de prison avec sursis pour avoir équipé, sans en avoir informé le salarié en question, le lieu de travail de caméra installées dans des faux plafonds.

Identification logique :
par le biais de solutions (Solutions d'authentification unique SSO, gestion des droits d'accès utilisateur, authentification forte, infrastructures à clés publiques…) destinées à identifier les utilisateurs au sein du système d'information et de l'entreprise et à contrôler leurs droits d'accès aux ressources du système d'information et aux locaux de l'entreprise, en associant un ensemble de droits et de restrictions à chacune des identités établies.

Identification unique SS0 :
évite les usurpations d'identité et vérifie les habilitations. L'authentification unique (en anglais Single Sign-On ou SSO) est une méthode qui permet à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications informatiques ou sites web sécurisés et permet de mettre en place une politique centralisée des accès pour les applications. De plus, le SSO traçant les accès utilisateurs aux applications cibles permet de faire le lien entre un utilisateur et un identifiant sur une application donnée.

Authentification forte :
pour éviter les usurpations d'identité et vérifier les habilitations. Cette procédure requiert la concaténation d'au moins deux éléments ou facteurs d'authentification. L'authentification forte garantit : l'autorisation ou contrôle d'accès (qui eut y avoir accès ?), la confidentialité (qui peut le voir), l'intégrité (qui peut le modifier), la traçabilité (qui l'a fait). Tendances actuelles : on distingue actuellement trois familles technologiques : One Time Password (mot de passe à usage unique), le certificat numérique, la biométrie.

Authentification forte Tokens :
objectif : éviter les usurpations d'identité et vérifier les habilitations. Un Token est une solution matérielle qui gère les identités et les accès. Tendance actuelle : évolution des solutions token USB capable de se connecter depuis toute machine sans middleware installé ni besoin d'être administrateur de la machine

Réglementation : identification et authentification logique répondent à une réglementation définit par l'article 34 de la Loi Informatique et Libertés sur l'obligation de sécurité et de confidentialité imposée à l'employeur. Travaux : conseils de la CNIL en matière de sécurité des systèmes d'information 12/10/2009 : adopter une politique de mot de passe rigoureuse, concevoir une procédure de création et de suppression des comptes utilisateurs, sécuriser les postes de travail, identifier précisément qui peut avoir accès aux fichiers.

LE CONTRÔLE DES CONTENUS INFORMATIQUES

Sécurité et contrôle de la messagerie :
l'enregistrement des emails entrants et sortants a pour but de préserver les intérêts de l'entreprise, de veiller à ce que les informations confidentielles ne soient pas transmises par ce biais ou que le contenu des emails expose l'employeur à des problèmes (dans le cas de contenus inappropriés par exemple). Tendance actuelle : analyse sémantique, morphologique, suivi et contrôle des outils de messagerie instantanée et autres outils Web 2.0.

Réglementation et jurisprudence : la norme simplifiée n°46 couvre les systèmes de messagerie électronique professionnelle SAUF si le système permet le contrôle individuel des salariés.
Deux jugements ont fait jurisprudence dans ce domaine : Cour de Cassation, ch. Soc. du 2 octobre 2001, Nikon – le salarié a droit, même au temps et au lieu de travail au respect de l'intimité de sa vie privée et au secret des correspondances ; l'employeur ne peut prendre connaissance des messages personnels émis et reçus par le salarié, même lorsque l'utilisation non-professionnelle de l'ordinateur avait été interdite.
Cour de Cassation, ch. Soc. du 17 juin 2009, arrêt du « corbeau » - l'employeur ne peut ouvrir (sauf risque ou événement particulier) les messages identifiés par le salarié comme personnels qu'en présence de ce dernier ou celui-ci dûment appelé.

Filtrage et traçabilité web :
élimination des logiciels espions et programmes malveillants pour filtrage des sites et services internet autorisés. Tendance actuelle : suivi des blogs et autres services 2.0 (réseaux sociaux par exemple).

Logiciels d'agrégation et de corrélation des logs :
ils permettent d'obtenir des informations brutes sur les activités d'un réseau pour respecter la réglementation, empêcher les employés d'accéder à des sites non autorisés et de permettre aux administrateurs d'analyser les utilisations des différentes ressources du parc informatique afin de sécuriser, fiabiliser et optimiser le système d'information. De plus, la journalisation offre une garantie juridique lorsque la responsabilité de l'entreprise est engagée ou lorsqu'un individu malveillant s'introduit au sein de son réseau. Tendance actuelle : prise en compte des applications web 2.0 (messagerie instantanée, réseaux sociaux, blogs…).

Réglementation et jurisprudence : la norme simplifiée n°46 couvre la mise à disposition d'outils destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux SAUF si le système permet le contrôle individuel des salariés. Le jugement rendu par la Cour de Cassation ch. soc. du 9 juillet 2008, Franck L./ Entreprise Martin stipulent que les connexions internet d'un salarié durant son temps de travail sont présumées avoir un caractère professionnel : l'employeur peut les rechercher et les identifier en son absence. Un autre jugement rendu par la Cour de Cassation, ch. soc. du 18 mars 2009, M.X/ Société Lauzin est constitutif d'une faute grave pour utilisation de la connexion internet de son entreprise à des fins non professionnelles, pour une durée totale d'environ 41 heures sur un mois.

Contrôle des postes utilisateurs :

pour éviter les divulgations d'informations en cas de perte ou de vol, veiller au respect de la politique de sécurité de l'entreprise, éviter des modifications non conformes des configurations informatiques (ces solutions peuvent également comprendre des fonctions de prise en main à distance).

Réglementation et jurisprudence : la norme simplifiée n°46 couvre la mise à disposition d'outils destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux (sauf si le système permet le contrôle individuel des salariés).
Plusieurs jugements ont fait jurisprudence.
La Cour de Cassation, ch. soc. du 17 mai 2005, Philippe X. c/Société Cathnet-Science a statué sur le fait l'employeur ne peut ouvrir les fichiers identifiés comme personnels qu'en présence de ce dernier ou celui-ci dûment appelé, sauf risque ou événement particulier.
La Cour de Cassation, ch. soc. du 18 octobre 2006, Jérémy L-F c/Technisoft : les dossiers et fichiers créés par un salarié sont présumés avoir un caractère professionnel, de sorte que l'employeur peuty avoir accès hors sa présence sauf si le salarié les identifie comme personnels.
La Cour de Cassation, ch. soc. 29 décembre 2009, Alain : l'intitulé des répertoires « Alain » ne permet pas d'identifier les fichiers litigieux comme personnels et n'interdisait pas leur ouverture par l'employeur en l'absence du salarié.

LE CONTRÔLE DES COMMUNICATIONS VOCALES

Registre des appels et des temps de communication :

pour contrôler le temps et le volume des communications, les numéros appelés ou reçus sur téléphones fixes et mobiles. Cette solution permet le contrôle du temps et du volume des communications, des numéros appelés ou reçus, d'observer et de taxer le trafic.

Réglementation et jurisprudence : norme simplifiée n°47 relative à l'utilisation de services de téléphonie fixe et mobile sur les lieux de travail. Deux jugements en Cour de Cassation ont fait jurisprudence : Cour de Cass. , ch.soc. 29 janvier 2008, M.X/Canon France : licéité de l'autocommutateur relevant simplement la durée, le coût et les numéros des appels passés à partir de chaque poste même en l'absence d'information préalable. Cour de Cassation, ch. soc. du 6 avril 2004, M.X/Société BDI Construction : les salariés investis d'un mandat électif/syndical doivent pouvoir disposer d'un matériel excluant l'interception de leurs communications et l'identification de leurs correspondants. Illicéité du matériel desservi par l'autocommutateur de l'entreprise fourni au délégué.

Enregistrement des appels téléphoniques (fixes et mobiles) :

cette solution permet à l'entreprise de présenter des preuves, de prévenir les pertes et divulgation d'informations, d'augmenter la qualité et la productivité des services téléphoniques.

Réglementation et jurisprudence : fiche pratique de la CNIL : enregistrement des conversations téléphoniques sur le lieu de travail portant sur les thèmes suivants : principes de légitimité de proportionnalité, déclaration normale, possibilité de neutraliser les enregistrements pour les appels privés, obligation d'information des salariés et des interlocuteurs, durée de conservation des enregistrements (entre 6 mois et 1 an).
Jurisprudence : Cour de Cassation, ch. Soc. 14 mars 2000, M.X/Instinet France : l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps du travail, l'emploi de procédé clandestin de surveillance est illicite. Les écoutes réalisées constituent un mode de preuve valable dès lors que les salariés ont été dûment avertis de ce que leurs conversations téléphoniques seraient écoutées.

Géo-localisation :

une solution pour piloter, gérer et contrôler en temps réel l'activité des équipes et matériels itinérants par le biais d'un GPS et d'un modem GPRS/3G, ce type de solution peut être embarqué ou lié à un terminal mobile et permet de fournir des rapports d'activités détaillés (horaires, temps d'arrêts et de trajets, distance, vitesse, lieu, etc.).

Réglementation et jurisprudence : norme simplifiée n°51 (délibération n°2006-067 du 16 mars 2006). Traitements automatisés destinés à géo-localiser les véhicules utilisés par les employés.
Jurisprudence : Cour d'Appel d'Agen, ch. Soc. 3 août 2005, Pierre T./SAS SICO : la géo-localisation d'un véhicule doit être proportionné au but recherché ; lorsqu'il existe d'autres moyens de vérifications, la mise sous surveillance permanente des déplacements des salarisé est disproportionnée donc illégale.
Cour d'Appel de Grenoble, ch. soc. 29 novembre 2006, Pierre C./SA STEM : sans information et consultation préalables des instances représentatives : le système de géo-localisation (GPS) utilisé pour contrôler les salariés est illégal – Les enregistrements constituent un moyen de preuve illicite même en cas de faute.

LES POINTS À RETENIR *

Indice de satisfaction des entreprises tous secteurs confondus dans le cadre du suivi de l'activité des salariés avec les TICs

- *52 % satisfaites*
- *5% tout à fait satisfaites*
- *39% inexistante*
- *4% insatisfaisantes*

* selon enquête ADESATT du 27/07/2010

6/ PRINCIPES JURIDIQUES GENERAUX DE LA CYBERSURVEILLANCE

6/ PRINCIPES JURIDIQUES GENERAUX DE LA CYBERSURVEILLANCE

LA RÉGLEMENTATION FRANÇAISE

La réglementation française en matière de cybersurveillance relève à la fois du Droit Social (pour ce qui concerne le dispositif de contrôle des salariés) et du Droit de la protection des données personnelles (pour ce qui du traitement de données personnelles).

Règles de Droit Social

La cybersurveillance doit être justifiée au regard de la tâche à accomplir dans le respect de la vie privée des salariés comme le prévoit l'article L. 1121-1 du Code du travail (règles de fond).
La cybersurveillance doit faire l'objet d'une information préalable du salarié (article L. 1222-4 du Code du Travail) de même qu'une information et consultation préalable des instances représentatives du personnel (articles L. 2323-13 et L. 2323-32 du Code du Travail)

Règles de Droit de la protection des données personnelles

(telles que définies par la Loi Informatique et Libertés du 6 janvier 1978, modifiée le 6 août 2004) :
Règles de fond : selon l'article 6 de la Loi Informatique et Libertés qui statue sur le traitement loyal et licite, les finalités déterminées, explicites et légitimes, les données adéquates, pertinentes, non excessives, exactes, complètes, à jour, la conservation pour la durée nécessaire aux finalités et l'article 34 de la Loi Informatique et Libertés (sécurité et confidentialité des données).

Règles de forme :

définies par l'article 32 de la Loi Informatique et Libertés qui a pour but d'informer au préalable les personnes dont les données sont collectées et par l'article 22 et suivants de la Loi Informatique et Libertés.

Mise en œuvre des règles juridiques

Les rapports de la CNIL sur la cybersurveillance (datant de mars 2001 et mars 2004) définissent les principes généraux de la mise en œuvre des règles juridiques, fournissent des recommandations concernant l'utilisation des outils de cybersurveillance et le rôle des administrateurs informatiques et comportent des propositions pour une meilleure prise en compte des principes informatiques et libertés sur les lieux de travail.
Le Guide de la CNIL (2008) à destination des employeurs et des salariés propose un rappel des principes généraux et des formalités à accomplir, des fiches pratiques sur les outils de cybersurveillance.

LES DIRECTIVES EUROPÉENNES

Selon la directive européenne relative à la protection des personnes physiques (directive 95/46 CE du 24 octobre 1995) dont les termes concordent avec les grands principes définis par la CNIL à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

☐ OUTILS TIC : LES ENTREPRISES SONT-ELLES SUFFISAMMENT INFORMÉES SUR LA RÉGLEMENTATION ?

- *22% des entreprises se considèrent très mal informées à propos de la réglementation portant sur les outils TIC utilisés par les salariés.*
- *Des différences apparaissent par secteur et par taille d'entreprises : 24% des petites entreprises de 10 à 19 salariés contre 17% dans les sociétés de plus de 100 salariés se considèrent très mal informées.*
- *32% dans les entreprises du secteur Etudes de marché et d'opinion et 30% dans les entreprises de l'ingénierie sont mal informés contre 4% et 15% respectivement dans les entreprises du secteur management et les SSII.*

ADESATT
3, rue Léon Bonnat
75016 PARIS

Tél. 01 44 30 49 00