UNIVERSITE DE LILLE

FACULTE DES SCIENCES JURIDIQUES, POLITIQUES ET SOCIALES

MEMOIRE DE MASTER II DROIT DU CYBERESPACE

RGPD ET CONTROLE EN ENTREPRISE

LES IMPACTS DU RGPD SUR LE CONTROLE DES SALARIES

Monsieur Adjété Fabrice Olufèmi WILSON

DIRECTEUR DU MEMOIRE

Michel RIME

DPO / Enseignant à la faculté des Sciences Juridiques, Politiques et Sociales de l'Université de Lille

SUFFRAGANT

Marcel MORITZ

Maitre de Conférences HDR / Directeur du Master Droit du Numérique de l'Université de Lille

ANNEE UNIVERSITAIRE 2018-2019

L'université de Lille n'entend donner aucune approbation ni improbation aux opinions émises dans ce document ; ces opinions doivent être considérées comme propres à leur auteur.

Dédicace

A mes parents, Ghislaine et Samuel

A ma tante Léontine et son époux Blaise

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma gratitude.

Je voudrais dans un premier temps remercier, mon directeur de mémoire M. RIME, DPO/Enseignant à l'université de Lille, pour sa patience, sa disponibilité et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion.

Je remercie également le professeur Marcel MORITZ, Maître de Conférence HDR à l'Université de Lille pour son écoute, sa disponibilité et ses précieux conseils, qui ont contribué à alimenter ma réflexion.

Je tiens également à remercier toute l'équipe pédagogique de l'université de Lille et les intervenants professionnels responsables de ma formation, pour avoir assuré la partie théorique de celle-ci.

Je tiens à témoigner toute ma reconnaissance aux personnes suivantes, pour leur aide dans la réalisation de ce mémoire :

Madame Caroline FLORINDA, pour la confiance placée en moi en m'accordant un stage de fin d'étude, ses précieux conseils tout au long du stage et son orientation dans le choix de ce sujet.

Monsieur Christian FRULEUX auprès de qui j'apprends beaucoup sur les défis à relever dans le monde professionnel. Il partage avec moi ses connaissances et expériences dans ce milieu, tout en m'accordant sa confiance et une large indépendance dans l'exécution de missions valorisantes.

Mesdames et messieurs Angélique DESMAREST, Sabrina BONIFAZI, Jean Pierre TEXIER et Laurent BREYNE pour les missions intéressantes et valorisantes qu'ils me permettent d'exécuter, ainsi que leurs précieux conseils quotidiens.

Mademoiselle Amandine BODJRENOU, pour son soutien, ses conseils et relecture.

Monsieur Cyrille NUGA, pour avoir relu et corrigé mon mémoire. Ses conseils de rédaction ont été très précieux.

Mesdemoiselles Philippine TAMIC et Stéphanie ESSIMI, pour leur soutien, conseils et relecture

MOTS-CLES – KEYWORDS

Ubiquité : ubiquité vient du latin "ubique" qui signifie "partout. Le don d'**ubiquité** est un don réservé aux dieux, puisqu'il s'agit d'une faculté divine permettant d'être présent partout ou à plusieurs endroits à la fois.

Ordiphone : téléphone intelligent. (Recommandation officielle pour smartphone.)

Obligation de moyens : l'obligation de moyen est une obligation juridique régie par l'article 1137 ancien du Code civil, en vertu de laquelle le débiteur s'engage à fournir tous les efforts nécessaires pour essayer d'atteindre l'objectif fixé. L'obligation de moyen s'oppose à l'obligation de résultat qui, comme son nom l'indique, fixe un résultat à atteindre. Ainsi, le fait de ne pas atteindre un résultat précis n'engagera pas automatiquement la responsabilité du débiteur d'une obligation de moyen. Cela signifie qu'en cas d'engagement de la responsabilité, il incombera au créancier de prouver que son débiteur n'a pas mis en œuvre toutes les solutions dont il disposait pour atteindre le résultat. Il n'est désormais plus défini par le Code Civil mais la doctrine fait référence aux conditions dans lesquelles elle s'exerce dans l'article 1231 du même Code.

Obligation de résultat : l'obligation de résultat est une obligation en vertu de laquelle un débiteur est contraint d'atteindre un résultat précis et déterminé en avance. Le fait pour le débiteur de ne pas atteindre le résultat escompté engage automatiquement sa responsabilité. L'obligation de résultat se distingue de l'obligation de moyen dans le sens où cette dernière n'entraine pas l'obligation pour son débiteur d'atteindre un résultat précis, mais lui impose seulement de tout mettre en œuvre pour tenter d'atteindre un objectif. Dans le cadre d'une obligation de résultat, le débiteur ne pourra échapper à sa responsabilité qu'en démontrant la survenance d'un cas de force majeure l'ayant empêché d'atteindre le résultat escompté.

SEVESSO II : la directive Seveso est le nom générique d'une série de directives européennes qui imposent aux États membres de l'Union européenne d'identifier les sites industriels présentant des risques d'accidents majeurs, appelés « sites Seveso », et d'y maintenir un haut niveau de prévention.

SOMMAIRE

LISTE DES ABREVIATIONS

AFNOR ..... Association Française de Normalisation

CNIL …….. Commission Nationale Informatique et Libertés, il s'agit de l'autorité de contrôle pour la FRANCE au sens du RGPD

DLP ……. Data Loss Prevention : ensemble de techniques qui permettent d'identifier, de contrôler et de protéger l'information grâce à des analyses de contenu approfondies, que l'information soit stockée, en mouvement ou traitée

G29 …… Le G29 ou Groupe de l'Article 29 est un regroupement de l'ensemble des autorités de protection des données personnelles en Europe

IDS ……. Intrusion Detection System : mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

IPS …… Internet Provider Security : utiliser par les gestionnaires de nom de domaine pour administrer la gestion d'un nom de domaine

PGI ……. Progiciel de Gestion intégrée : outil informatique permettant de piloter le Système d'Information d'une entreprise

WAF …… Web Application Firewall : politique de sécurité mise en place entre une application web et l'utilisateur final

INTRODUCTION

L'ancien président de la Commission Nationale Informatique et Libertés disait en 2011 dans son ouvrage intitulé La vie privée en péril: «les caméras nous filment, les lecteurs biométriques nous identifient et nous reconnaissent, les dispositifs de géolocalisation nous repèrent et nous suivent, les applications Internet nous profilent, analysent nos goûts et enregistrent nos habitudes, les micros nous écoutent, l'arsenal des fichiers nationaux, européens et internationaux se déploie, le nuage numérique enveloppe la planète, l'informatique contextuelle comblera peu à peu les espaces disponibles entre nos pensées respectives, les nanotechnologies rendront les systèmes invisibles et donc innombrables et irréversibles »[1].

Le monde fait et continuera de faire face à n'en point douter, à une constante évolution des technologies numériques. L'on ne conçoit plus aujourd'hui une économie qui ne place le développement des technologies numériques au centre de ses objectifs. Les défis numériques sont de plus en plus importants et certains pays prennent plus à cœur ces défis que d'autres.

Les Etats Unis depuis le développement de l'Arpanet dans les années 1960 restent de façon incontournable les maîtres incontestés de la technologie numérique. L'Europe quant à elle fait des efforts, mais est toujours en retrait face à la Chine qui monte en puissance depuis les années 2000.[2]

Cette évolution s'accompagne d'une augmentation de la vulnérabilité des entreprises et d'une recrudescence des cybers attaquants.

Les moyens de surveillance et de protection des systèmes d'information sont donc des manifestations de lucidité de la part des employeurs. Pas une semaine, en effet, ne se passe sans qu'une faille majeure de sécurité ne vienne s'ajouter au cirque incessant des désastres informatiques.

Conscient de la nécessité d'assurer une protection minimale, le législateur a imposé une obligation de sécurité à tout responsable du traitement de données personnelles. La loi informatique et libertés elle, oblige, en effet, de mettre en place toutes les

[1] Alex Türk, La vie privée en péril, 2011, p 261

[2] Cyrielle Gaglio et Sarah Guillou, L'Europe face aux défis numériques, Dans L'économie Européenne(2019), pp 113-124

précautions utiles afin de protéger son traitement. En vertu de cette obligation, et pour assurer la préservation de leurs biens informatiques, les organisations mettent souvent en œuvre des systèmes de détection et de prévention contre les intrusions (IDS, IPS, DLP, WAF, etc.)[3], des systèmes de prévention des fuites de données (DLP…), la surveillance vidéo, le contrôle d'accès par badge ou biométrie, le recours à des détectives privés et même parfois la géolocalisation des véhicules des salariés.

De manière générale, les obligations liées à l'exploitation de ces différentes technologies de contrôle de l'activité des salariés sont de deux ordres au moins : celles spécifiques au droit du travail (pouvoir de contrôle de l'employeur sur l'activité des salariés, devoir de loyauté…), et celles relatives à la loi informatique et libertés ainsi qu'au Règlement Général sur la Protection des données (information, proportionnalité…).

Du point de vue technique, le besoin de renforcement de la sécurité au sein des entreprises se fait de plus en plus ressentir. Pour atteindre cet objectif sécuritaire et faire face efficacement aux défis de la transformation numérique, et dans le respect de leur obligation légale, les employeurs mettent en œuvre des moyens de contrôle de l'activité des salariés.

[3] Confère liste des abréviations

A- Les enjeux et défis de la transformation numérique

L'utilisation des technologies de l'information (GPS, mouchards, surveillance des mails, biométrie...) soumet les salariés à une surveillance diffuse et permanente qui se concilie difficilement avec les principes fondamentaux du droit du travail tels que le droit à la vie privée. L'émergence de cette nouvelle forme de contrôle managérial sur les salariés tend à poser des problèmes d'ordre juridique et d'ordre éthique.[4]

L'influence des technologies de l'information et de la communication (TIC) sur la gestion des ressources humaines a alimenté une réflexion abondante depuis le début de la décennie tant de la part des juristes que des gestionnaires. Les juristes ont été invités à se prononcer sur les conditions de conciliation des mécanismes de cyber surveillance et du droit fondamental des salariés à la vie privée. Les gestionnaires ont tenté de mesurer l'influence des nouvelles technologies sur la flexibilité de l'organisation, sur l'émergence de nouvelles formes de pouvoir et sur la conciliation possible entre les besoins organisationnels et les désirs des individus.[5]

Notre société moderne est structurée autour de l'idée d'une rationalisation intégrale du système de surveillance. L'organisation sociale, telle que la prison, l'hôpital ou l'usine, est organisée selon le principe de l'efficacité du contrôle qui relaie le théâtre du châtiment.[6]

L'homme est donc considéré comme un être opprimé au sein de la société qui s'adapte et essaye bien souvent d'échapper aux mailles du filet.[7]

---

[4] Christine Noël-Lemaître, Humanisme et Entreprise, La cybersurveillance au travail, une nouvelle version du panoptisme managerial ? 2007/5 (n° 285), pages 49 à 64

[5] Yannick CHATELAIN et Loïck ROCHE, Le webmarketing en action, p 25

[6] Michel Foucault ; Surveiller et Punir. Naissance de la prison ; Collection Bibliothèque des histoires, Gallimard 1975

[7] Ibid 6

Marshall McLuhan pense que les technologies se développent et ont un impact sur la société. Pour lui, les technologies hypnotisent la société et c'est pour cette raison que « Toute nouvelle technologie diminue l'interaction des sens et de la conscience, et plus précisément dans le domaine nouveau des innovations où se produit une sorte d'identification du sujet et de l'objet »[8].

L'évolution du système d'information a été marquée par des vagues successives de centralisation, comme l'automatisation dans les années 1950 ou la mise en service des progiciels de gestion intégrés, et de décentralisation comme l'arrivée de l'informatique individuelle ou plus récemment des technologies Internet. Elle a abouti à une diffusion massive des TIC dans les entreprises : 94 % sont aujourd'hui connectées à Internet. Les taux d'équipement révèlent cependant des variations importantes en fonction de la taille de l'entreprise et du secteur d'activité.[9]

Cette évolution des systèmes d'information n'a toutefois pas connu de cycle de renouvellement systématique et le parc des matériels et logiciels a généralement grossi sans que ses nouveaux composants soient systématiquement intégrés à l'existant.

D'un autre côté, les technologies numériques ont apporté de grands changements au sein des entreprises. Ces changements impactent à la fois l'organisation, le management, la culture, le rapport au travail ainsi que tous les acteurs de l'entreprise.

L'apparition de l'internet et l'utilisation des outils mobiles permettent quant à eux un travail nomade avec plus d'autonomie dans le travail et une grande flexibilité.

De plus en plus, les entreprises ont recours à de nouveaux outils technologiques et les mettent à la disposition de leurs salariés pour permettre un travail plus rapide et plus efficient.

L'ordinateur portable est aujourd'hui largement répandu dans les entreprises qui en dotent prioritairement les salariés cadres. La majorité en dispose[10], à un niveau

[8] Marshall McLuhan, D'œil à oreille, avec Derrick de Kerckhove, Hurtubise HMH, 1977, (titre original : (en) Processus and Media) (Recueil d'articles et de commentaires), P 489

[9] Tristan Klein & Daniel RETIER, l'Impact des TIC sur les Conditions de travail, p 19

[10] 43 % dans l'enquête Conditions de travail de 2005 et 62 % dans le Baromètre Stress CFE-CGC

correspondant prioritairement à peu près au taux d'équipement du personnel. Ces ordinateurs portables fournis aux salariés garantissent généralement un accès à distance au réseau de l'entreprise à près de 69% d'entre eux selon le Baromètre Stress CFE-CGC OpinionWay.

En revanche, le téléphone mobile fait en grande majorité l'objet d'un achat privé qui concerne près de 90% des salariés. Près de la moitié des cadres en sont cependant dotés par l'employeur, mais cette diffusion en entreprise du téléphone mobile comme de l'ordinateur portable par l'employeur se réduit de plus en plus au profit de la mise à disposition d'ordiphone. 28% des cadres en sont équipés et la progression en est très rapide, de l'ordre de 10% en moins d'un an.[11]

Les ordiphones atteignent des niveaux de performance proches des ordinateurs portables et peuvent comme eux être connectés au réseau de l'entreprise. Certaines versions des Progiciels de Gestion intégrée (PGI) les plus puissants du marché sont utilisables à partir des ordiphones mis à la disposition des salariés. Cela pose sans nul doute des problèmes de sécurité nouveaux en multipliant les failles dans la protection du réseau d'entreprise.

Dans le cadre de la révolution technologique, les salariés sont donc directement impactés dans la mesure où les technologies numériques renforcent les exigences des collègues, supérieurs hiérarchiques, mais aussi des clients. Ceux-ci peuvent grâce aux technologies mobiles les joindre à tout moment, mais aussi simultanément développer le contrôle qu'ils ont dans leurs activités.[12]

Le travail se transforme, non seulement dans ses formes, mais aussi dans son contenu et dans son organisation, du fait des changements technologiques – numériques en particulier. D'un côté, la révolution numérique est porteuse de nouvelles opportunités d'emplois moins pénibles et moins répétitifs, d'une promesse d'autonomie et d'un accès facilité à la mise à niveau des compétences. De nombreuses entreprises sont

---

OpinionWay, Vague 15, de novembre 2010.

11 Baromètre Stress CFE-CGC OpinionWay, Vague 15, novembre 2010.

12 Charles-Henri Besseyre des Horts et Henri Isaac, l'impact des TIC mobiles sur les activités des professionnels en entreprise, Revue Française de Gestion 2006/9-10 n°168-169, pp 243 à 263

axées sur des projets de transformation numérique autour de l'Internet des Objets (IOT), l'automatisation des processus et le cloud. La mise en place de ces technologies au sein de l'entreprise accroît également de façon considérable le risque cyber pour les entreprises. Elles doivent donc de plus en plus faire face aux vulnérabilités et attaques potentielles tant à l'intérieur que venant de l'extérieur de l'entreprise.

Face à ces différents risques, les entreprises mettent sur pied des procédures de contrôle des salariés dans le cadre de leur contrat de travail.

B- Le lien de subordination face à la vie privée du salarié

Le lien de subordination n'est pas défini dans le Code du travail. Il conditionne cependant la qualification d'un contrat en contrat de travail. C'est la jurisprudence qui, dans l'arrêt dit « Société Générale » a posé les critères pour reconnaître ce lien[13]. Il se caractérise 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 de son subordonné.

Bien avant la transformation numérique, les modalités de management ont été considérablement bouleversées lorsque les organisations en mode projet se sont mises en place. En l'espèce, dès lors que le manager hiérarchique n'est pas nécessairement le chef de projet, il ne contrôle plus directement :

- les directives à exécuter ;
- leur bonne exécution.

Avec l'entreprise employeur regroupant bien les trois critères, le lien de subordination n'est pas juridiquement remis en cause.

Le manager conserve l'évaluation du managé. Toutefois, dans les organisations basées sur le management de projet, des tensions peuvent naître du fait que le manager ne maîtrise pas nécessairement les directives à exécuter. Il ne peut donc valablement en contrôler leur bonne exécution. La transformation numérique ne fait qu'ajouter une nouvelle complexité au management de projet, et accélère donc les évolutions numériques.

S'agissant des cas de travail à distance, le contrôle de l'exécution peut constituer une zone de tension et rapidement se réduire à un contrôle des livrables. Le risque est alors de transformer progressivement l'obligation de moyens en une obligation de résultat. Le lien de subordination se trouve toutefois confronté au respect de la vie privée du salarié.

---

[13] Cour de Cassation, Chambre sociale, du 13 novembre 1996, 94-13.187, Bull. civ. V, no 386 (https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000007035180)

L'article 9 du code civil dispose : « Chacun a droit au respect de sa vie privée ». L'article 8 de la Convention Européenne des Droits de l'Homme et des Libertés Fondamentales rajoute « … et familiale, de son domicile et de sa correspondance ». C'est pourquoi, l'article L 1121-1 du code du travail est venu préserver ce droit en énonçant « 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 ».

Le développement des technologies numériques a conduit à un abondant contentieux entre vie privé et droit de l'employeur de veiller au bon fonctionnement de l'entreprise par le contrôle de l'activité des salariés notamment.

Dans le même temps, il est mis à la charge de l'employeur une obligation de sécurité du salarié. Cette obligation est indispensable pour toute personne susceptible de travailler sous l'autorité hiérarchique d'une autre personne. Depuis un arrêt de la Cour de Cassation en 2002, cette obligation mise à la charge de l'employeur est devenue une obligation de résultat.[14]

L'employeur a donc l'obligation de mettre en œuvre des procédures garantissant non seulement la sécurité des locaux, mais également celle de ses salariés.

Ainsi, l'entreprise impose que des règles morales encadrent l'activité de ses membres. L'obligation de la conformité des pratiques aux bonnes mœurs est une obligation dévolue à l'employeur et il doit y veiller même s'il ne se fait pas censeur de ses salariés. Les technologies numériques rendent cependant difficiles cette obligation de l'employeur, car le salarié accède plus facilement à des contenus contraires aux bonnes mœurs et en publie sur internet plus que de lire dans l'entreprise un magazine répréhensible moralement ou de placarder des affiches insultantes.[15]

---

[14] Arrêt n° 835 du 28 février 2002, Cour de cassation - chambre sociale

[15] Matthieu Démoulain, Thèse « Nouvelles technologies et droit des relations de travail, Edition Panthéon Assas, 2012, Page 22

Toutefois, pour faire ressortir la distinction entre vie privée et vie professionnelle, les juges européens n'opposent pas l'espace de vie privé à l'espace de vie professionnelle.[16]

Pour les juges, l'atteinte à la correspondance peut naître de l'écoute des conversations téléphoniques d'un salarié, passées depuis un poste expressément dévolu à l'activité professionnelle alors même qu'est tenu à sa disposition un appareil dédié à ses conversations personnelles.[17]

L'objectif du législateur est de ce fait d'encadrer la mise en œuvre par les employeurs des moyens de contrôle des salariés afin d'éviter les abus.

Tout dispositif de contrôle mis en œuvre doit alors être toujours justifié et respecter la finalité recherchée.

C'est ainsi que dans le cadre de son devoir de prévention, l'employeur peut être amené à décider de mesures de surveillances destinées notamment à permettre une intervention rapide des secours dans les situations d'urgence.

Pour la réalisation de certains travaux, présentant des risques particuliers et graves, le Code du travail peut également imposer une étude de sécurité spécifique devant déboucher sur des mesures de sécurité particulières.

À ce titre, est admise par la CNIL la protection assurée par un système d'empreintes d'une zone spécifique à l'intérieur d'une installation nucléaire de base ou de certains sites classés SEVESO II.[18]

La finalité est de protéger des installations comportant un risque élevé d'explosion ou de diffusion de matières dangereuses ou de détournement de celles-ci par des tiers non autorisés, et d'assurer la protection de personnes exposées à des risques particuliers en raison de ces activités.

---

16 CEDH, 16 déc.1992, Série A n°. 251-B, p33

17 CEDH, 25 juin 1997, Halford c. Royaume-Uni, Recueil des arrêts et décisions 1997-III, p1016.

18 Confère liste des abréviations

En application de ces textes, le contrôle de l'activité des salariés doit toujours être justifié et strictement proportionné à la finalité recherchée par le dispositif mis en œuvre.

C- Le RGPD, un outil de réglementation du contrôle en entreprise

Le contrôle de l'activité des salariés n'a pas commencé avec le RGPD, un cadre légal existait bien avant et encadrait la mise en œuvre des moyens de contrôle par le salarié.

L'article L1222-4 du Code du travail prévoyait déjà une obligation d'information du salarié avant une quelconque mise en place d'un dispositif servant à recueillir des informations personnelles concernant un salarié.[19]

Les violations de données étant devenues récurrentes avec l'évolution des technologies numériques, la mise en place des dispositifs de surveillance a commencé à se renforcer avec la directive dite « Paquet télécoms ».

L'article 34 bis de la loi n° 78-17 du 6 janvier 1978 modifiée prévoyait déjà une obligation de notification à la CNIL de toute violation de données à caractère personnel. Cette obligation s'imposait uniquement aux Fournisseurs de services de communications électroniques au public, tels que définis par l'article L33-1 du Code des Postes et Télécommunications. Elle concernait fondamentalement les Fournisseurs d'accès à internet et les opérateurs de téléphonie fixe et mobile.

Il faut noter qu'une violation de données pouvait être retenue avec la directive dite « Paquet télécoms » lorsque trois conditions étaient réunies. Il faut d'une part qu'il y ait une intrusion dans la base de données de gestion d'un FAI, une faille dans la boutique en ligne d'un opérateur mobile permettant de récupérer les numéros de cartes de crédits des clients ayant commandé un nouveau téléphone associé à un forfait, un email confidentiel destiné à un client d'un FAI, diffusé par erreur à d'autres personnes ou la perte d'un contrat papier d'un nouveau client par un agent commercial d'un opérateur mobile dans une boutique. Si l'une de ces conditions était réunie, le Fournisseur d'accès à internet avait l'obligation de notifier dans les 24h qui suivent la violation à la CNIL.

[19] Article L1222-4 du Code du Travail (www.legifrance.gouv.fr)

Le RGPD est venu étendre la notification de violation à tous les secteurs d'activité et apporte une définition précise à la violation de données en son article 4-12. La violation de données à caractère personnel est définie comme : « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ».

Dans le même sens, l'article 34 bis de la loi informatique et libertés modifiée dispose que « la violation de données à caractère personnel est toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques. »

Le G29[20], aujourd'hui dénommé Comité Européen de la Protection des Données, dans son avis 03/2014 sur la notification des violations, considérait que les violations pouvaient être classées selon trois principes de sécurité de l'information bien connus[21] :

- Violation de la confidentialité : la divulgation ou l'accès non autorisés ou accidentels à des données à caractère personnel
- Violation de l'intégrité : l'altération non autorisée ou accidentelle de données à caractère personnel
- Violation de la disponibilité : la destruction ou la perte accidentelle ou non autorisées de l'accès à des données à caractère personnel

Les employeurs, craignant de plus en plus le risque de violation de données pouvant être dû à des collaborateurs qui ne maitrisent pas forcément la réglementation, renforcent de plus en plus les moyens de contrôle mis en place.

---

20 Confère sigles

21 Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, version révisée le 6 février 2018, I-B-2

Face à cette recrudescence du contrôle en entreprise, il convient de se demander si l'entrée en vigueur du RGPD a permis un renforcement de la vie privée des salariés face aux moyens de contrôle mis en place. Se contente-t-il de rappeler les normes existantes et de les faire respecter ou apporte-t-il de nouvelles évolutions pour un renforcement de la vie privée des salariés ?

Le contrôle de l'activité des salariés existait bien avant, surtout du fait d'un développement très rapide des technologies numériques et de l'obligation légale mise à la charge de l'employeur. Il ne peut cependant être omis que le RGPD offre des règles permettant un usage pour le moins plus contrôler de ces technologies numériques. Induisant des variations dans la mise en place des moyens de contrôle, il encadre les moyens de contrôle existant (Première partie) et tente de corriger les imperfections du cadre juridique actuel en adaptant le droit social aux évolutions technologiques pour permettre ainsi d'aboutir à un renforcement du cadre juridique du contrôle des salariés (Deuxième partie).

PARTIE I.

L'ENCADREMENT PAR LE RGPD DES MOYENS DE CONTROLE EXISTANTS

L’intégration des moyens de contrôle des salariés dans l’entreprise est une réalité qui ne saurait être ni ignorée, ni combattue. Les procédés de contrôle mis en place sont multiples et variés, allant des contrôles informatiques jusqu’à la fouille du salarié.

L’employeur a ainsi le droit d’accéder au matériel informatique mis à la disposition du salarié et d’en consulter les fichiers sauf lorsque ceux-ci sont marqués confidentiels.

De nombreuses personnes y voient un outil intrusif visant à faire tomber les barrières séparant vie professionnelle et vie privée. Les libertés ne prospérant et ne s’épanouissant que dans des cadres solides, des moyens de contrôle sont mis en place au sein des locaux de l’entreprise (Chapitre 1), mais également en dehors des locaux de l’entreprise (Chapitre 2).

Chapitre I.

Le Contrôle au sein de l’entreprise

L'obligation de contrôle est une obligation légale de l'employeur, corollaire du lien de subordination. Sa mise en œuvre passe par des dispositifs tels que le contrôle de l'accès aux locaux, l'obligation de décompte du temps de travail etc. Ainsi, les employeurs sécurisent les accès aux locaux et cela leur permet d'éviter au maximum les fuites de données (Section 1). Par ailleurs, ils mettent également en place parfois des systèmes de contrôle vidéo (Section 2).

SECTION I. LA PREVENTION DES FUITES DE DONNEES ET LE CONTROLE D'ACCES

Les données constituent aujourd'hui pour les entreprises une richesse. Qu'il s'agisse des données clients, des activités ou le fonctionnement interne de l'entreprise, elles peuvent être un atout concurrentiel important face aux autres entreprises du marché. C'est donc pour protéger ces données détenues que des technologies anti intrusion et perte de données (A) sont mises en place. Des technologies comme la biométrie sont également mises en œuvre et le RGPD vient apporter sa contribution à leur encadrement (B).

A. LES DISPOSITIFS DE CONTROLE ANTI INTRUSION ET PERTE DE DONNEES

En Janvier 2015, l'Association Française de Normalisation (AFNOR) publiait son premier guide de bonnes pratiques de prévention et de la gestion des fuites d'informations (AFNOR BP Z90-001). Dans cette perspective, les entreprises ont de plus en plus recours aux technologies de Data Loss Prevention, mais mettent également en place des technologies de contrôle d'accès aux locaux de l'entreprise.

- **Le Data Loss Prevention (DLP)**

L'évolution des menaces et de la réglementation pousse les entreprises à être de plus en plus attentives à leurs données et à orienter les protections sur ce périmètre. Les solutions de prévention contre la fuite d'information, ou DLP, apportent des éléments de réponses à leur problématique. Il est de notoriété constante que le savoir-faire d'une entreprise se trouve surtout dans ses bases de données. Depuis les listes clients, les factures, les déclarations financières jusqu'aux produits et projets d'ingénierie, les organes vitaux d'une entreprise résident majoritairement dans les données électroniques, les réseaux informatiques et les ordinateurs portables.

Le DLP se définit comme une solution qui, s'appuyant sur la politique interne de l'entreprise identifie, contrôle et protège l'information stockée, en mouvement et traitée à l'aide d'analyses de contenus approfondies.[22] L'objectif principal poursuivi par les solutions de DLP est de limiter la fuite de données sensibles que celle-ci soit accidentelle ou intentionnelle.

L'utilisation par les entreprises de technologie DLP leur permet ainsi de réduire les risques de fuite de données, de faire des économies, de sécuriser les bases de données internes pour un meilleur respect des politiques de sécurité de l'entreprise afin d'être en conformité avec les textes et règlements encadrant la protection des données.

Grâce à des agents déployés sur le réseau et/ou sur les postes de travail, la copie d'un fichier sur un périphérique externe va pouvoir être empêchée, de même que l'envoi d'un document sensible par email, l'impression d'un document ou encore la publication d'une information confidentielle sur les réseaux sociaux.

Après analyse et filtrage des données par la solution DLP, différentes mesures de prévention peuvent être prises, avec un impact plus ou moins élevé pour l'utilisateur : alertes, demande de justification, blocage…

[22] Claire Bernier et Anne Baudequin ; Plan de Prévention et de Gestion des fuites d'informations, Votre entreprise a-t-elle les bons réflexes et les bonnes procédures ; 2015/1 Volume 52, Pages 25 à 26

Il convient de noter que les acteurs du marché mettent de plus en plus l'accent sur le contexte d'utilisation de la donnée. Certains éditeurs proposent ainsi des fonctionnalités de gouvernance au sein de leur solution de DLP permettant par exemple de savoir exactement où se trouvent les données sensibles et qui y a accès.

Les logiciels de la DLP peuvent être assimilés aux logiciels mis en place dans les centres d'appels pour contrôler l'activité des salariés. Ces logiciels permettent aux superviseurs de tout savoir, en temps réel, des performances des agents : durée de traitement des appels, temps passé entre chacun, taux de concrétisation si le salarié a l'initiative du coup de fil, etc.

La mise en œuvre de la technologie DLP doit s'accompagner d'une sensibilisation des salariés aux politiques de sécurité de l'entreprise. Les collaborateurs étant les plus à mêmes d'occasionner des fuites de données, il est nécessaire qu'ils aient une bonne connaissance des pratiques afin d'éviter les pertes de données au sein de l'entreprise. La mise en œuvre des technologies DLP suppose donc au préalable une information du personnel.

Les technologies DLP contribuent en général pour les employeurs à mettre en œuvre leur obligation de sécurité et de confidentialité au sein de l'entreprise.

Elles ne sont pas les seules mises en œuvre au sein de l'entreprise, elles s'accompagnent bien souvent du contrôle d'accès qui est également une des mesures de sécurité mise en place par l'entreprise afin de limiter les risques de perte de données.

- **Le contrôle d'accès**

L'article L1224-4 du Code du travail dispose : « Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance ». Le Code du travail prévoyait donc déjà une obligation d'information à l'endroit des salariés avant la mise en place de tout dispositif de contrôle d'accès. Le RGPD est venu renforcer cette obligation d'information en mettant à la charge des responsables de traitement le devoir de transparence qui se manifeste par une information claire et précise de toute activité de traitement à l'égard des informations collectées sur une personne.

Plusieurs types de dispositifs peuvent être mis en place pour contrôler l'accès aux locaux, mais en même temps le temps de travail des salariés. Ces dispositifs ne doivent pas être disproportionnés et doivent avoir une finalité précise qui ne doit être autre que celle du contrôle des accès et des horaires des employés.

Suite à l'entrée en application du RGPD, les normes simplifiées qui étaient prises par la CNIL n'ont plus de valeur juridique. Toutefois, la CNIL a décidé de les conserver en attendant la production de nouveaux référentiels basés sur le RGPD.

C'est ainsi que la norme simplifiée NS-042 encadre les traitements mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux des salariés et des visiteurs, la gestion des horaires ainsi que la gestion de la restauration.

La norme ne concerne que les dispositifs contrôlant les entrées et sorties du lieu de travail et ne permet pas le contrôle des déplacements à l'intérieur du lieu de travail à l'exception des zones sensibles identifiées et faisant l'objet d'une restriction de circulation justifiée par des mesures de sécurité.

Les données traitées sont relatives à l'identité, la vie professionnelle, aux badges, aux accès au parking, aux visiteurs, aux heures d'entrée et de sortie et à la gestion de la restauration.

Les données relatives au contrôle du temps de travail ainsi qu'aux motifs d'absence ne doivent pas être conservées plus de cinq (5) ans et les éléments relatifs aux déplacements des personnes sont conservés au maximum trois (3) mois. Les salariés et toutes les personnes concernées doivent être informés de l'existence de tel dispositif conformément au RGPD et à la Loi informatique et libertés modifiée.

Outre les technologies DLP, les centres d'appels et les contrôles d'accès, les employeurs peuvent parfois avoir recours à la biométrie. Une technologie strictement encadrée par les différentes réglementations en matière de protection des données personnelles, notamment le RGPD.

B. La place du RGPD dans l'encadrement juridique de la biométrie sur le lieu de travail

On parle de biométrie lorsque des techniques informatiques sont mises en place pour permettre d'identifier un individu à partir de ses caractéristiques physiques, biologiques, voire génétiques (empreintes digitales, iris, voix, visage ou même la démarche). A titre d'illustration, le contrôle d'accès par reconnaissance de l'empreinte digitale fonctionne de la manière suivante :

- Un échantillon biométrique de référence ou « gabarit » créé à partir de l'image de l'empreinte et ne retenant que les points distinctifs des sillons digitaux est enregistré ;
- Ce gabarit de référence est comparé au doigt posé sur le lecteur biométrique, lors du contrôle d'accès.

La biométrie nécessite une authentification des personnes et est courante dans notre quotidien. Sur nos téléphones aujourd'hui, nous faisons pour la plupart des actions par processus biométrique. Cette technologie est considérée par les employeurs comme étant plus efficace que le contrôle d'accès par badge, qui peut se révéler parfois encombrant et le badge peut également être égaré facilement.

En effet, les données biométriques permettent à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut s'affranchir. Pour autant, et précisément pour ces raisons, leur traitement génère des risques importants pour les droits et les libertés des personnes, dans l'hypothèse où ces données seraient compromises.

Le règlement européen sur la protection des données (RGPD) a consacré le caractère particulier des données biométriques en les qualifiant de « sensibles », au même titre que les données concernant la santé, les opinions politiques ou les convictions

religieuses. Le RGPD en qualifiant les données biométriques de données sensibles vient donc ainsi poser un principe d'interdiction du contrôle par biométrie. Sous certaines conditions, limitativement énumérées par le règlement, le contrôle d'accès par biométrie est toutefois possible et peut être mis en place par les employeurs.

Pour ce faire, avant toute mise en place d'un dispositif de contrôle par biométrie au sein de l'entreprise, il appartiendra à l'employeur de :

- Justifier d'un contexte spécifique rendant nécessaire un niveau de protection élevé, par exemple la manipulation des machines ou produits particulièrement dangereux, l'accès à des fonds ou des objets de valeur, à du matériel ou produits faisant l'objet d'une réglementation spécifique (substances psychotropes et leurs précurseurs, produits chimiques pouvant être utilisés pour la fabrication d'armes, etc.);
- Démontrer l'insuffisance ou l'inadéquation des moyens moins intrusifs tels qu'un badge ou un code d'accès (par exemple, environnement dans lequel une identification forte est nécessaire pour prévenir une usurpation d'identité en cas de vol de badge ou d'interception des codes d'accès).

Le RGPD étant dans une logique de responsabilisation des acteurs, elle insère une conformité dynamique sur le plan du contrôle biométrique. Cette démarche de conformité dynamique oblige les organismes à s'assurer en interne de la licéité de leurs traitements et des conditions de leur mise en œuvre, et veiller plus globalement au respect de l'ensemble des obligations en matière de protection des données. Le RGPD vient ainsi encadrer rigoureusement le recours au dispositif biométrique par les employeurs et ainsi renforcer la protection de la vie privée des salariés.

C'est d'ailleurs l'entrée en vigueur du RGPD qui a amené la Commission Nationale de l'informatique et des libertés à la mise sur pied lors de sa délibération n° 2019-001 du 10 janvier 2019 d'un Règlement type relatif à la mise en œuvre de dispositifs

ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail.[23]

Ce règlement opère une classification des différents types de procédés biométriques et permet ainsi une classification des traitements biométriques en trois types. Il s'agit notamment de :

- Le "type 1" ou gabarit sous maîtrise exclusive de la personne concernée.

Dans le type 1, les supports de stockage des gabarits sont individuels (un support donné ne peut contenir qu'un seul gabarit) et détenus par chaque salarié concerné lui-même (sans qu'aucune copie ne soit conservée par l'employeur ou les prestataires techniques).

Concrètement, il peut s'agir d'une carte ou d'un badge équipés d'une puce sur laquelle le gabarit est stocké. Ce support est remis au salarié qui doit alors le présenter lors du contrôle d'accès en même temps que la caractéristique biométrique enregistrée : le dispositif va alors comparer le gabarit stocké sur ce support à la caractéristique biométrique (iris, empreinte digitale, etc.) présentée au terminal du dispositif.

Le recours à ce type de dispositif permet l'identification et l'authentification des salariés, tout en limitant le risque d'accès non-autorisé à leurs données biométriques : dans la mesure où il n'existe pas de base de données centralisée des gabarits biométriques de l'ensemble des employés, il est impossible de la pirater.

- Le "type 2" ou gabarit sous maîtrise partagée.

Dans ce schéma, une base de données contenant les gabarits de l'ensemble des employés, existe.

Toutefois, ces données sont chiffrées de manière à ce qu'aucune donnée ne puisse être lue et exploitée sans l'intervention de l'individu concernée. Pour cela, chaque

[23] Délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail

individu se voit attribuer un élément personnel (une information, par exemple un code, ou un objet comme par exemple un badge) qui doit être présenté au dispositif au moment de l'authentification.

A supposer qu'une telle base de données soit compromise (par exemple, suite à une attaque externe ou une fuite de données en interne), le risque pour les personnes concernées de voir leurs données biométriques exposées demeurera très faible car les données seront illisibles.

- Le "type 3" ou gabarit sous maîtrise exclusive du responsable de traitement

Dans cette hypothèse, les gabarits de l'ensemble des salariés sont conservés dans une base de données centralisée. Le salarié n'a aucune maîtrise sur le support du stockage, et n'a pas à communiquer au dispositif un secret permettant de déchiffrer le gabarit.

Si cette solution présente certains avantages opérationnels (pas de code à mémoriser ou de badge à porter pour le salarié), ils sont assortis de risques particulièrement importants pour les droits et libertés des salariés.

L'existence d'une base centralisée rend en effet possible une fuite de ces données, fuite qui peut potentiellement exposer de manière irréversible des données biométriques des personnes concernées.[24]

La mise en place par l'employeur d'un dispositif de contrôle par biométrie doit donc répondre aux conditions d'un de ces trois types de traitement, mais également avoir une finalité déterminée comme préconisée par le RGPD, et dans le respect d'une des exceptions limitatives au traitement des données sensibles.

Dans certaines conditions, selon la nature des travaux à accomplir et du risque inhérent à l'activité, le salarié fera l'objet non seulement d'une surveillance médicale spécifique, mais également d'une surveillance de son exposition au risque (surveillance radiologique) donnant lieu à la tenue d'une fiche d'exposition qui porte

[24] Question-réponses sur le règlement type biométrie, disponible en ligne sur le site www.cnil.fr

la trace de cette surveillance. De manière générale, dans le cadre de son devoir de prévention, l'employeur peut être amené à décider de mesures de surveillances destinées notamment à permettre une intervention rapide des secours dans les situations d'urgence. Pour la réalisation de certains travaux, présentant des risques particuliers et graves, le code du travail peut également imposer une étude de sécurité spécifique devant déboucher sur des mesures de sécurité particulières. Tel est le cas pour les travaux sur les ascenseurs, qui doivent être précédés d'une étude sur les risques nés d'une intervention isolée.[25] La surveillance est alors au nombre des mesures de sécurité qui doivent être définies et mises en œuvre.

A ce titre, est admise par la CNIL la protection assurée par un système d'empreintes d'une zone spécifique à l'intérieur d'une installation nucléaire de base ou de certains sites classés SEVESO II. La finalité est de protéger des installations comportant un risque élevé d'explosion ou de diffusion de matières dangereuses ou de détournement de celles-ci par des tiers non autorisés, et d'assurer la protection de personnes exposées à des risques particuliers en raison de ces activités.[26]

Le RGPD a donc une place prépondérante dans la mise en place de la biométrie sur les lieux de travail et permet ainsi de rendre plus claire la frontière entre la vie privée du salarié et sa vie professionnelle.

Hormis ces différents types de moyens de contrôle, les employeurs ont également recours à d'autres moyens de contrôle qui servent non seulement au contrôle des salariés, mais également à la sécurité des biens de l'entreprise ainsi que des produits vendus le cas échéant.

---

25 H. Lanouzière, Prévenir la santé et la sécurité au travail, vol. 2, p. 307, éd. Lamy, 2012

26 Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données.

Section II : LA VIDEO SUR LE LIEU DE TRAVAIL

La grande majorité des entreprises dans le but de protéger les biens et les services qu'elles fournissent à leurs clients, ainsi que la sécurité de leur personnel mettent en place des systèmes de vidéo protection et de vidéosurveillance dans leurs magasins et sur les lieux de travail.

Lorsque le système de surveillance vidéo est installé sur des lieux ouverts au public, il est qualifié de système de vidéo protection et est régi par la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité. Par contre lorsque le système est installé sur des lieux réservés à l'usage du personnel, on le qualifie de système de vidéosurveillance (A).

Dans le cas de la vidéo protection, comme celui de la vidéosurveillance, il y a lieu de respecter un certain nombre de règles afin de ne pas empiéter sur les droits et libertés des personnes. Le RGPD est venu encadrer ces règles existantes pour un meilleur contrôle des systèmes vidéo en entreprise (B).

A. La vidéo protection et la vidéosurveillance mise en œuvre par l'entreprise

L'employeur a depuis plusieurs décennies été autorisé en vertu de son pouvoir de direction sur ses salariés, de mettre en place des dispositifs de contrôle. Il est donc fondé à installer un système de vidéo-protection dans les locaux de l'entreprise. Toutefois, il se doit de respecter les contraintes réglementaires lors du déploiement et de ne pas utiliser le dispositif pour contrôler le salarié à son insu.

Des caméras peuvent ainsi être installées dans les lieux du magasin ouverts au public comme les zones marchandes et les zones de circulation afin d'assurer la sécurité des biens et des personnes. Le système ne doit pas permettre de placer les employés sous surveillance constante (annexe 2), mais pourra permettre de surveiller les employés qui sont en contact direct avec l'argent afin d'éviter les vols. Il doit dans le cas d'un caissier par exemple filmer plus la caisse que le caissier. Toutefois, une autorisation de la préfecture de police doit être demandée avant toute installation sur des lieux ouverts au public.

S'agissant des espaces de travail non ouverts au public, le contrôle des salariés par ce moyen de contrôle est prévu par le Code de la sécurité intérieure en ses articles L251-1 et suivants, ainsi que les articles L1121-1 et L1222-4 du Code de travail qui encadre tous les moyens de contrôle de l'activité des salariés.

L'information ou la consultation du comité d'entreprise est requise avant toute installation de système de vidéo sur le fondement de deux articles spécifiques :

Article L. 2323-13 du Code du travail :

> « Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail. »

Article L. 2323-32, alinéa 3 du Code du travail :

« 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. »

La première étape de la mise en place consiste à informer collectivement les salariés. Conformément à l'article L2323-47 du code du travail, « 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 ».

Toutefois, il est à retenir que l'installation d'un dispositif vidéo destiné à assurer la protection de pièces ou locaux non accessibles aux salariés n'est soumise à aucune condition particulière.

A titre d'exemple, l'employeur est libre de mettre en place des procédés de surveillance des entrepôts ou autres locaux de rangement dans lesquels les salariés ne travaillent pas.[27]

Si un salarié accède malgré tout à un tel local, l'employeur peut se prévaloir des éléments recueillis au moyen de ce système de vidéosurveillance pour établir la preuve des faits reprochés à l'intéressé, comme un vol ou une dégradation de matériel.[28]

Par conséquent, dans cette hypothèse, l'employeur n'a ni à informer ou consulter les représentants du personnel ni à informer les salariés.

[27] Cour de Cassation, Chambre sociale, du 31 janvier 2001, 98-44.290, Publié au bulletin

[28] Cour de cassation, Chambre sociale du 19 avril 2005, 02-46.295

B- La place du RGPD dans l'encadrement juridique du contrôle vidéo en entreprise

Depuis l'entrée en vigueur du RGPD, il n'est plus nécessaire de demander une autorisation à la CNIL avant la mise en œuvre d'un système de contrôle par vidéo.

Le RGPD vient également imposer une information claire et visible faite aux salariés. Ceux-ci doivent être informés, d'abord collectivement par le biais des représentants du personnel, puis ensuite individuellement par tout moyen (note de service, règlement intérieur, intranet) et au moyen d'un panneau affiché de façon visible dans les locaux sous vidéosurveillance :

- De l'existence du dispositif,
- Du nom de son responsable,
- De la base légale du dispositif (dans la quasi-totalité des cas, l'intérêt légitime de l'employeur de sécuriser ses locaux),
- De la durée de conservation des images,
- De la possibilité d'adresser une réclamation à la CNIL,
- De la procédure à suivre pour demander l'accès aux enregistrements visuels les concernant.

Le pouvoir de sanction déjà reconnu à la CNIL le demeure et s'intensifie. C'est sans doute ce qui a amené la CNIL par sa délibération n° SAN-2019-006 du 13 juin 2019 à prononcer à l'encontre de la société UNIONTRAD COMPANY une amende de 20000 euros et l'a enjoint de mettre en conformité son contrôle vidéo avec les dispositions de l'article 32 du règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des données.

La CNIL, après avoir remarqué que la société UNIONTRAID COMPANY mettait sous surveillance constante ses employés, a d'abord décidé de mettre en demeure cette dernière. Malgré cette mise en demeure, la société ne s'est pas conformée aux exigences comme elle le lui a pourtant indiqué.

La CNIL a alors conformément aux pouvoirs qui lui sont conférés en tant qu'autorité locale de protection des données personnelles décidées de mettre à la charge de la société une amende et de rendre publique sa décision.

Par la publicité de sa décision, la CNIL a pour objectif de rappeler la particulière sensibilité de la vidéosurveillance des salariés sur leur lieu de travail. Elle met aussi en avant l'importance de répondre aux mises en demeure de la CNIL. C'est le refus affiché par la société de prendre les mesures pour se mettre en conformité et ce, malgré l'accompagnement de la CNIL vers la conformité dont elle a bénéficié, qui a, en l'espèce, justifié qu'une procédure de sanction soit engagé.

On peut retenir que le RGPD vient encadrer la vidéo en entreprise sur trois axes fondamentaux : les panneaux d'affichage doivent désormais mentionnés des informations plus détaillées qui affiche la durée de conservation des images filmées, mais également fournir les informations aux salariés afin d'exercer leurs droits et en cas de non satisfaction de se plaindre à l'autorité de contrôle qu'est la CNIL.

De même, avec l'entrée en vigueur du RGPD, une analyse d'impact à la vie privée peut être requise en cas de surveillance systématique à grande échelle sur des espaces de travail ouverts au grand public. Cette étude d'impact lorsqu'elle est réalisée par l'employeur lui permet de savoir exactement si le dispositif à mettre en place n'apporte pas de risques considérables pour les droits et libertés des salariés.

Les employeurs peuvent également avoir recours à des services de personnes extérieures à l'entreprise ou mettre en place des moyens de contrôle qui sont extérieurs au périmètre de l'entreprise.

Chapitre II.

Les outils de contrôle extérieurs à l’entreprise

Les employeurs ont de plus en plus recours à des outils et techniques pour la bonne marche du travail au sein de leurs entreprises. Ainsi, chaque année en France, plusieurs milliers d'employés font l'objet d'une surveillance de la part de tiers embauchés par leurs employeurs (Section 1). De plus, certains employeurs ont recours à des dispositifs de géolocalisation soit des véhicules mis à la disposition de leurs salariés, soit des téléphones (Section2), ce qui leur permet de faire des économies et en même temps de contrôler l'activité de leurs salariés.

Section 1 : Le recours aux services des tiers

Les employeurs peuvent parfois avoir recours à des détectives privés (A) pour contrôler l'activité de leurs salariés en dehors des locaux de l'entreprise. Ce recours à des détectives privés est encadré par les textes et le RGPD est venu y apporter également une touche afin de renforcer le respect de la vie privée des salariés (B).

A- Le recours aux services d'un détective privé

Lorsque l'employeur soupçonne son salarié d'avoir un comportement déloyal, comme par exemple travailler pour un autre employeur ou à son propre compte durant son temps de travail, il peut être tenté d'avoir recours à un détective privé afin de constituer une preuve en cas de litige.

En effet, des salariés sont parfois amenés à faire un usage abusif des arrêts maladie ou même ont des absences fantaisistes afin d'offrir leurs services à une autre société et ou même d'effectuer des activités en tant qu'autoentrepreneur à leurs heures réglementaires de travail.

Mais ni la loi ni la jurisprudence ne rendent la surveillance par le recours à un détective privé facile pour l'employeur.

La règle de base, s'agissant de la surveillance du salarié est le fait que le salarié doit avoir été préalablement informé et averti des moyens qui peuvent être mis en œuvre pour le contrôler.

Ainsi, la validité et la loyauté d'une filature par un détective privé ne sont admises que si le salarié a été préalablement averti qu'un tel moyen pouvait être mis en œuvre à son encontre[29].

La surveillance doit également être limitée au temps de travail du salarié uniquement et ne doit pas s'étendre en dehors de ses heures réglementaires.

Sur le principe, la surveillance n'est pas illégale mais très encadrée et du coup très limitée. Rajoutons que pour toute enquête de détective privé, les moyens déployés pour surveiller un salarié doivent être proportionnés aux intérêts légitimes du demandeur.

Si la surveillance par détective privé peut éventuellement permettre d'obtenir des informations, l'utilisation de ces informations comme mode preuve est, dans les faits, difficile. Toutefois, le constat d'huissier effectué dans certaines conditions, même initié par une filature d'un détective privé, constitue un moyen de preuve licite.

L'employeur a donc la possibilité de procéder à une filature, puis par la suite de faire intervenir un huissier pour constater les infractions identifiées par le détective privé.

Même si devant un Tribunal de Prud'hommes il apparaît difficile voire presque impossible pour l'employeur d'utiliser les preuves issues de filatures, il pourra tout de même les faire valoir sur la base de l'article 1240 du Code Civil afin d'obtenir réparation du préjudice subi des faits commis par son salarié.

La Cour de Cassation a d'ailleurs dans un arrêt du 26 Septembre 2018 rejeté le moyen soulevé par l'employeur pour justifier la mise en place de la filature de son employé ;

La Cour de Cassation confirme ainsi la décision des juges d'appel en affirmant qu' « attendu qu'ayant constaté que l'employeur avait fait suivre le salarié par une

29 Cour de Cassation, Chambre sociale, du 4 février 1998, 95-43.421, Publié au bulletin

agence de détective privé pendant plusieurs heures, la cour d'appel a exactement décidé que ce procédé était attentatoire à la vie privée du salarié et a caractérisé un comportement déloyal de l'employeur ; »[30].

Les juges ont donc le pouvoir souverain de déterminer si oui ou non la preuve obtenue grâce au service d'un détective privé même en l'absence de son information préalable porte atteinte ou non à la vie privée du salarié. Il y a donc ici une mise en balance de l'intérêt de l'employeur face au droit au respect de la vie privée du salarié.

[30] Cour de cassation, civile, Chambre sociale, 26 septembre 2018, 17-16.020

B- L'encadrement juridique du recours au contrôle en dehors de l'entreprise et les apports du RGPD

Les moyens mis en œuvre pour le contrôle des salariés en dehors des locaux de l'entreprise doivent être proportionnels au but recherché. Ainsi, la durée de l'intervention notamment devra être maitrisée, une durée trop longue pouvant rendre la filature irrecevable.

La première chambre civile de la Cour de Cassation dans une décision en date du 25 février 2016 affirmait : « Attendu que le droit à la preuve ne peut justifier la production d'éléments portant atteinte à la vie privée qu'à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit proportionnée au but poursuivi. »[31], vient ainsi concrétiser le principe de proportionnalité applicable entre autres au recours au service d'un détective privé.

Par cette affirmation, la Cour vient sans doute attirer l'attention des employeurs sur le fait qu'ils ne peuvent, au nom de leur pouvoir de direction s'incruster dans l'espace privé du salarié par tout moyen à leur convenance afin de pouvoir contrôler sa bonne exécution du travail ou sa loyauté envers son employeur.

Concernant le respect à la vie privée, plusieurs fondamentaux sont à respecter concernant la surveillance d'un salarié.

Les investigations doivent être cantonnées aux horaires et jours de travail du salarié.

La captation d'image n'est autorisée que dans les lieux publics.

Avec l'entrée en vigueur du RGPD, l'accent est mis sur l'information des salariés. L'employeur est désormais dans une logique de responsabilisation qui doit l'amener à vérifier que les moyens de contrôle externes qu'il souhaite mettre en place sont bien proportionnés à la finalité recherchée avant de les déployer. De plus, si l'entreprise dispose d'un Délégué à la Protection des Données (DPD en Anglais

[31] Cour de cassation, civile, Chambre civile 1, 25 février 2016, 15-12.403, Publié au bulletin

DPO)[32], l'employeur doit procéder à la mise en œuvre des moyens de contrôle externe en étroite collaboration avec celui-ci.

Ce même encadrement est applicable aux systèmes de géolocalisation mis en place par l'employeur.

[32] DPO pour Data Protection Officer

Section 2 : La géolocalisation des salariés

De plus en plus mise en œuvre par les employeurs, car ne nécessitant pas d'énormes coûts financiers, elle peut être axée sur les véhicules et les ordiphones mis à la disposition des salariés (A) ; Pour ce faire, la CNIL a posé des principes légaux afin de garantir le respect de la vie privée des salariés (B).

A- La géolocalisation des véhicules et des ordiphones des salariés

L'employeur peut recourir à des dispositifs de géolocalisation des véhicules mis à la disposition de ses salariés ou même des ordiphones mis à leur disposition.

Rappelons que la géolocalisation est une technique permettant ici à l'employeur de prendre connaissance de la position géographique des employés, à un instant donné ou en continu, grâce à la localisation des véhicules ou des téléphones portables mis à leur disposition pour leur mission.

La Cour de Cassation dans un arrêt du 3 Novembre 2011[33] a estimé que la géolocalisation ne peut s'appliquer aux véhicules des salariés qui ont une indépendance dans l'organisation de leur temps de travail.

En l'espèce, il s'agissait d'un employeur qui avait installé un dispositif de géolocalisation sur le véhicule de l'un de ses vendeurs qui disposait d'une liberté dans l'organisation de ses déplacements. L'employeur s'est servi du dispositif pour suivre le temps de travail de son salarié et calculer sa rémunération, puis a procédé à son licenciement pour non-respect de ses horaires de travail. Le salarié a alors pris acte de la rupture de son contrat de travail par son employeur, puis c'est porté devant les juridictions compétentes pour se voir rétablir dans ses droits. Condamné par la Cour d'Appel de Paris pour licenciement sans cause réelle et sérieuse, l'employeur a saisi la Cour de Cassation.

[33]Cour de cassation, civile, Chambre sociale, 3 novembre 2011, 10-18.036

La chambre sociale de la Cour de Cassation a confirmé cette décision le 3 novembre 2011, dans un arrêt qui servira de jurisprudence sur les questions relatives à la géolocalisation des véhicules de salariés.

La Cour de Cassation rejoint ainsi la CNIL en considérant que : « l'utilisation d'un système de géolocalisation pour assurer le contrôle de la durée du travail, laquelle n'est licite que lorsque ce contrôle ne peut pas être fait par un autre moyen, n'est pas justifiée lorsque le salarié dispose d'une liberté dans l'organisation de son travail ». Elle a également constaté "qu'un système de géolocalisation ne peut être utilisé par l'employeur pour d'autres finalités que celles qui ont été déclarées auprès de la Commission nationale de l'informatique et des libertés, et portées à la connaissance des salariés".

Or, le salarié avait été informé que le dispositif était mis en place pour analyser les temps nécessaires à ses déplacements pour une meilleure optimisation des visites effectuées. Cette utilisation du dispositif de géolocalisation étant illicite, la rupture du contrat de travail aux torts de l'employeur était justifiée selon la Cour.

L'entrée en vigueur du RGPD ayant conduit à un abandon de la procédure de déclaration au profit de la responsabilisation des acteurs, l'employeur se doit désormais de tenir un registre des activités de traitement indiquant dans quel but il met en place des dispositifs de géolocalisation et il se doit d'associer le DPO avant tout déploiement de dispositif de contrôle s'il l'a désigné au sein de son entreprise.

Par ailleurs, l'employeur a l'obligation de s'assurer que le dispositif remplit les règles de sécurité adéquate en vue d'éviter une perte ou un vol des données de ses salariés enregistrés par ce dispositif. L'accès aux informations du dispositif de géolocalisation doit être limité au personnel habilité des services concernés, à l'employeur et au personnel habilité d'un client ou donneur d'ordre auprès duquel une prestation est justifiée. Le salarié dispose également d'un droit d'accès sur les données de géolocalisation du véhicule mis à sa disposition.

La CNIL veille à ce que la mise en place par l'employeur d'un contrôle par géolocalisation des salariés ne porte pas entrave à leur vie privée.

B- Les conditions légales de géolocalisation posées par la CNIL

La Commission Nationale de l'Informatique et des Libertés énumère les conditions dans lesquelles l'employeur peut mettre en place un système de géolocalisation des véhicules de ses salariés.

Des dispositifs de géolocalisation peuvent être installés dans des véhicules utilisés par des employés pour :

- « Suivre, justifier et facturer une prestation de transport de personnes, de marchandises ou de services directement liée à l'utilisation du véhicule. Par exemple : les ambulances dans le cadre de la dématérialisation de la facturation de l'assurance maladie.
- Assurer la sécurité de l'employé, des marchandises ou des véhicules dont il a la charge, et notamment retrouver le véhicule en cas de vol (par exemple, avec un dispositif inerte activable à distance à compter du signalement du vol).
- Mieux allouer des moyens pour des prestations à accomplir en des lieux dispersés, notamment pour des interventions d'urgence. Par exemple : identifier l'employé le plus proche d'une panne d'ascenseur ou l'ambulance la plus proche d'un lieu d'accident.
- Accessoirement, suivre le temps de travail, lorsque cela ne peut être réalisé par un autre moyen.
- Respecter une obligation légale ou réglementaire imposant la mise en œuvre d'un dispositif de géolocalisation en raison du type de transport ou de la nature des biens transportés.
- Contrôler le respect des règles d'utilisation du véhicule. »

En ce qui concerne les entreprises, l'utilisation d'outils de géolocalisation des véhicules utilisés par les salariés pour l'accomplissement de leur mission est régie en France par la norme simplifiée n° NS-051 élaborée par la CNIL en attendant l'élaboration d'une nouvelle norme basée sur les prescriptions du RGPD.

Celle-ci fixe le cadre de conformité applicable, sur la base duquel la CNIL considère que le dispositif ne porte pas atteinte à la vie privée ou aux libertés.

La CNIL précise aussitôt que « le traitement peut avoir pour finalité accessoire le suivi du temps de travail, lorsque ce suivi ne peut être réalisé par un autre moyen, sous réserve notamment de ne pas collecter ou traiter de données de localisation en dehors du temps de travail des employés concernés ». Elle renvoie ainsi au principe de minimisation de données évoquées par l'article 3 du RGPD.

Compte tenu du renforcement de la responsabilisation et par ricochet de la responsabilité des acteurs, le RGPD ne peut que conduire à ce que la jurisprudence continue de faire preuve de sévérité, d'autant que la protection des personnes à l'égard du traitement de données personnelles les concernant est érigée en « droit fondamental » par le Code Civil.

PARTIE II.

LE RENFORCEMENT PAR LE RGPD DU CADRE JURIDIQUE EXISTANT

La porosité accrue de la frontière entre vie professionnelle et vie privé et le développement des technologies de contrôle et de surveillance au travail (caméras, logiciels, localisation, réseaux, etc.) justifient l'inquiétude des employés. La majeure partie des entreprises mettent en place des moyens de contrôle de l'activité de leurs salariés et parfois au détriment du respect de la vie privée.

En ce sens, le RGPD, qui s'applique aux entreprises, associations, collectivités territoriales et administrations, est venu responsabiliser les acteurs et mieux protéger les individus.

Le contrat conclu, il n'est pas de moment où son exécution échappe aux technologies numériques, que ce soit de manière modeste ou aussi fort que la défaillance du matériel informatique peut venir empêcher l'exécution normale de la tâche à accomplir. De même, les moyens de contrôle mis en œuvre au sein de l'entreprise en arrivent à fonder la preuve d'une rupture du contrat de travail.

L'entrée en vigueur du RGPD s'est intéressée à la question et de procéder à un encadrement rigoureux de ses moyens de contrôle. Ainsi, l'article 88 du RGPD dispose en son alinéa 1 : «Les États membres peuvent prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail, aux fins, notamment, du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, de la protection des biens appartenant à l'employeur ou au client, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail… »

Le RGPD vient ainsi prendre en compte les différents moyens de contrôle des salariés pouvant être déployés dans le cadre du contrat de travail.

Pour ce faire, elle s'intéresse au cadre juridique existant en vue de conduire à la stabilisation des règles juridiques déjà mises en place (Chapitre 1). Les différentes évolutions technologiques et leurs répercussions sur les relations de travail amènent à repenser le droit social afin de l'adapter (Chapitre 2).

Chapitre I.

Le contrôle des salariés en entreprise : un cadre juridique non encore stabilisé

Antérieurement à l'entrée en vigueur du RGPD, le 25 mai 2018, l'employeur, en tant que responsable du traitement des données de ses salariés, devait effectuer des formalités spécifiques auprès de la CNIL, préalablement à toute opération effectuée sur des données à caractère personnel.

Dans ce contexte, la CNIL avait élaboré des autorisations uniques, qui permettaient de standardiser les déclarations pour les traitements courants.

Depuis le 25 mai 2018, le choc de simplification opéré par le RGPD a remplacé de telles déclarations préalables par un « principe de responsabilité ». En conséquence, l'employeur qui souhaite installer un système de géolocalisation de ses salariés pour contrôler la durée de leur temps de travail par exemple n'a plus à se rapprocher de la CNIL pour déclencher le traitement des données à caractère personnel de ses salariés ou mettre en œuvre des moyens de contrôle de leur activité.

La responsabilité des moyens de contrôle mis en place est laissée à la charge des employeurs et est encadrée par un certain nombre de textes mis en vigueur et sous le contrôle des différentes juridictions ainsi que de la CNIL qui représente l'autorité de contrôle pour la FRANCE. Ces différents textes servent donc ensemble à l'interprétation et au règlement des litiges pouvant naître du contrôle de l'activité des salariés.

Ainsi on remarque une cohabitation des référentiels CNIL face au RGPD (Section 1). Ces différents textes se doivent pour une meilleure efficacité du contrôle d'être pris en compte par le RGPD afin d'aboutir à un cadre unique stable (Section 2).

Section 1 : La coexistence des référentiels CNIL face au RGPD

L'entrée en vigueur du RGPD a fait perdre aux autorisations uniques et règlements types leur valeur juridique. Toutefois, face à l'absence de prise de référentiels conformes au RGPD, la CNIL a décidé en France de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mises en conformité.

Ainsi, on assiste à un maintien provisoire des référentiels CNIL qui permettent d'orienter les actions de mise en conformité des dispositifs au RGPD (A). Il apparaît toutefois primordial de penser à une refonte de ses référentiels afin d'aboutir à un cadre juridique du contrôle des salariés en entreprise plus stable (B).

A- Le maintien provisoire des référentiels CNIL face au RGPD

Les référentiels CNIL existants avant l'entrée en vigueur du RGPD dans le cadre de l'encadrement des moyens de contrôle de l'activité des salariés demeurent applicables afin de faciliter la tâche aux responsables de traitement dans le cadre de leur action de mise en conformité.

La norme simplifiée n° 46 qui concerne la gestion des ressources humaines par exemple reste applicable. Cette norme a pour finalité la gestion administrative des personnels (dossier professionnel, annuaires, élections professionnelles…) ; la mise à disposition d'outils informatiques (suivi et maintenance des matériels, annuaires informatiques, messagerie électronique, intranet…) ; l'organisation du travail (agendas professionnels, gestion des tâches) ; la gestion des carrières (évaluation, validation des acquis, mobilité…) ; la formation des personnels.[34]

Les destinataires des données sont : les personnes habilitées chargées de la gestion du personnel ; les supérieurs hiérarchiques des salariés ; les instances représentatives du

[34] Norme simplifiée n° 46 : Délibération n°2005-002 du 13 janvier 2005 portant adoption d'une norme destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organismes publics et privés pour la gestion de leurs personnels.

personnel et les délégués syndicaux. Les données peuvent, sous certaines conditions, être transmises vers un pays situé hors de l'union européenne. Les données doivent être supprimées après le départ de la personne concernée. Cette norme continue à être mise en œuvre en se conformant aux conditions du RGPD et de la Loi Informatique et Libertés modifiée.

Cette norme simplifiée permet d'ailleurs le contrôle de l'accès à internet et de la boîte mail des salariés.

La Cour de cassation a affirmé, dans un arrêt du 2 octobre 2001 dénommé arrêt « Nikon », qu'un employeur ne saurait prendre connaissance de messages personnels d'un employé sans porter atteinte à la vie privée de celui-ci (article 9 du code civil) et au principe du secret des correspondances (article 226-15 du code pénal), quand bien même une utilisation à des fins privées aurait été proscrite par l'employeur.

Pour autant, le principe du secret des correspondances connaît des limites dans la sphère professionnelle. Il peut également être levé dans le cadre d'une instruction pénale ou par une décision de justice. De plus, La Cour de Cassation dans un arrêt du 30 mai 2007 a jugé que tout courriel envoyé de la boîte mail professionnel est réputé avoir un caractère professionnel sauf pour le salarié à l'identifier formellement comme personnel.

Le contrôle de la boîte mail ou de l'utilisation d'internet du salarié est donc librement accessible à l'employeur, qui se doit de respecter les obligations édictées par la NS-046.

Depuis l'entrée en vigueur du RGPD, la mise en place de tout dispositif de contrôle de l'activité des salariés doit également respecter les prescriptions du RGPD, c'est-à-dire avoir une finalité définie prévue par les textes en vigueur. Ainsi l'employeur est libre de mettre en œuvre les dispositifs de contrôle sur la base des prescriptions du Code de travail, des différents référentiels mis en œuvre par la CNIL, ainsi que du RGPD. Il devra sur la base de ce dernier pouvoir rapporter la preuve de sa conformité en cas de contrôle de l'autorité.

Ces différents textes encadrant les dispositifs de contrôle de l'activité des salariés doivent être repris sur la base du RGPD afin de mettre en place un cadre unique et clair pour un encadrement plus efficace du contrôle du salarié.

B- La nécessité d'une refonte des référentiels existants pour se conformer au RGPD

Le pouvoir de direction accordé à l'employeur par le Code du travail lui accorde la possibilité de surveiller et de contrôler l'activité de ses salariés pendant le temps de travail.[35] L'arrivée du RGPD a entraîné des changements dans la mise en œuvre des moyens de contrôle des salariés.

Les textes existants doivent donc prendre en considération les exigences du RGPD afin de mieux veiller à la protection de la vie privée des salariés.

Pour encadrer les moyens de contrôle, la CNIL se base aujourd'hui sur les textes existants ainsi que les dispositions du RGPD afin de rendre des avis lorsque ces moyens de contrôle portent atteinte à la vie privée des salariés.

La CNIL déjà avant l'entrée en vigueur du RGPD se basait sur les dispositions de la loi informatique et libertés pour décider de la légalité ou non d'un dispositif de contrôle des salariés mis en place au sein d'une entreprise.

Ainsi, la CNIL avait décidé de suspendre le système vidéo installé au sein d'une entreprise bien qu'étant conforme aux dispositions du Code du travail, mais n'ayant pas fait l'objet d'une déclaration préalable.[36]

L'entrée en vigueur du RGPD est venue supprimer le système de la déclaration préalable sauf dans les cas rares de données de santé.

Il serait donc opportun pour le législateur de travailler à l'adaptation de toutes les normes simplifiées existantes comme c'est le cas avec le projet de référentiel relatif aux traitements de données à caractère personnel mis en œuvre par des organismes privés ou publics aux fins de gestion du personnel[37] ainsi que le projet de référentiel

[35] Cour de Cassation, Chambre sociale, du 14 mars 2000, 98-42.090, Publié au bulletin

[36] Délibération n°2010-112 du 22 avril 2010 de la formation restreinte décidant l'interruption d'un traitement mis en œuvre par la Société X…

[37] CNIL, Projet de référentiel relatif aux traitements de données à caractère personnel mis en œuvre par des organismes privés ou publics aux fins de gestion du personnel

relatif aux traitements de donnée à caractère personnel destinés à la mise en œuvre d'un dispositif d'alerte.[38]

La mise en œuvre des moyens de contrôle des salariés en ressortira plus efficace, avec une frontière mieux établie entre vie professionnelle et vie privée du salarié.

[38] CNIL, Projet de référentiel relatif aux traitements de donnée à caractère personnel destinés à la mise en œuvre d'un dispositif d'alerte

Section 2 : La vulnérabilité des salariés face aux moyens de contrôle mis en place

Le RGPD est venu non seulement modifier la procédure de mise en œuvre des moyens de contrôle des salariés, mais il a également reconnu ensemble avec le G29 la qualité de personnes vulnérables aux salariés (A). Il est venu par ailleurs renforcer l'obligation d'information due par l'employeur avant toute mise en place de moyens de contrôle, ainsi qu'un droit d'accès qui se trouve limité pour le salarié (B).

A- La soumission du traitement des données des salariés à l'Analyse d'impact

Les données gérées par les employeurs peuvent contenir des informations sensibles sur les employés, telles que leur origine ethnique, des données médicales ou encore un passé criminel. Les employeurs doivent donc se conformer aux restrictions et protections particulières, présentées par le RGPD lors du traitement des données de leurs salariés qui sont des données réputées sensibles.

De plus, le traitement des données des salariés eu égard au lien de subordination qu'ils ont avec leur employeur, ne jouit pas de certaines prérogatives et les employés peuvent se retrouver contraints d'accepter un tel traitement de données. C'est pour toutes ces raisons que le RGPD et le G29 classent les salariés dans la catégorie des personnes vulnérables.[39]

Pour ce faire, les lignes directrices du G29 et le RGPD imposent une analyse d'impact à la protection des données (AIPD, PIA en Anglais) pour les données RH.

L'AIPD permet de répondre à l'approche par les risques du RGPD. Conformément à cette approche, il n'est pas obligatoire d'effectuer une AIPD pour chaque opération de traitement. Une AIPD n'est requise que lorsque le traitement est «susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques».[40]

[39] Article 37 du Règlement Général pour la Protection des données

[40] Article 35, paragraphe 1 du Règlement Général pour la Protection des Données

Un « risque » rappelons-le est un scénario qui décrit un événement et ses effets, estimés en termes de gravité et de probabilité. La «gestion du risque» peut, quant à elle, se définir comme un ensemble d'activités coordonnées dans le but de diriger et de piloter un organisme vis-à-vis du risque.[41]

L'AIPD se décompose en trois parties :

° Une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels

° L'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quels que soient les risques ;

° L'étude, de nature plus technique, des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.

Ainsi, une analyse d'impact à la protection des données réalisée conformément aux prescriptions du RGPD permet d'identifier les principaux risques pour les droits et libertés des personnes et de savoir si le traitement peut être mis en œuvre ou pas.

Un « risque sur la vie privée » est selon la CNIL un scénario décrivant :

« Un événement redouté (atteinte à la confidentialité, la disponibilité ou l'intégrité des données, et ses impacts potentiels sur les droits et libertés des personnes) ;

Toutes les menaces qui permettraient qu'il survienne. »

En outre, les lignes directrices du G29[42] relèvent 9 critères nécessitant une étude d'impact. Le Groupe de travail retient que lorsqu'un traitement est compatible avec deux critères de cette liste, une analyse d'impact à la protection des données est requise.

---

[41] Définition du groupe de travail de l'article 29 figurant dans les lignes directrices sur l'analyse d'impact relative à la protection des données

[42] Le G29 réunissait l'ensemble des Cnil européennes. Il a été remplacé par l'EDPB (Comité européen à la protection des données) depuis le RGPD

Il s'agit notamment des critères suivants :

« – évaluation/scoring (y compris le profilage) ;

– décision automatique avec effet légal ou similaire ;

– surveillance systématique ;

– collecte de données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques ou de santé, données biométriques et données concernant la vie ou l'orientation sexuelle) ;

– collecte de données à caractère hautement personnel (données relatives à des communications électroniques, données de localisation, données financières…) ;

– croisement de données ;

– collecte de données personnelles à large échelle ;

– personnes vulnérables (patients, personnes âgées, enfants, **salariés**…) ;

– usage innovant (utilisation d'une nouvelle technologie) ;

– exclusion du bénéfice d'un droit/contrat. »

La CNIL dans une délibération du 11 Octobre 2018 a d'ailleurs précisé les traitements pour lesquels une AIPD est requise.

Au nombre de ces opérations de traitement, on a les traitements établissant des profils de personnes physiques à des fins de gestion des ressources humaines, les traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés et les traitements ayant pour finalité la gestion des alertes et des signalements en matière sociale et sanitaire.

C'est dire à quel point la CNIL considère les salariés comme des personnes vulnérables auxquelles il est important d'accorder une protection particulière sur leur vie privée.

Ce n'est qu'à la suite de l'AIPD que l'employeur pourra décider si oui ou non il a la possibilité de mettre en œuvre le dispositif de contrôle ou pas.

Lorsque le dispositif à mettre en place présente donc des risques importants pour les droits et libertés des salariés, ou pourrait porter un coup à leur intérêt juridique, l'employeur doit se résoudre à ne pas les mettre en place ou dans le pire des cas il devrait renforcer les moyens de protection de la vie privée de ses salariés avant de penser à les mettre en place.

B- Le renforcement de l'obligation d'information par le RGPD et les limites au droit d'accès du salarié

L'employeur avant toute mise en œuvre de moyens de contrôle des salariés au sein de l'entreprise doit satisfaire avec le RGPD à la même obligation d'information que dans le cadre d'un traitement de donnée à caractère personnel usuel.

Cette obligation d'information s'effectue pour l'employeur à un double niveau. Il doit d'abord informer les instances représentatives du personnel avant d'utiliser des techniques d'aide au recrutement ou de gestion du personnel par exemple.[43]

Par ailleurs, Candidats comme employés doivent être informés :

• de l'identité du responsable du fichier (cabinet de recrutement ou service des ressources humaines) : le responsable du fichier est ici assimilable au responsable de traitement, c'est-à-dire la personne physique ou morale en charge des interactions avec le fichier, en général le propriétaire du fichier

• de l'objectif poursuivi (gestion des candidatures ou gestion du personnel), l'objectif est assimilable à la finalité. Il faut se poser ici les bonnes questions. Par exemple se demander pourquoi ai-je besoin de mettre ces outils en place ? Pourquoi un dispositif biométrique et pas simplement un accès par badge ? La réponse à ces questions permet une mise en œuvre conforme des moyens de contrôle.

• de la base légale du dispositif (obligation légale issue du code du travail par exemple, ou intérêt légitime de l'employeur), La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre, ce qui donne le droit à un organisme de traiter des données à caractère personnel. On peut également parler de « fondement juridique » ou de « base juridique » du traitement.[44]

[43] Travail et données personnelles, Le recrutement et la gestion du Personnel

[44] Définition de la base légale, disponible sur https://www.cnil.fr/fr/definition/base-legale

• du caractère obligatoire ou facultatif des réponses ainsi que des conséquences à leur égard d'un défaut de réponse,

• des destinataires des informations (autres cabinets de recrutements, par exemple),

• de la durée de conservation des données, elle doit être définie ou il doit exister des indications qui permettent de l'identifier.

• des conditions d'exercice de leurs droits d'opposition (pour motif légitime), d'accès et de rectification, les salariés doivent être informés des droits dont ils disposent sur les données recueillies par les dispositifs de contrôle mis en place.

• de la possibilité d'introduire une réclamation auprès de la CNIL. Les salariés doivent obligatoirement être informés de ce qu'ils disposent de la possibilité s'ils ne sont pas satisfaits avec la réponse à eux apportée quand ils décident de mettre en œuvre les droits conférés sur leurs données de recourir à l'autorité de contrôle pour une réponse plus satisfaisante.

Aucune information concernant un employé ne peut donc être collectée par un dispositif qui n'a pas été préalablement porté à sa connaissance.

Par ailleurs, le RGPD accorde au salarié un droit d'accès sur les données (sur simple demande et sans avoir à la motiver, un candidat ou un employé peut obtenir une copie des données qui le concernent c'est-à-dire les données sur son recrutement, l'historique de sa carrière, ses données de rémunération, l'évaluation des compétences, un dossier disciplinaire…).

Le problème se pose quant à l'accès du salarié aux courriels de sa boîte mail professionnelle. Les courriels dans la boîte mail du salarié s'ils sont supposés être une expertise apportée sur une question relative à l'entreprise, devraient être considérés comme des données de l'employeur. Le salarié en cessation de travail ou en interruption de contrat ne devrait donc pas pouvoir demander un accès à sa boîte mail. Cela pourrait constituer une limite au droit d'accès reconnu au salarié par le RGPD.

Le RGPD est ainsi dès sa mise en œuvre venu procéder aux renforcements des outils juridiques existants dans le cadre de l'encadrement des moyens de contrôle mis en place avant son arrivée.

Il permet également de faire prendre conscience aux employeurs des abus pouvant découler de la mise en place des dispositifs trop intrusifs dans la vie privée de leurs salariés et les responsabilisent donc davantage pour un meilleur encadrement du contrôle.

C'est dans cette optique qu'il apparaît nécessaire de travailler à une adaptation du droit social aux évolutions technologiques. Cela constituera sans doute la clé d'un mieux-être des salariés en entreprise et installera un climat de confiance pour un contrôle mieux orienté et moins intrusif.

Chapitre II.

L'ADAPTATION DU DROIT SOCIAL AUX EXIGENCES DU RGPD ET AUX EVOLUTIONS TECHNOLOGIQUES

L'évolution des technologies numériques, ainsi que celle des différentes législations relatives à la protection des données apportent de profonds bouleversements dans les relations de travail.

Depuis une décennie, le processus organisationnel et les structures d'entreprises ont considérablement évolué avec la mise en place des technologies numériques et en particulier d'internet.[45]

Les salariés travaillant dans des entreprises ayant adopté une technologie TIC, notamment un ERP[46] ou des outils de traçabilité, déclarent plus souvent que leur rythme de travail est imposé par des cadences machiniques.[47]

Les technologies numériques sont toutefois on ne peut le nier bénéfique pour la rapidité du travail au sein de l'entreprise.

Les avantages qu'elles procurent sont souvent mis en avant pour justifier l'adoption et le déploiement de ces outils dans le contexte du travail : une amélioration des capacités de communication, de coordination et de collaboration; une possibilité renforcée d'accès aux décideurs, une meilleure réactivité et une plus grande autonomie dans les décisions.[48]

Mais ces avantages sont susceptibles d'être relayés au second rang par des inconvénients décrits comme potentiellement liés à l'usage de ces technologies : l'absence de frontière entre travail non-travail, la discontinuité des activités, le culte de l'urgence, l'absence de réflexion dans les décisions, la surcharge informationnelle, le contrôle renforcé des activités.[49]

---

[45] Charles-Henri Besseyre Des Horts et Henri Isaac, L'IMPACT DES TIC MOBILES SUR LES ACTIVITÉS DES PROFESSIONNELS EN ENTREPRISE, P 243

[46] Un ERP (Enterprise Resource Planning) ou également appelé PGI (Progiciel de Gestion Intégré) est un système d'information qui permet de gérer et suivre au quotidien, l'ensemble des informations et des services opérationnels d'une entreprise.

[47] Impact des TIC sur les conditions de travail, P 105

[48] Isaac H., Kalika M., Campoy E., « Contribution des technologies de l'information à la perception de l'urgence et de la surcharge informationnelle chez les salariés français : une analyse longitudinale », Communication Colloque e-GRH, AIM-AGRH, université Paris-Dauphine, mai 2006.

[49] Jarvenpaa S.L., Lang K.L., "Managing the paradoxes of mobile technology", Information Systems Management, Fall 2005, p. 7-23.

Il est donc important que les instruments juridiques actuels en matière de protection sociale tiennent compte des nouvelles formes de travail (Section 1), afin que l'humain puisse retrouver sa place de choix au sein de l'entreprise pour un meilleur rendement (Section 2).

Section 1 : La nécessité d'une adéquation des instruments juridiques aux nouvelles formes de travail

La pyramide mise en œuvre par MASLOW[50] (Annexe 1), sur la théorie des besoins de l'employé nous permet de comprendre dans quel ordre d'importance un employé peut être motivé en fonctions de ses besoins. L'idée est qu'on ne peut agir sur les motivations "supérieures" d'une personne qu'à la condition expresse que ses motivations primaires (besoins physiologiques et de sécurité) soient satisfaites.

Maslow indique dans sa classification des besoins que les hommes cherchent la satisfaction de leurs besoins par niveau.

Dès que l'homme sent ses besoins d'un niveau satisfait, il passe au niveau suivant. Ainsi, dans l'ordre de satisfaction des besoins des salariés, il existe un besoin de se sentir en confiance dans l'entreprise et de sentir que son employeur lui fait confiance.

C'est ainsi que de plus en plus les employeurs mettent en œuvre le travail à distance. Cela permet au salarié de s'épanouir davantage, mais quelques fois, le salarié peut se sentir étouffer, stresser et voir la frontière disparaître entre sa vie privée et sa vie professionnelle.

C'est la raison pour laquelle il s'avère important de procéder à un encadrement du travail à distance, mais aussi de mettre en place un droit à la déconnexion pour l'employé pour un meilleur rendement au sein de l'entreprise, le tout en adéquation avec les évolutions technologiques et législatives.

Cette adéquation des instruments juridiques passe par un encadrement du télétravail et du droit à la déconnexion (A), conformes au RGPD puis par une meilleure prise en compte de la place de l'humain au sein de l'entreprise(B).

50 Abraham Harold Maslow, Psychologue Américain, 1er Avril 1908-8 Juin 1970

A- L'encadrement du télétravail et la nécessité de sa mise en conformité au RGPD

Le télétravail rappelons-le est selon la définition de l'accord national interprofessionnel du 19 juillet 2005 « 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 pu être réalisé dans les locaux de l'employeur, est effectué hors de ces locaux de façon régulière ».[51] Il s'agit d'une forme d'organisation du travail basée sur les technologies de l'information et de la communication (TIC).

Le salarié peut donc travailler :

° soit chez lui,

° soit dans un télécentre.[52]

Conçu au départ comme un moyen de réduire les temps de transport ou les coûts immobiliers de l'entreprise, le télétravail semble devenir un mode d'organisation du travail flexible associé à une meilleure ergonomie temporelle pour les salariés.[53]

Certaines recherches sur le télétravail se sont concentrées sur la caractérisation de cette pratique : elles ont conduit à étudier la prévalence ou non de cette pratique sur les lieux de travail, les caractéristiques individuelles des télétravailleurs, les effets du télétravail, et plus récemment les raisons pour lesquelles il est mis en œuvre.[54]

On retient que le télétravailleur est confronté à un paradoxe : le télétravail est censé permettre de renforcer l'autonomie et réduire les conflits entre le travail et la vie

---

[51] https://www.anact.fr/accord-national-interprofessionnel-du-19-juillet-2005-relatif-au-teletravail - consulté le 8-7-107 – citation article 1 p.92.

[52] En général lorsque son domicile est très loin de son entreprise

[53] Aubert N., Gruère J. P, Jabes J, Laroche H. et Michel S., Management, aspects humains et organisationnels, Paris, PUF Fondamental, 1991.

[54] Cocula F. et Fredy-Planchot A: « Pratiquer le management à distance », Gestion 2000, n° 1, janvier-février 2003, p. 43-63.

privée, mais dans le même temps, il risque de détériorer la communication avec ses collègues et son manager.[55]

Le contrôle dans le cadre du télétravail peut se caractériser par une analyse approfondie des résultats et du travail fourni. Le salarié se retrouve donc en télétravail en même temps autonome, mais bien souvent plus stressé que lorsqu'il est en entreprise.

L'autonomie peut se définir dans le cadre du télétravail comme la capacité de l'individu à initier et réguler ses propres actions, lui permettant ainsi de s'adapter à des situations changeantes, afin de prendre des décisions plus pertinentes pour résoudre les problèmes rencontrés dans son travail au quotidien.[56]

Cette autonomie accordée au salarié par le télétravail amène toutefois à un sentiment de rupture du lien social et peut l'amener à se détacher de l'entreprise tout en se sentant constamment surveiller. Le télétravail conduit en effet le salarié à un autocontrôle, accroissant sa responsabilité mais également les risques pouvant être liés à de mauvaises initiatives.

Les travaux présentés montrent que la mise en place du télétravail implique des effets potentiellement négatifs sur la charge de travail, la gestion de l'activité professionnelle, la motivation et la satisfaction au travail, l'identification aux normes et valeurs de l'organisation, la communication et la collaboration au sein des équipes, les relations et l'insertion socio-professionnelle, la reconnaissance, la socialisation et l'évolution au sein de l'organisation mais aussi la santé physique et psychologique.

Afin d'éviter ces risques et d'aider le salarié dans la pratique du télétravail, des modalités de contrôle pourront être mises en place, dans le cadre d'une gestion individualisée du salarié.[57] Cette surveillance constante amène bien souvent

---

[55] Ibid 49

[56] Ettighoffer D., L'entreprise virtuelle, Nouveaux modes de travail, nouveaux modes de vie ?, Paris, Editions d'Organisation, 2001.

[57] Emilie Vayre, LES INCIDENCES DU TÉLÉTRAVAIL SUR LE TRAVAILLEUR DANS LES DOMAINES PROFESSIONNEL, FAMILIAL ET SOCIAL ; PUF « Le travail humain », P 1-39

l’employeur à s’infiltrer dans le domaine privé du salarié et c’est la raison pour laquelle il est important que le télétravail se mette en conformité avec le RGPD.

Cette mise en conformité pourrait passer par la mise en place d’un dispositif d’informations détaillées sur l’encadrement par l’entreprise du télétravail, notamment des modalités d’accès au matériel mis à la disposition du salarié, de l’information également sur les logiciels installés sur son matériel et lui permet d’accéder depuis son domicile ou un télécentre aux ressources de l’entreprises.

La mise en œuvre d’un planning clair également des heures de télétravail mettrait certainement le salarié plus en confiance et le rendrait à n’en point douter beaucoup plus productif même lorsqu’il est en télétravail.

Mis à part le télétravail, il est également nécessaire de procéder à un encadrement de la technologie mobile mise à la disposition du salarié dans le cadre de son travail.

B- L'encadrement de l'utilisation des technologies mobiles et la nécessité de sa mise en conformité au RGPD

L'évolution des technologies numériques ont fortement contribué à un bouleversement des outils et matériels de travail au sein des entreprises. Ainsi, on remarque dans les entreprises que les salariés sont de plus en plus dotés d'ordinateurs portables, ainsi que d'ordiphones.

L'usage de ces outils mobiles transforme profondément les rapports traditionnels au temps et à l'espace qu'entretiennent les individus dans le contexte du travail et en dehors du travail. Les technologies mobiles dotent les individus de capacités d'ubiquité en ce sens que ces derniers peuvent exercer leurs activités professionnelles potentiellement n'importe quand, n'importe où, voire dans des contextes inhabituels.[58]

Les avantages à en retirer sont nombreux, au premier rang desquels l'accroissement de la productivité individuelle grâce à la réduction des exigences spatiales et temporelles dans la réalisation du travail, l'accroissement de la flexibilité, la diminution des coûts de coordination, l'amélioration de la communication et de l'échange de connaissances. En outre, les technologies mobiles facilitent l'immédiateté de l'accès à l'information, la hausse de la performance dans la prise de décision, et, ainsi, l'accroissement de la réactivité face aux clients.[59]

Au sein de l'entreprise, le téléphone mobile en particulier apparaît comme un instrument au service de l'indépendance et de la mobilité des salariés. Il n'en est pas moins également le symbole d'un maintien des « chaînes hiérarchiques » au-delà même des frontières de l'entreprise. L'utilisation par les salariés des technologies mobiles permet potentiellement aux entreprises, au travers d'une « traçabilité digitale

[58] Chen L., Nath R., "Nomadic culture: cultural support for working anytime, anywhere", Information Systems Management, Fall 2005, p. 56-64.

[59] Gribbins M.L., Gebbauer J., Shaw M. J., "Wireless B2B mobile commerce: a study on the usability, acceptance, and process fit", Ninth Americas Conference on Information Systems, 2003.

», d'exercer sur eux un contrôle et une surveillance continus, en dehors de l'espace de travail, ce qui ne va pas sans provoquer un certain stress et accroître les risques d'empiètement sur la vie privée.[60]

De plus, les individus peuvent se sentir oppressés par l'émergence d'une véritable « culture de la vitesse et de l'instantanéité » qui les oblige à prendre des décisions dans l'urgence, ou dans des contextes inadaptés à la prise de décision, ce qui peut s'avérer finalement contre-productif. Cette contre productivité peut produire des effets ambivalents voire paradoxaux, et provoquer des conséquences « ironiques et perverses ».[61]

Ces risques pour le salarié, mais également pour l'entreprise nécessite qu'on s'y penche pour qu'un encadrement pouvant passer par un droit à la déconnexion soit mis en place.

Le droit à la déconnexion rappelle le fait désormais partie, tout comme l'égalité homme et femme, systématiquement des points de négociations annuelles collectives par les représentants du personnel (Annexe 3).

Le droit à la déconnexion se définit comme « la capacité, pour le salarié, à pouvoir ou devoir rester injoignable en dehors de son temps de travail. Il est important de souligner que l'aspect psychologique, et non simplement matériel, de ce droit doit être pris en compte. D'une certaine manière, il est une composante du droit au repos minimal. »[62]

Le salarié peut exercer ce droit, sous réserve de répondre à l'employeur si dans le cadre d'un arrêt de travail, ce dernier le contacte juste dans le but d'obtenir le code de son ordinateur.[63]

---

[60] Cousins C.K., Robey D., "Human agency in a wireless world: Patterns of technology use in nomadic computing environments", Information and Organization, vol. 15, n° 2, 2005, p. 151-180.

[61] Arnold M., "On the phenomenology of technology: the "Janus-faces" of mobile phones", Information and Organization, 13, 2003, p. 231-256.

[62] Lamy Temps de travail, En quoi consiste le droit à la déconnexion et quelles sont les obligations de l'entreprise en la matière ?

[63] Cour de cassation, Chambre sociale, Arrêt nº 843 du 18 mars 2003, Pourvoi nº 01-41.343

La Cour de cassation l'a d'ailleurs affirmé s'agissant d'un ambulancier qui avait été licencié pour faute grave, après avoir refusé de répondre aux appels téléphoniques de son employeur en dehors de ses heures de travail. Elle a jugé le licenciement abusif en ces termes : « Qu'en statuant comme elle l'a fait, alors que le fait de n'avoir pu être joint en dehors des horaires de travail sur son téléphone portable personnel est dépourvu de caractère fautif et ne permet donc pas de justifier un licenciement disciplinaire pour faute grave »[64].

Ce faisant, la Cour pour rendre sa décision a eu recours au droit à la déconnexion du salarié, même si elle ne l'a pas mentionné explicitement. Ce droit à la déconnexion pour se conformer aux exigences du RGPD doit faire état d'une information aux salariés et il doit leur être notifié les conditions dans lesquelles il s'applique.

L'humain étant au cœur de toute ces problématiques, il s'avère indispensable que les employeurs pensent à sa revalorisation et son bien-être pour un meilleur rendement aussi bien dans l'entreprise qu'en dehors de l'entreprise.

64 Cour de cassation, Chambre sociale, Arrêt nº 332 du 17 février 2004, Pourvoi nº 01-45.889

Section 2 : La nécessité d'une revalorisation de l'humain par l'entreprise

A l'ère de la révolution numérique absorbant automatisation, robotisation, intelligence artificielle, les interactions entre les travailleurs et les machines font craindre un risque de déshumanisation dans les entreprises.

Or, selon les Tendances Ressources Humaines 2019, 86 % des entreprises ont conscience de l'importance d'un environnement de travail centré sur l'humain et fondé sur l'expérience collaborateur. En effet, les règles du jeu ont changé, les collaborateurs sont en quête d'entreprises qui sont profondément humanistes. Ils sont à la recherche de sens, de reconnaissance, de transparence et de confiance. La viabilité économique de leur entreprise n'est plus un critère suffisant pour s'y engager, elle doit également avoir un impact dans la société.[65]

L'enjeu de l'entreprise porte sur sa transformation en entreprise sociétale prenant en compte son empreinte sociale (interne) et sociétale (externe), afin de jouer un rôle modèle pour ses pairs.[66]

De nombreux employeurs l'ont compris et mise de plus en plus sur un bien être du salarié au sein de l'entreprise.

Ce bien être passe par une mise en place de charte informatique et de règlement intérieur prenant en compte le droit à la vie privée du salarié conforme au RGPD (A), ainsi que la prise en compte des situations de stress liées au contrôle des salariés (B) en entreprise.

65 2019 DELOITTE GLOBAL HUMAN CAPITAL TRENDS

66 LAMYLINE, Les Cahiers du DRH, Nº 265, 1er juin 2019

A- La nécessaire mise en place de charte informatique et règlement intérieur conformes aux exigences de sécurité du RGPD

Le maillon faible de l'entreprise reste et demeure bien souvent l'humain. De même qu'il doit voir sa vie privée protéger, il peut également par des négligences être à l'origine de violation de données au sein de l'entreprise. Ainsi, il est nécessaire de mettre en œuvre une charte informatique ensemble avec le règlement intérieur.

Cette charte devra préciser les différentes obligations découlant de sa signature pour le salarié ainsi que de toute personne contractant avec l'employeur.

La CNIL préconise que la charte informatique comprenne les informations suivantes :

« 1. Le rappel des règles de protection des données et les sanctions encourues en cas de non-respect de celles-ci.

2. Le champ d'application de la charte, qui inclut notamment :

- les modalités d'intervention des équipes chargées de la gestion des ressources informatiques de l'organisme ;
- les moyens d'authentification utilisés par l'organisme ;
- les règles de sécurité auxquelles les utilisateurs doivent se conformer, ce qui doit inclure notamment de :
  - signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
  - ne jamais confier son identifiant/mot de passe à un tiers ;
  - ne pas installer, copier, modifier, détruire des logiciels sans autorisation ;

- verrouiller son ordinateur dès que l'on quitte son poste de travail ;
- ne pas accéder, tenter d'accéder, ou supprimer des informations si cela ne relève pas des tâches incombant à l'utilisateur ;

Respecter les procédures préalablement définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité.

3. Les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition comme :

- le poste de travail ;
- les équipements nomades (notamment dans le cadre du télétravail) ;
- les espaces de stockage individuel ;
- les réseaux locaux ;
- les conditions d'utilisation des dispositifs personnels ;
- l'Internet ;
- la messagerie électronique ;
- la téléphonie.

4. Les conditions d'administration du système d'information, et l'existence, le cas échéant, de :

- systèmes automatiques de filtrage ;
- systèmes automatiques de traçabilité ;
- gestion du poste de travail. »

De plus, la charte devrait contenir pour se conformer au RGPD, un article sur la protection de la vie privée indiquant qu'il est ou non possible pour un salarié de faire à titre personnel et ce afin d'encadrer un tel usage. En effet, si la charte peut rappeler que la messagerie, les moyens confiés sont des outils professionnels et non destinés à des usages privés, il n'est pas possible d'interdire totalement l'usage à titre personnel

des messages électroniques, moyens informatiques et ce notamment au vu de la dernière jurisprudence en la matière.[67]

La charte doit également comprendre un article mesures de sécurité qui doit préciser les conditions d'accès au réseau, la gestion des mots de passe, les conditions de protection de certains fichiers, la sécurité liée aux PC portables etc. (par exemple : « Ne jamais laisser son PC portable accessible et sans surveillance », « Ne pas quitter son poste de travail en laissant accessible une session ouverte, pendant une absence prolongée »).

Cette charte informatique viendra en complément du règlement intérieur qui doit également comporter des mesures de sécurité et garantir la protection de la vie privée des salariés.

C'est en effet l'article L 1311-2 du Code du travail qui a rendu obligatoire depuis 1982 la mise en place d'un règlement intérieur pour les entreprises de plus de vingt (20) salariés.

Le règlement intérieur évolue au fur et à mesure des lois qui l'affectent. Ainsi, en matière de sécurité, le contenu du règlement intérieur s'apparentait, en 1982, à une mesure de police. Il devait fixer « les mesures d'application de la réglementation en matière d'hygiène et de sécurité dans l'entreprise ou l'établissement ».

Cette prescription est maintenue, l'hygiène ayant simplement fait place à la santé, mais la loi a été complétée pour intégrer « les conditions dans lesquelles les salariés peuvent être appelés à participer, à la demande de l'employeur, au rétablissement de conditions de travail protectrices de la santé et de la sécurité des salariés, dès lors qu'elles apparaîtraient compromises ».

Ce rappel indirect de l'obligation de prévention est significatif d'une évolution qui se confirme par l'ajout dans le règlement intérieur des « dispositions relatives aux harcèlements moral et sexuel et aux agissements sexistes prévues par le présent code»[68].

---

[67] LAMY DROIT DU NUMERIQUE, 4077- CONTENU DE LA CHARTE

[68] Article L. 4121-1 du Code du travail

Le législateur guide ainsi l'employeur. Puisque celui-ci doit prendre toutes les mesures nécessaires pour assurer la sécurité et protéger la santé des salariés, la mobilisation du règlement intérieur ne doit pas être oubliée, même s'il n'est pas question de s'en contenter.

Le règlement intérieur doit prendre en compte aujourd'hui les prescriptions du RGPD dans sa mise en œuvre en faisant mention des dispositions du RGPD en cas de mise en œuvre des dispositifs de contrôle de l'activité des salariés au sein de l'entreprise.

Le bien être des salariés tenant de plus en plus à cœur aux dirigeants des entreprises, des dispositions concernant le harcèlement moral, sexuel et aux agissements sexistes doivent figurer dans le règlement intérieur.

Toutes ces mesures doivent s'accompagner de la prise en compte des situations de stress vécus par le salarié au sein ou en dehors de l'entreprise afin de lui permettre d'offrir un bon rendement au sein de l'entreprise.

B- La prise en compte des situations de stress liées au contrôle de l'activité des salariés

Il est de plus en plus perceptible au sein des entreprises aujourd'hui que les salariés sont constamment connectés, même bien souvent en dehors de leurs horaires réglementaires de travail, de telle sorte que la frontière déjà très restreinte existant entre vie privée et vie professionnelle se trouve perturber.[69]

Cette perturbation entraîne le plus souvent du stress, voir du burn-out.

Le Dictionnaire de la langue française appelé « Le Petit Robert » donne la définition suivante du stress : il s'agit d'une « réponse de l'organisme aux facteurs d'agressions physiologiques et psychologiques ainsi qu'aux émotions (agréables ou désagréables) qui nécessitent une adaptation ».

Dans la sphère du travail, le salarié peut se retrouver confronter à un stress dit psychologique qui selon De keyser et Hansez, deux psychologues du travail est « une réponse du travailleur face aux exigences de la situation pour lesquelles il doute de disposer de ressources nécessaires et auxquelles il estime devoir faire face ».[70]

Ce stress psychologique peut être la cause de l'hyperconnexion remarquée des salariés et a bien souvent des répercussions sur la motivation du salarié qui se retrouve parfois être moins productif et donc apporte une plus-value moindre pour l'entreprise.

La Fondation April, qui mène des actions de prévention et des études sur la santé, a réalisé un baromètre sur les impacts de l'hyper-connexion, présenté le 26 juin 2018 (Annexe V). Ce baromètre indique que les Français sont très exposés aux écrans et

[69] Lamy Protection Sociale Informations, Une hyperconnexion mauvaise pour la santé et la sécurité ; Nº 1128, 4 juillet 2018

[70] De Keyser, V., & Hansez, I. (1996). Vers une perspective transactionnelle du stress au travail : Pistes d'évaluations méthodologiques. Cahiers de Médecine du Travail, 33 (3), 133-144.

multi équipés : les deux tiers en possèdent trois ou plus, le smartphone étant le plus répandu. Ils passent près de 4 heures 30 minutes par jour devant leurs écrans, davantage pour les 18-34 ans (6 heures 28 minutes) et les cadres (7 heures 13 minutes). 72 % pensent qu'il serait bon pour leur santé d'y consacrer moins de temps, mais sept sur dix ne pourraient pas s'en passer plus d'une journée. « Seule la moitié des Français sont conscients que l'hyperconnexion peut avoir des impacts négatifs sur la vision, l'activité physique, l'alimentation et le sommeil, et un tiers s'estime mal informé sur ces risques »[71].

En entreprise, les mesures contraignantes, comme les restrictions d'e-mails ou la déconnexion forcée la nuit, sont massivement rejetées. « Chacun veut garder sa liberté d'usage, mais dans le même temps demande à être protégé de la sur-sollicitation.

De plus, il faut reconnaître que le digital a déstabilisé tout dans l'organisation du travail.

Désormais, l'efficacité et la productivité ne suffisent plus et sont détrônées par une impérieuse nécessité d'innover dans un contexte aussi souple qu'hyperconcurrentiel.

Face à cette transformation de l'entreprise, les jeunes diplômés ne sont plus attirés par le sacrifice d'une vie personnelle au profit d'une carrière stressante. Ils sont donc en quête perpétuelle de bien-être et choisissent leurs entreprises en fonction des valeurs prônées par cette dernière.

Le bien-être se résume souvent à la qualité de la relation qu'entretient le salarié avec son supérieur hiérarchique, la relation avec ses collègues immédiats, un rapport entre les temps privé et professionnel qu'il estime équilibré et son environnement physique de travail.[72]

Pour la plupart des jeunes diplômés, l'entreprise idéale est donc celle où il existe un management participatif, où l'innovation est libérée et le bien-être du salarié occupe une place capitale. Bien souvent, les jeunes diplômés, lorsqu'ils arrivent au sein

[71] Pierre Wolf, médecin et membre du CA de la Fondation APRIL

[72] Institut national de la jeunesse et de l'éducation populaire, Le rapport des jeunes au travail, Rapport d'études, Février 2017

d'entreprises qui ne remplissent pas les conditions du bien-être, n'arrivent pas à donner le meilleur de leur potentiel et préfèrent zapper pour aller rechercher dans une autre entreprise le bien-être pour une meilleure motivation.

Ils exigent que leur emploi ait un sens et soit un vecteur de développement personnel. Le contenu de l'emploi et l'ambiance au travail comptent ainsi plus que les conditions matérielles associées à un métier. D'ailleurs, moins d'un sur deux considère la rémunération ou le temps de travail comme des notions importantes. Par contre, plus de 8 étudiants sur 10 qualifient l'intérêt du poste et le bien-être au travail de critères très importants.[73]

La qualité du futur emploi est primordiale. Ainsi, une enquête ipsos réalisée sur un échantillon de jeunes étudiants révèle que l'intérêt du poste compte pour 88 % d'entre eux, l'ambiance pour 84 % et 75 % veulent faire un métier en corrélation avec leurs valeurs. Les jeunes et futurs salariés souhaitent avant tout créer du sens : utilité, innovation et développement des compétences d'autrui sont les trois premières sources de fierté chez eux.

Les jeunes diplômés souhaitent également être au service des autres : 53 % d'entre eux considèrent qu'être utile aux autres est un prérequis absolu dans le cadre de leur travail. Mais qu'est-ce qu'être « utile » selon eux ? Servir l'intérêt général pour 65 %, améliorer la vie des gens pour 54 % et permettre de changer les choses pour 40 % d'entre eux. Les jeunes femmes témoignent d'un plus fort attrait pour l'ESS[74]. Sans doute parce qu'elles la connaissent mieux (87 % contre 81 % des hommes). Elles sont nombreuses à vouloir s'engager dans cette voie : c'est même une réelle envie pour 61 % d'entre elles.[75]

Plusieurs entreprises ont compris aujourd'hui l'importance de mettre sur pied des politiques en vue de permettre à leur salarié de se sentir bien au sein de leur entreprise et même en dehors. Le plus pertinent est donc d'élaborer une charte de

[73] Ipsos Publications : Société Qu'est-ce que les jeunes des grandes écoles attendent de leur emploi ? disponible sur https://www.ipsos.com/fr-fr/quest-ce-que-les-jeunes-des-grandes-ecoles-attendent-de-leur-emploi

[74] Economie Sociale Solidaire

[75] Ibid 72

bonnes pratiques en concertation avec les salariés, obligeant à questionner l'organisation et les pratiques de travail ».[76]

L'élaboration de la charte de bonne pratique rentre alors de plus en plus dans les plans d'actions des employeurs.

Contrairement au règlement intérieur qui est expressément prévu dans le Code du travail, l'entreprise n'a pas l'obligation de mettre en place une charte de bonne pratiques ou charte relationnelle en son sein.

La rédaction de cette charte relationnelle est donc totalement libre et chaque entreprise pourra y mettre un contenu prenant en compte des comportements à adopter, une éthique et des valeurs morales prônées par l'entreprise et qui permettront que les salariés soient moins stressés et plus productifs.

[76] Fabienne Ernoult, déléguée générale RSE de la Fondation April

ANNEXES

ANNEXE 1 : PYRAMIDE DES BESOINS DU SALARIE SELON ABRAHAM MASLOW

ANNEXE 2 : EXEMPLE D'IMAGE D'INSTALLATION CONFORME D'UN DISPOSITIF DE SURVEILLANCE VIDEO EN ENTREPRISE

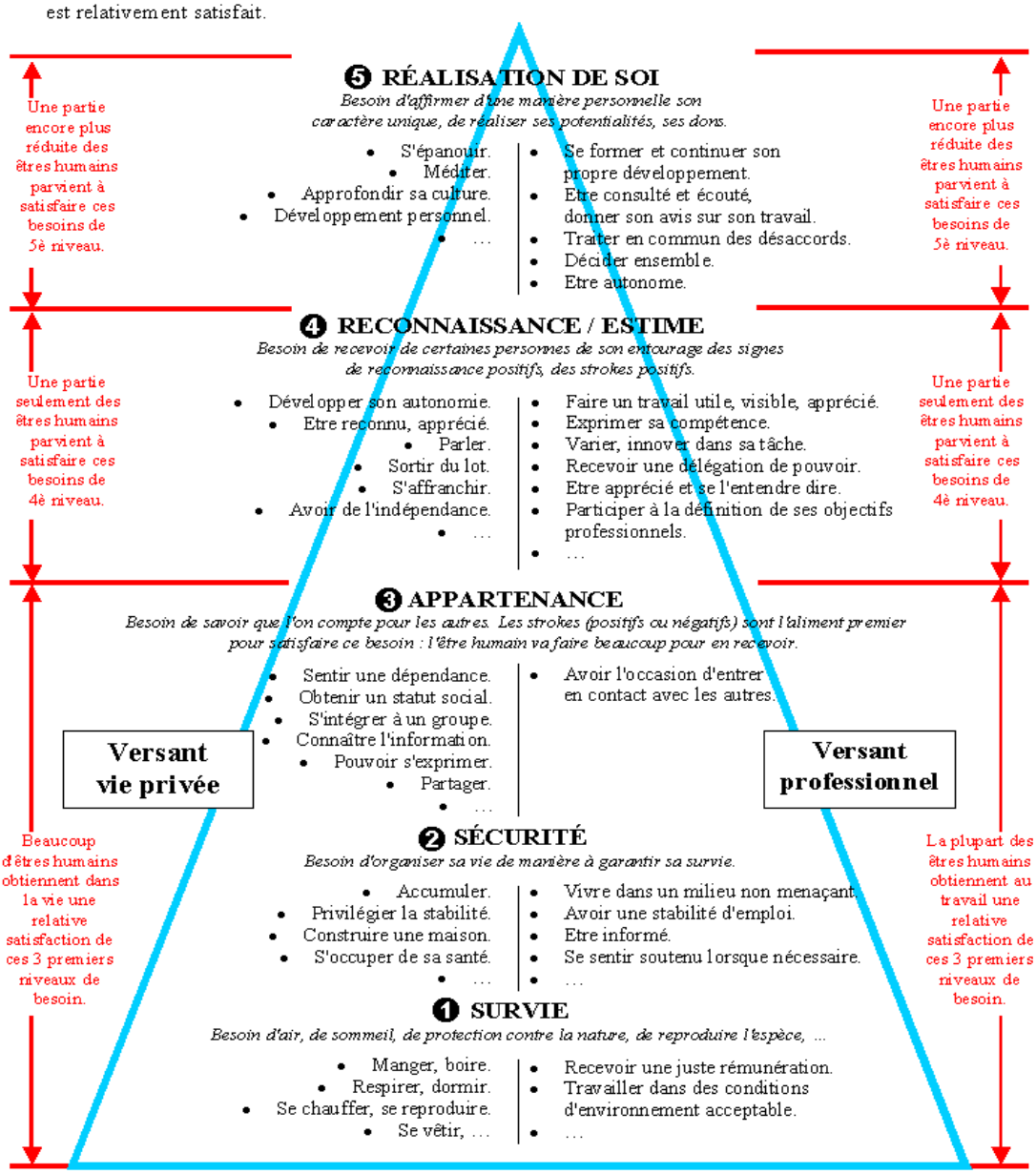
ANNEXE 3 : LAMY DROIT DES REPRESENTANTS DU PERSONNEL, LE DROIT A LA DECONNEXION

ANNEXE 4 : ELEAS, Qualité de Vie au travail et risques psycho sociaux ; Enquête « Pratiques numériques des actifs en France en 2016

ANNEXE 5 : BAROMETRE ACTINEO 2019 SUR LE BIEN ETRE AU TRAVAIL

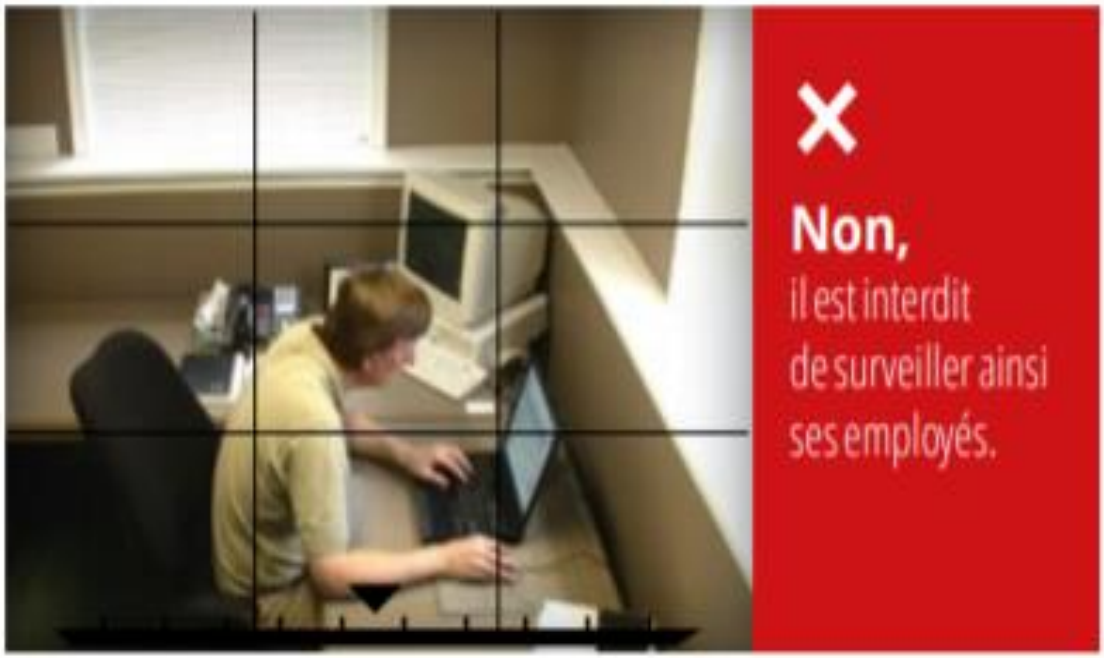
Besoins propres au monde occidental.

1. pyramide particulièrement intéressante pour le monde du travail
2. les humains ne ressentent l'apparition d'un besoin supérieur que lorsque le besoin actuel est relativement satisfait.



ANNEXE 1

ANNEXE 2 : INSTALLATION CORRECTE D'UN DISPOSITIF DE SURVEILLANCE VIDEO EN ENTREPRISE



ANNEXE 3

Le Lamy droit des représentants du personnel

837 - Droit à la déconnexion

Depuis le 1er janvier 2017, en vertu de la loi Travail du 8 août 2016, la négociation annuelle obligatoire d'entreprise « sur l'égalité professionnelle entre les femmes et les hommes et la qualité de vie au travail » doit également porter sur *« les modalités du plein exercice par le salarié de son droit à la déconnexion et la mise en place par l'entreprise de dispositifs de régulation de l'utilisation des outils numériques, en vue d'assurer le respect des temps de repos et de congé ainsi que de la vie personnelle et familiale »* (C. trav., art. L. 2242-17, 7º).

Le droit à la déconnexion a pour objectif d'assurer l'effectivité du droit à la santé et au repos (repos quotidien, hebdomadaire, congés) et une meilleure articulation entre la vie professionnelle et la vie personnelle et familiale. Est évidemment visée la « surconnexion » aux outils numériques professionnels en dehors du temps de travail (courriels, communications téléphoniques, etc.). Cela pose également la question du caractère raisonnable ou non de la charge de travail du salarié. Par exemple, un salarié qui reçoit d'innombrables courriels de ses managers durant son temps de travail mais également en dehors ce temps pourra se sentir contraint d'y répondre et de se connecter à ses outils numériques professionnels en dehors de son temps de travail. Autant de problématiques dont les organisations syndicales et les employeurs doivent donc se saisir.

À défaut d'accord sur les modalités d'exercice du droit à la déconnexion, **l'employeur doit élaborer une charte, après consultation du CSE**. Cette charte doit définir ces modalités d'exercice du droit à la déconnexion et prévoir la mise en œuvre, à destination des salariés et du personnel d'encadrement et de direction, d'actions de formation et de sensibilisation à un usage raisonnable des outils numériques (C. trav., art. L. 2242-17, 7º).

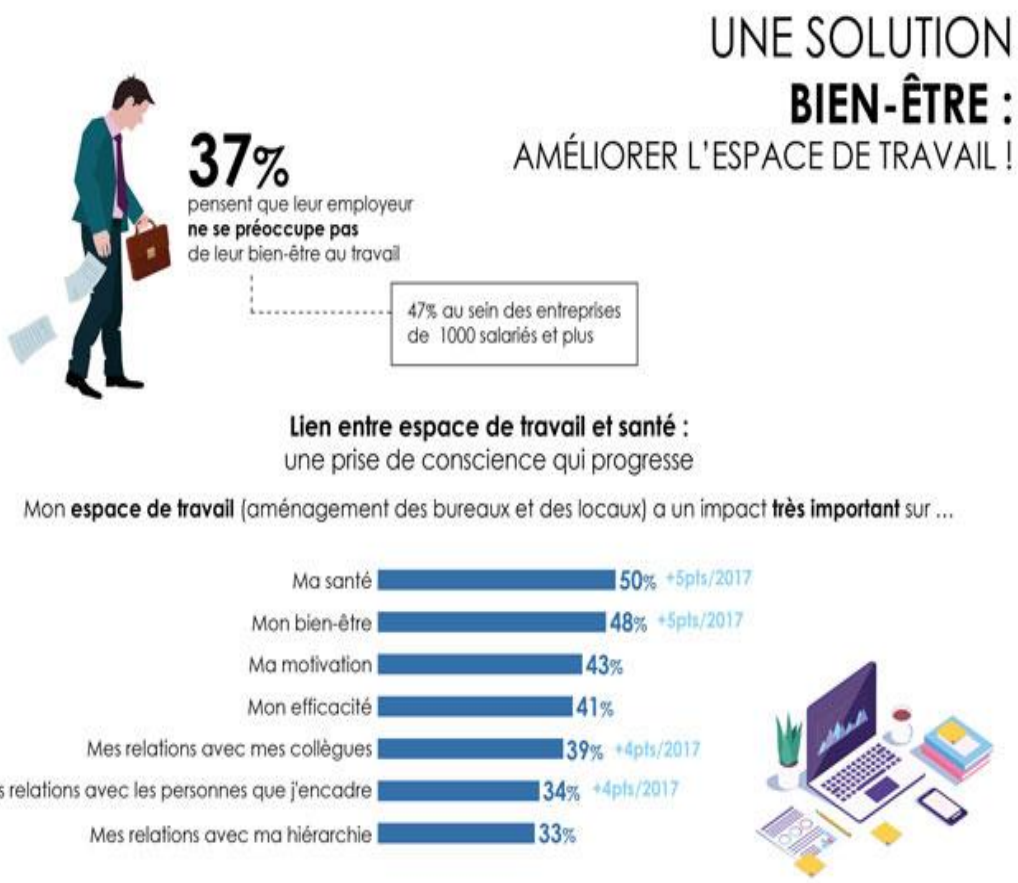
En outre, l'accord prévoyant la conclusion de conventions individuelles de forfaits annuels en jours doit fixer, entre autres, les modalités selon lesquelles le salarié en

forfait-jours peut exercer son droit à la déconnexion (C. trav., art. L. 3121-64). Si l'accord ne prévoit pas ces modalités, les modalités d'exercice par le salarié de son droit à la déconnexion doivent être définies par l'employeur et communiquées par tout moyen aux salariés concernés (C. trav., art. L. 3121-65, II). Dans les entreprises d'au moins 50 salariés, ces modalités doivent être conformes à la charte mentionnée à l'article L. 2242-17, 7º du Code du travail (voir ci-dessus).

Sur le droit à la déconnexion, voir : « Droit à la déconnexion : l'arbre qui cache la forêt ? », L. de Montvallon, SSL, nº 1743, 7 nov. 2016 ; « Droit à la déconnexion : un nouveau thème de négociation décrypté par J.-E. Ray » et « Négocier sur : Le droit à la déconnexion » (dossier convention collective), LSQ, nº 17212, 1er déc. 2016 ; H. Lanouzière, « De nouveaux cadres de régulation doivent être trouvés », SSL, nº 1755, 6 févr. 2017 ; « Retour sur le droit à la déconnexion à l'aube de 2ème anniversaire », Corinne Metzger et Marjorie Fredin, Les Cahiers Lamy du CSE nº 183, juill. 2018.

ANNEXE 4


HYPERCONNEXION : QUEL IMPACT SUR LA SANTÉ DES FRANÇAIS ?
Chiffres clés du baromètre 2019 Fondation APRIL / Institut BVA
fondation apri
Les Français sont de plus en plus équipés, connectés... et dépendants !
73 % des Français se disent dépendants de leurs outils connectés (67 % en 2018)
1 Français sur 10 déclare ne pas pouvoir passer une heure sans être connecté (1 sur 20 en 2018)
4 h 30 c'est le temps que les Français passent en moyenne par jour devant un écran (+ 8 minutes par rapport à 2018)
88 % possèdent un smarphone*. (80% en 2018)
79 % un ordinateur portable (78% en 2018)
57 % une tablette tactile (55% en 2018)
50 % un ordinateur fixe (57% en 2018)
1 Français sur 4 possède désormais ces 4 équipements
* équipement numérique le plus populaire
33 %
33 % des Français trouvent qu'Internet occupe une place trop importante dans leur vie (22 % en 2018)
Et pourtant, ils sont mieux informés des risques liés à l'hyperconnexion
72 % des Français pensent que limiter le temps passé sur les écrans serait bénéfique pour leur santé, et même « très bénéfique » pour 24 % d'entre eux :
37 % chez les 18-34 ans (26 % en 2018)
37 % chez les parents d'enfants de moins de 10 ans (29 % en 2018)
32 % chez les cadres (31 % en 2018)
Que feraient-ils en priorité avec ce temps gagné ?
51 % Se promener (+ 8 points par rapport à 2018)
47 % Passer du temps avec son entourage, famille et amis (+ 6 points)
44 % Se détendre et se reposer (+ 9 points)
72 % des Français déclarent connaître les impacts de l'exposition prolongée aux écrans sur leur santé et leur bien-être (65 % en 2018)
Impacts positifs :
66 % apprentissages et connaissances (77 % en 2018)
40% stimulation du cerveau (50 % en 2018)
22% moral (25 % en 2018)
Impacts négatifs :
71 % vision (76 % en 2018)
68% activité physique (57 % en 2018)
58% sommeil (56 % en 2018)
Vie privée, vie professionnelle : où en sont les Français ?
9 parents sur 10 se disent convaincus des conséquences néfastes des écrans sur la santé de leurs enfants
» 3 parents sur 4 adoptent un comportement exemplaire en limitant leur temps de connexion en présence de leurs enfants
» Mais dans les faits : Les parents jugent efficace d'instaurer des règles de limitation de l'usage des écrans de leurs enfants (45 %), et d'être exemplaires (44 %). En pratique, 57 % ne maîtrisent pas le temps de connexion de leurs enfants
6 h 03 c'est le temps moyen passé par les cadres devant leurs écrans, dont 3h36 pour des motifs professionnels. De bonnes pratiques s'installent peu à peu au bureau :
» 58 % limitent l'envoi des e-mails professionnels en dehors des heures de travail
» 57 % évitent de consulter leurs e-mails professionnels en dehors des heures de travail
» 52 % des salariés se déplacent ou téléphonent à leurs collègues pour éviter d'envoyer un e-mail
En moyenne, les Français passent plus de temps par jour sur leurs écrans pour des motifs personnels (3 h 06) que professionnels (1 h 24)
» 98 % des Français passent au moins une heure par jour devant des écrans pour des motifs personnels
Près d'1 Français sur 2 laisse son téléphone portable allumé la nuit à côté de son lit (soit 47 %)
» Chez les jeunes de 18-34 ans, ils sont 3 sur 4 (74 %) à adopter cette pratique.
Enquête réalisée par BVA par internet du 15 au 16 mai 2019 auprès d'un échantillon représentatif de 1 000 Français de 18 ans et plus. Cet échantillon a été constitué selon la méthode des quotas.


UNE SOLUTION
BIEN-ÊTRE :
AMÉLIORER L'ESPACE DE TRAVAIL !
37%
pensent que leur employeur
ne se préoccupe pas
de leur bien-être au travail
47% au sein des entreprises
de 1000 salariés et plus
Lien entre espace de travail et santé :
une prise de conscience qui progresse
Mon espace de travail (aménagement des bureaux et des locaux) a un impact très important sur ...
Ma santé 50% +5pts/2017
Mon bien-être 48% +5pts/2017
Ma motivation 43%
Mon efficacité 41%
Mes relations avec mes collègues 39% +4pts/2017
Mes relations avec les personnes que j'encadre 34% +4pts/2017
Mes relations avec ma hiérarchie 33%

ANNEXE 5

BIBLIOGRAPHIE

I. OUVRAGES

- Edouard Edouard Geffray, Alexandra Guérin-François, Code de protection des données personnelles annoté et commenté, Editions Dalloz, 5 septembre 2018

II. ARTILCES DE REVUES, DOCUMENTS ELECTRONIQUES

- Actualités juridiques, IT for business, Me Pierre-Randolph DUFAU ; Télétravail et RGPD, comment éviter la faille de sécurité ? Janvier 2019
- Bernard PRAS, ENTREPRISE ET VIE PRIVÉE ; Le « privacy paradox » et comment le dépasser ? Revue CAIRN.INFO, « Revue française de gestion », 2012/5 N° 224 | pages 87 à 94
- Charles-Henri Besseyre Des Horts et Henri Isaac ; L'IMPACT DES TIC MOBILES SUR LES ACTIVITÉS DES PROFESSIONNELS EN ENTREPRISE ; Revue CAIRN.INFO ; 2006/9 n° 168-169 | pages 243 à 263
- Editions Législatives, Les réseaux sociaux à la frontière entre Vie privée et vie professionnelle, 08/02/2019, disponible sur le site : https://www.editions-legislatives.fr/actualite/les-reseaux-sociaux-a-la-frontiere-entre-vie-privee-et-vie-professionnelle
- Emilie VOIRON, Avocat, Le contrôle du travail des salariés est-il remis en cause avec le RGPD ? Article disponible en ligne sur https://www.juritravail.com/Actualite/protection-donnees-rgpd/Id/288034
- Emmanuelle Destaillats, Avocat, Les nouvelles obligations de l'employeur en matière de protection des données personnelles des salariés ; mercredi 13 juin 2018 Article Expert, disponible sur internet : https://www.village-justice.com/articles/les-nouvelles-obligations-employeur-matiereprotection-des-donnees-personnelles,28756.html
- Eric Hazane, (IN)SÉCURITÉ NUMÉRIQUE ET PME : TRANSFORMER LES DÉFIS EN ATOUTS ; REVUE CAIRN.INFO, « Sécurité et stratégie » ; 2016/2 22 | pages 14 à 19
- Guilhem Giraud ; COMMENT RÉAGIR FACE AU VOL OU À LA PERTE D'INFORMATIONS ? La DLP comme point de départ d'une nouvelle approche en matière de protection de l'information ; Revue CAIRN.info, « Sécurité et stratégie » ; 2010/2 4 | pages 81 à 89
- Jérémie ROSANVALLON ; Le contrôle du travail, entre réalités et perceptions : le cas de la messagerie électronique, Revue CAIRN.INFO, Sociologie Pratiques 2011/I (n° 22), PAGES 19 à 33

- Linda Ben Fekih Aissi ; Monitoring électronique des performances : sources de stress, Revue CAIRN.INFO, Management & Avenir 2010/7 (n° 37), pages 306 à 328
- Marc Dumas et Caroline Ruiller ; LE TÉLÉTRAVAIL : LES RISQUES D'UN OUTIL DE GESTION DES FRONTIÈRES ENTRE VIE PERSONNELLE ET VIE PROFESSIONNELLE? « Management & Avenir » ; 2014/8 N° 74 | pages 71 à 95
- Marilia Maciel-Hibbard, PROTECTION DES DONNÉES PERSONNELLES ET CYBER(IN)SÉCURITÉ, « Politique étrangère », 2018/2 Été | pages 55 à 66
- Michèle Heitz et Jean-pierre Douard ; Stress au travail, la gestion du temps incriminée, Revue CAIRN.INFO, La souffrance au travail : quelle responsabilité de l'entreprise ? (2012), pages 201 à 230
- Monique Pontier, TÉLÉTRAVAIL INDÉPENDANT OU TÉLÉTRAVAIL SALARIÉ : QUELLES MODALITÉS DE CONTRÔLE ET QUEL DEGRÉ D'AUTONOMIE, La revue des sciences de gestion, 2014/1 N° 265 | pages 31 à 39, disponible sur internet : https://www.cairn.inforevue-rimhe-2017-3-page-3.html
- Myriam Quéméner, LA DIRECTIVE NIS, UN TEXTE MAJEUR EN MATIÈRE DE CYBERSÉCURITÉ, Revue CAIR.INFO, « Sécurité et stratégie » ; 2016/3 23 | pages 50 à 56
- Revue LAMY Droit Social, Le bien-être au travail peut se nicher dans la participation, Protection Sociale Informations, n° 1177, 10 Juillet 2019
- Revue LAMY Droit Social, n° 132-17 - Quelles sont les obligations de l'employeur relatives à la protection des données personnelles ?
- Revue LAMYLINE Liaisons sociales quotidien, Les implications du RGPD pour les services RH, Le dossier pratique, Nº 40/2018, 28 février 2018
- Revue LAMYLINE, Droit du travail au quotidien, n° 132-30 - L'employeur peut-il recourir à la vidéosurveillance ?
- Revue LAMYLINE, Droit du travail au quotidien, La mise en place d'un dispositif d'évaluation des salariés est-elle obligatoire ? n° 132-5
- Social Pratique, Surveillance des salariés, quelle marge de manœuvre pour l'employeur ? 25/09/2013, disponible sur www.wk-rh.fr/actualites/actualites_imprimer.php?action=imprimer&actualite_id=69590
- Sophia ALBERT, Avocat, La surveillance des salariés, disponible en ligne sur : https://www.juritravail.com/Actualite/consultation-comite-entreprise-conditions-emploi/Id/91081

III. RAPPORTS, CONTRIBUTIONS, COLLOQUES

- Centre d'Analyse Stratégique, L'impact des TIC sur les conditions de travail, Rapports et Documents 2012, n° 49
- CNIL, Sécurité : Sensibiliser les utilisateurs, disponible en ligne sur : https://www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs
- CNIL, Les outils informatiques au travail : le contrôle de l'utilisation d'internet et de la messagerie : dans quel but ? disponible en ligne sur : https://www.cnil.fr/fr/les-outils-informatiques-au-travail
- CNIL, La vidéosurveillance-vidéoprotection au travail, disponible en ligne sur : https://www.cnil.fr/fr/la-videosurveillance-videoprotection-au-travail
- CNIL, La géolocalisation des véhicules des salariés, disponible en ligne sur : https://www.cnil.fr/fr/la-geolocalisation-des-vehicules-des-salaries
- CNIL, L'accès aux locaux et le contrôle des horaires sur le lieu de travail, disponible en ligne sur : https://www.cnil.fr/fr/lacces-aux-locaux-et-le-controle-des-horaires-sur-le-lieu-de-travail
- Direction de l'animation de la recherche, des études et des statistiques, Document d'études, Les changements d'organisation du travail dans les entreprises : conséquences sur les accidents du travail des salariés, Septembre 2011
- HISCOX, RAPPORT CYBERSINISTRES, 2018
- Manuel de Droit européen en matière de protection des données, Edition 2018
- OCEAN AVOCATS, La Surveillance du salarié : les régimes applicables, disponible sur internet : www.ocean-avocats.com/surveillance-du-salarie-les-regimes-applicables/
- Deloitte Human Capitals Trends, Leading the social enterprise : reinvent with a human focus ; 2019

IV. TRAVAUX UNIVERSITAIRES

- Alain SUPIOT, Cours de Droit Social, Les nouveaux visages de la subordination, Université de Nantes, Février 2000
- Cécile Nicod, Maître de conférences à l'Université Lumière Lyon 2 et Jean-François Paulin, Maître de conférences à l'Université Lyon 1, Directeur de l'Institut de formation syndicale de Lyon 2, La subordination en cause, Semaine sociale Lamy Supplément, 28 mars 2011, n°1485
- Matthieu DEMOULAIN, Nouvelles Technologies et droit des relations de travail, Essai sur une évolution des relations de travail, Edition Panthéon Assas, 2012

V. JURISPRUDENCE

- Cour de Cassation, Chambre sociale, Arrêt nº 843 du 18 mars 2003, Pourvoi nº 01-41.343
- Cour de Cassation, Chambre sociale, 13 novembre 1996, 94-13.187, Bull. civ. V, no 386
- Cour de Cassation, Chambre sociale, Arrêt n° 835 du 28 février 2002, 00-11.793, Publié au bulletin
- CEDH, 25 juin 1997, Halford c. Royaume-Uni, Recueil des arrêts et décisions 1997-III
- Cour de Cassation, Chambre sociale, 31 janvier 2001, 98-44.290, Publié au bulletin.
- RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
- Guidelines3/2019 on processing of personal data through video devices, Adopted on10July2019
- Opinion13/2019on the draft list of the competent supervisory authority ofFranceregarding the processing operationsexemptfromthe requirement of a data protectionimpact assessment(Article 35(5)GDPR), Adopted on10July2019

TABLE DES MATIERES