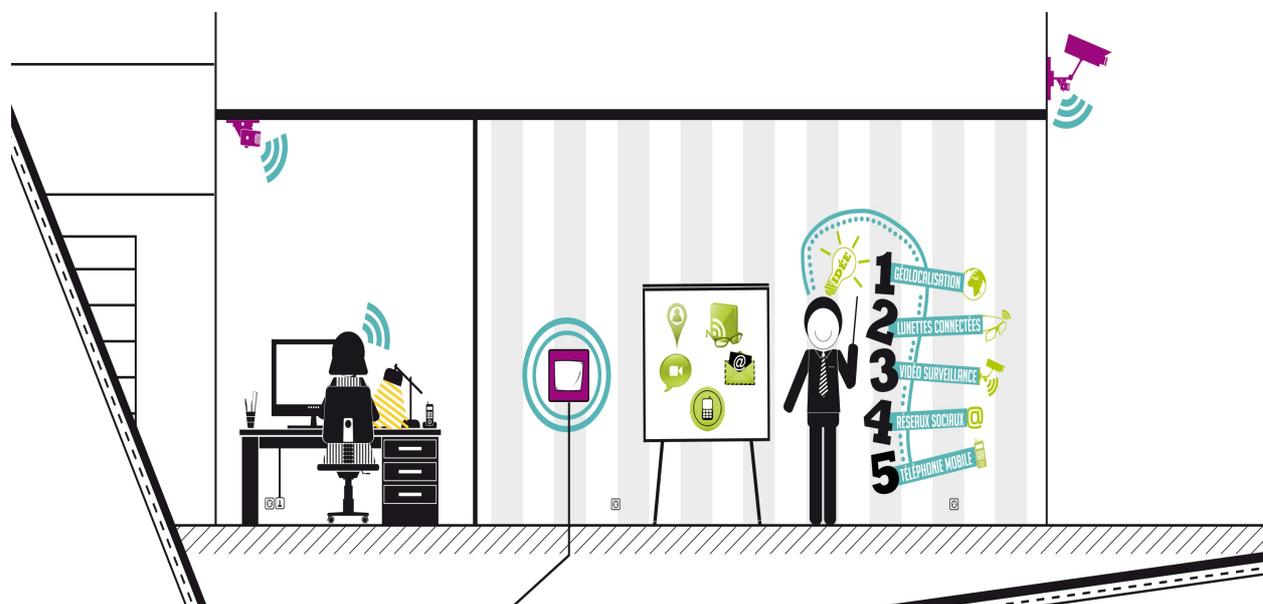


LE TRAVAIL CONNECTÉ



Par Audrey ALBAGLY et Anaïs JOSEPH-GABRIEL

Table ronde du vendredi 13 février 2015 « Le Droit et l'Internet des objets »

Master 2 Droit des médias et des télécommunications

Remerciements

Nous remercions tout d'abord Messieurs ISAR et LAURIE pour leur implication dans l'organisation de cette table ronde « Le Droit et l'internet des objets ».

Nous remercions ensuite Madame TOUBOUL pour ses précieux conseils ainsi que son implication pendant l'élaboration de notre projet.

Nous remercions finalement Monsieur Calvo pour avoir gentiment offert ses services pour sa participation au graphisme de notre page de couverture.

Une pensée particulière pour Monsieur TOUHAMI, camarade de notre master, pour son rôle de graphiste des affiches officielles de la table ronde 2015.

SOMMAIRE

Introduction

I. L'impact des objets connectés sur l'organisation du travail dans l'entreprise

A. L'impact positif des objets connectés sur l'organisation et les conditions de travail

B. L'impact négatif des objets connectés sur l'organisation et les conditions de travail

II. L'état des lieux du droit du travail appliqué aux objets connectés

A. L'application possible du droit du travail

B. Vers l'émergence d'un droit du travail 2.0 ?

CONCLUSION

Introduction

Les objets connectés sont en passe d'entraîner une véritable révolution, et ce dans un certain nombre de secteurs différents. Il s'agit de secteurs comme la santé¹ ou encore la sécurité. Au sein de l'entreprise cependant, les objets connectés traditionnels existent déjà depuis un certain nombre d'années, à l'instar de la caméra de surveillance, l'ordinateur, les Smartphones ainsi que les tablettes. C'est pourquoi, le droit du travail a eu le temps de s'adapter aux mutations technologiques passées afin de proposer un cadre juridique précis. Dans le monde du travail, il faut donc parler « d'évolution » plutôt que « révolution ». Effectivement, dans les années à venir nous allons assister à une propagation des objets connectés au sein de l'entreprise. Et la véritable révolution se concentre dans le fait que ces objets connectés vont sortir de l'enceinte de l'entreprise, afin de se greffer sur le salarié lui-même et cela va encore plus loin car certaines sociétés ont déjà eu l'idée d'implanter des puces RFID, puces habituellement présentes dans les objets connectés, directement dans le corps du salarié². Les objets connectés, qui se portent sur le corps, s'appellent les « wearables » ; il faut comprendre « portable ». Une étude récente de Forrester³ a révélé que l'appétence pour les wearables est considérable dans la sphère professionnelle. Ainsi, 68% des décideurs technologiques dans le monde estiment que les wearables sont une priorité pour leur entreprise et pensent que le bouleversement que ces objets vont engendrer est comparable à l'arrivée du smartphone en 2010. Selon une étude réalisée par le cabinet Deloitte⁴, le marché des objets connectés est très prometteur, et ce principalement pour les entreprises. En effet, en 2015 plus de 60% du milliard d'objets connectés existants seront achetés essentiellement par les entreprises. Ainsi à titre d'exemple, la croissance du chiffre d'affaire du drone sera notamment amplifiée par la consommation des entreprises. Donc, la multiplication des objets connectés dans l'enceinte de l'entreprise va principalement impacter les habitudes professionnelles et il y a de fortes chances qu'aucun secteur ne soit épargné.

Il convient donc de s'interroger, d'une part sur les conséquences de l'intégration des nouveaux objets connectés dans l'entreprise et d'autre part, sur la capacité de l'arsenal juridique existant à répondre aux nouveaux enjeux que posent les objets connectés.

¹ CHOUX (L.), ESTRUCH (L.) et GONZALVES (S.), rapport sur « La santé connectée », Table ronde Iredic, 13 février 2015, Aix-en-Provence.

² MADJOUR (R.) « Des puces électroniques implantées sous la peau d'employés suédois » *Kobini.com*, 5 février 2015

³ BISEUL (X.), « Demain les salariés seront bardés d'objets connectés », *01net*, 9 décembre 2014

⁴ BISEUL (X.), « En 2015, les entreprises seront à l'avant-garde de l'équipement digitale », *www.01net.com*, 5 février 2015

Dès lors, nous aborderons d'abord l'intégration et la mise à l'épreuve de l'organisation du travail des salariés dans l'entreprise, avant de nous pencher sur la question de savoir si l'encadrement, par le droit du travail, est suffisant face à la multiplication des objets connectés.

I) L'impact des objets connectés sur l'organisation du travail dans l'entreprise

Un certain nombre d'objets connectés nouveaux sont en passe de prendre possession de la sphère professionnelle. Ces objets connectés sont multiples et variés et un certain nombre d'objets sont d'ores et déjà utilisés dans le monde du travail. Cette utilisation permet d'une part d'observer des effets positifs pour l'entreprise **(A)** et d'autre part, permet d'anticiper une multiplication des risques existants pour le salarié dans l'entreprise **(B)**

A) L'impact positif des objets connectés sur l'organisation et les conditions de travail

L'utilisation des nouveaux objets connectés dans le monde de l'entreprise est variée, cependant certains objets connectés semblent plus importants que d'autres au regard de leur impact sur l'organisation et les conditions de travail. Il semble donc opportun de dresser une liste non exhaustive de ces objets connectés (a), avant d'en détailler l'utilité sur l'organisation et les conditions de travail (b).

a) Liste non exhaustive des objets connectés utilisés dans le monde du travail

Les principaux objets connectés utilisés dans le monde de l'entreprises sont divers et variés. Cela va du stylo connecté à la lumière intelligente en passant par le clavier connecté⁵. Nul doute que dans un futur proche tout objet le plus anodin soit-il, pourra devenir un objet connecté. Cependant, certains objets connectés semblent être plus importants que les autres tant pour leur utilité que pour leur impact sur l'organisation et les conditions de travail.

Il s'agit d'objets tels que le bracelet connecté. Certaines sociétés telle que la société Yahoo ont offert un bracelet connecté à leurs onze mille salariés⁶. Ces bracelets permettent aux salariés d'avoir accès à leurs e-mails, aux appels téléphoniques, à leurs messages téléphoniques, leurs agendas mais aussi permettront aux salariés de suivre leurs données de santé.

Les lunettes connectées se démarquent également. Ainsi des sociétés telle que la SNCF testent les lunettes connectées sur leurs contrôleurs⁷. Il s'agit de lunettes intelligentes qui permettent aux salariés d'avoir accès à leurs agendas, mails, messages téléphoniques, GPS ou encore une caméra.

Les drones sont le troisième objet connecté à attirer notre attention. Effectivement, des sociétés telles que Amazone ou encore Dominos pizza ont investi dans les drones pour assurer leurs

⁵ DRAGO (J.), « Les 8 objets connectés qui vont révolutionner le travail » *monkey-tie.com*, 27 juin 2014

⁶ ROZIER (U.), « Marissa Mayer offre un bracelet connecté Jawbone Up a ses employés », *frandroid.com*, 13 juillet 2013

⁷ RONFAUT (L.), « La SNCF équipe ses contrôleurs de Google Glass », *lefigaro.fr*, 24 octobre 2014

livraisons⁸ ou encore la société EDF qui prévoit d'utiliser des drones pour surveiller ses lignes à hautes tensions⁹.

Il s'agit également d'objets comme les imprimantes 3D, pour lesquelles de nombreuses sociétés, telle que la société PSA Peugeot Citroën, ont investi pour la fabrication de voitures¹⁰.

En outre, nous trouvons d'autres objets comme les vêtements connectés. Il s'agit d'une tenue de travail connectée qui permet de mesurer le rythme cardiaque, la température de la peau ou encore l'humidité. Cet objet connecté a pu être testé sur les pompiers, afin de surveiller leurs fonctions vitales, pendant des interventions à risque par exemple¹¹.

b) Les aspects positifs des objets connectés

Les objets connectés impactent indéniablement l'organisation de l'entreprise et ont un effet sur la rentabilité économique de l'entreprise.

Tout d'abord, l'introduction d'un objet connecté dans l'entreprise permet un gain de temps à l'instar des agents de la SNCF qui utilisent déjà les lunettes connectées pour scanner les billets des usagers. Ils pourront ainsi, à l'aide de leurs lunettes connectées voir apparaître toutes les informations concernant le détenteur du billet, tout en ayant les mains libres.

Puis, les objets connectés permettent également une meilleure sécurité du travailleur.

C'est l'exemple des personnes exerçant des métiers à risque, tels que les pompiers. Ainsi, le port des vêtements connectés pourra permettre à celui qui reçoit les informations d'anticiper d'éventuels risques liés au danger de s'aventurer dans certaines zones comme au cours d'un incendie, puisque les capteurs présents sur ses vêtements vont lui indiquer la présence de gaz toxique par exemple.

Qui plus est l'entreprise pourra gagner en efficacité car l'objet connecté va permettre de robotiser l'accomplissement de certaines missions des salariés. C'est l'exemple de la société Amazone qui utilise déjà les drones pour livrer ses marchandises.

Finalement, les entreprises pourront voir accroître leur productivité. Effectivement, elles bénéficieront d'une augmentation de leur croissance économique puisque l'objet connecté permettra de produire plus dans un temps réduit. C'est le cas pour l'imprimante 3D qui va révolutionner la conception de la production de masse. Par exemple, certaines entreprises proposent déjà de modéliser des objets puis de les vendre en les fabriquant à l'aide d'une imprimante 3D. Les clients choisissent un modèle virtuel et l'entreprise s'occupe de l'imprimer en 3D. L'imprimante permet de modéliser plusieurs types d'objets et donc de gagner en productivité en répondant à une demande plus étendue.

⁸ POIDEVIN (B.) et VANCOSTENOBLE (C.), « Drones : Responsabilité pénale, vie privée et données personnelles », *Expertises des systèmes d'information*, Avril 2014, n° 390, p. 144

⁹ BLOCH (M.), « Cinq usages méconnus des drones », *francetvinfo.fr*, 28 mai 2013

¹⁰ CLAPUD (A.), « PSA s'offre la plus grosse imprimante 3D du marché », *01net.com*, 10 juin 2013

¹¹ GRALLET (G.), « le vêtement connecté, cette nouvelle peau électronique », *lepoint.fr*, 19 novembre 2014

B) L'impact négatif des objets connectés dans l'organisation et les conditions de travail

L'apparition récente des objets connectés va avoir un impact négatif sur l'organisation du travail dans l'entreprise ainsi que sur le salarié lui-même. En effet, de nouvelles problématiques vont apparaître en lien avec l'apparition de ces nouveaux objets. De la même manière qu'Internet a révolutionné le monde de l'entreprise et a fait apparaître de nouveaux risques notamment concernant le droit à la vie privée du travailleur, sa santé ainsi que la nouvelle organisation qui en a découlé, ces nouveaux objets connectés vont être également à l'origine de nombreux changements dans le futur. Ces changements sont susceptibles d'intervenir aussi bien dans le cadre de l'embauche (a), qu'au niveau de l'exécution du contrat de travail lui-même (b). Finalement, les impacts négatifs des objets connectés se ressentent aussi dans la phase de rupture de contrat de travail car il est possible que cette utilisation mène au licenciement du salarié (c).

a) L'embauche

La première phase concerne le recrutement du travailleur. En matière de recrutement « classique », on peut observer depuis quelques années maintenant de nouvelles pratiques. En effet, les demandes d'emplois sont mises en ligne régulièrement, des applications de recrutement sur mobile ont vu le jour. De même, les entretiens d'embauche peuvent se faire via des logiciels comme Skype. Et les CV des candidats sont directement mis en ligne sur des réseaux sociaux spécifiques (LinkedIn). On parle alors de e-recrutement¹².

Cela a fait survenir une pratique dite de « googlelisation » du candidat. Le but est de rechercher des informations sur le potentiel futur salarié : les recruteurs recherchent son e-réputation. L'existence des réseaux sociaux peut également permettre au recruteur de constituer d'immenses bases de données. Cela revient à la problématique du Big Data¹³.

En pratique, le recruteur « googlelise » le candidat avant même de le rencontrer, afin de lui permettre d'obtenir toutes les informations à son sujet. Un certain nombre de nos données personnelles se retrouve déjà sur Internet. Mais avec l'Internet des objets, il va pouvoir connaître l'état de santé du candidat avec précision ou encore pouvoir le localiser dans ses déplacements, que ce soit dans des manifestations politiques ou dans des lieux de culte. Bref, toutes les données sensibles du candidat seront connues du recruteur. Il s'agit des origines raciales, des opinions philosophiques, syndicales ou religieuses, de sa vie sexuelle ou de son état de santé.

¹² TRICOIT (J-P.), « Recrutement, rupture du contrat de travail et TIC », *JCP S*, 1^{er} octobre 2013, n°40, p 10.

¹³ TRICOIT (J-P.), *op. cit.*, p. 12.

De même, le salarié en période d'essai pourra être équipé de ces objets connectés. Ces derniers vont potentiellement recueillir des données qui lui sont personnelles, données dont l'employeur va pouvoir avoir connaissance.

Prenons l'exemple du bracelet connecté conçu pour mesurer la santé du travailleur. Ce bracelet permet de mesurer les conditions physiques de celui qui le porte. Il a pu être envisagé pour des métiers qui demandent une bonne condition physique comme pour les pompiers ou les policiers¹⁴. Si les données révèlent une forme physique un peu en baisse, l'employeur aura la possibilité de mettre fin à la période d'essai pour des causes abusives. Or, la période d'essai doit seulement permettre d'évaluer les compétences du salarié et pas autre chose.

D'une manière générale, on peut considérer que le fait pour l'employeur d'avoir accès à ces données de santé l'influencera nécessairement car un salarié dont la santé est fragile se mettra plus facilement en arrêt maladie. Ce qui entraînera automatiquement une augmentation des coûts pour l'entreprise (indemnité liée à l'arrêt maladie) et un manque d'effectif (obliger de recruter afin de remplacer la personne absente).

La présence d'un bracelet permettant de déceler la véritable forme du salarié contribue donc à augmenter les risques de discrimination durant cette phase d'embauche.

Outre le fait que l'état de santé du salarié va pouvoir être mesuré à l'aide de ces objets connectés et que cela va pouvoir conduire l'employeur à une discrimination illégale relative à des conditions physiques défavorables, les Technologies de l'Information et de la Communication (TIC) sont considérées comme un facteur de risque sur la santé des travailleurs. Même si officiellement, il est interdit de collecter des données qui ont trait à la santé d'un individu, quel qu'il soit, par la loi du 6 janvier 1978 « Informatique et Liberté »¹⁵. Cependant, malgré cette prohibition le développement de ces nouvelles technologies numériques est de nature à entraver ce principe.

b) L'exécution du contrat de travail

Lorsque cette phase de recrutement est passée, qu'en est-il alors de l'impact de ces objets connectés sur l'exécution du contrat de travail lui-même ? Tout d'abord, la problématique concernant la surveillance des salariés est envisagée maintenant depuis plusieurs années. En effet, la plupart des entreprises prévoient des systèmes permettant de suivre le salarié à distance par le biais de caméras de surveillance ou de système GPS. Cela est encadré très sérieusement par le code du travail notamment afin de protéger un des droits les plus fondamentaux qui soit qui est le droit à la vie

¹⁴ TARRIERE (M.), « Les vêtements de travail connectés c'est pour demain », *Companeo.com*, 21 mars 2014.

¹⁵ TILMAN (L.) et FRIMAT (P.), « TIC et santé au travail : la protection des données de santé », *JCP S*, 26 novembre 2013, n° 48, p. 24.

privée. La CNIL veille à ce respect par le biais d'un certain nombre de règles qui incombent aux responsables de tels systèmes.

Néanmoins, on constate que l'objet connecté quel qu'il soit permet la traçabilité du salarié. Peu importe sa fonction, le salarié peut être géolocalisé en toutes circonstances. La géolocalisation permet de manière générale de déterminer la position ou l'emplacement d'un objet ou d'une personne et génère donc automatiquement des données à caractère personnel¹⁶. Ces nouveaux objets sont alors d'autant plus porteurs de ce risque d'accroissement d'atteinte à la vie privée.

Prenons des utilisations concrètes afin d'illustrer nos propos. La montre connectée qui a pour finalité de recueillir à la fois les données de santé du salarié, ses mails ou toutes autres correspondances, va devoir être reliée à un système qui va permettre également la traçabilité du salarié. Le stylo connecté¹⁷, bien que son utilisation semble anodine, peut également avoir pour but de géolocaliser le salarié du moment que ce dernier le porte sur lui. Même enjeu pour les lunettes connectées et pour tout autre objet qui est relié à un système récoltant des données GPS.

Tous les développements en matière de TIC a un impact sur la santé du travailleur et notamment sur son stress. C'est un phénomène reconnu en droit du travail. En effet, depuis quelques années est apparue cette notion de stress au travail qui implique un déséquilibre entre ce que la personne se sent capable de faire et la perception qu'elle a des contraintes dont elle doit faire face. Avec la multiplication des TIC, cette notion est encore plus sensible. Il est recommandé aux entreprises d'envisager leur utilisation dans la limite de ne pas accentuer la charge de travail pesant sur le salarié. Or, avec l'apparition de ces nouveaux objets connectés, nous pouvons craindre une intensification du stress que ce dernier va pouvoir ressentir. On parle alors de « technostress ».

On peut considérer qu'il y a deux volets à ce phénomène de « technostress » :

Tout d'abord, la connexion à outrance du salarié va provoquer une certaine psychose chez lui puisqu'il va avoir conscience que ses faits et gestes sont analysés. Par exemple, lorsqu'il va prendre sa pause café ou sa pause cigarette, il va sans cesse imaginer qu'il est surveillé, épié et donc il est possible qu'il ressente une pression sur ses actions quotidiennes.

Puis, les nouveaux objets connectés nécessitent également une nouvelle organisation du travail. Le salarié va devoir s'adapter à ces nouvelles utilisations. Ça peut être un chamboulement considérable dans la vie professionnelle du salarié. Il va devoir répondre à des informations qui arrivent en masse et de manière plus rapide.

¹⁶ VIVANT (M.) et *alii*, *Lamy Droit du numérique – 2014*, Wolters Kluwer, 1^{ère} éd., France, 2014, § 4396 La géolocalisation.

¹⁷ GRAGO (J.), « Les 8 objets connectés qui vont révolutionner le travail », *Monkeytie.com*, 27 juin 2014.

Lorsque l'usage de ces objets va s'imposer à l'employeur et afin de limiter ce risque, l'adoption d'une « charte d'usage des TIC » a été d'ores et déjà validée par la Cour de cassation¹⁸.

L'apparition de ces nouveaux objets connectés va une fois de plus entraver la séparation entre vie privée et vie professionnelle. L'un des points clés du droit du travail dès l'apparition d'Internet a été de réglementer cet aspect. En effet, dès l'utilisation de la messagerie électronique, le législateur s'est empressé de déterminer avec précision le cadre de distinction entre usage privé et usage professionnel. Cette utilisation de l'internet des objets dans l'entreprise a deux conséquences importantes, d'une part, cela permet au salarié une meilleure autonomie, d'autre part, cette pratique est de nature à inciter l'employeur à exercer un contrôle accru de son employé.

Une nouvelle pratique commence à émerger. C'est le BYOD (Bring Your Own Device) qui littéralement se traduit par « apportez vos appareils personnels ». Dorénavant, les salariés utilisent leurs Smartphones, ordinateurs ou tablettes personnels sur leur lieu de travail, par confort et facilité. Afin d'éviter ces intrusions au sein de l'entreprise, la nouveauté vient des professionnels eux mêmes qui recommandent d'apporter leurs propres appareils sur leur lieu de travail¹⁹.

Déjà la distinction entre sphère privée et sphère professionnelle n'était pas aisée, mais avec ce phénomène le brouillage tend à se développer davantage. La circulation des données pour des appareils connectés non contrôlés accentue les risques, que ce soit en matière de protection de données personnelles du salarié que pour la sécurité de l'entreprise elle même. Le système dit « MDM » offre la faculté à l'employeur de préparer le terminal utilisé afin de sécuriser son contenu. Pour cela, il aurait alors accès à la totalité des données de l'appareil, sans possibilité de filtrage entre les informations professionnelles et les informations personnelles. C'est ainsi que des alternatives ont pu être envisagées. Des entreprises spécialisées ont alors prévu un espace hermétique au sein du terminal, dédié uniquement à son usage professionnel. Le contrôle par l'entreprise ne s'effectuera que pour ce compartiment²⁰.

Ce n'est pas la seule solution qui est préconisée. Le CYOD (Choose Your Own Device) littéralement « Choisi ton propre appareil » est un concept dans lequel l'employeur propose à son salarié, parmi une liste de terminaux choisis, son utilisation à des fins professionnelles, qu'il pourra utiliser également dans le cadre privé. Il a donc le choix d'accepter ou de refuser l'utilisation d'un appareil dont les données sont sécurisées. Une dernière possibilité a été envisagée : le COPE (Corporate Owned, Personaly Enabled). Dans ce cas, c'est l'entreprise qui achète et détient ces

¹⁸ FANTONI-QUINTON (S.) et LEBORGNE-INGALAERE (C.), « L'impact des TIC sur la santé au travail », *JCP S*, 26 novembre 2013, n°48, p.21.

¹⁹ Lettre innovation et prospective de la CNIL, n°7, juin 2014, p.1

²⁰ Lettre innovation et prospective de la CNIL, n°7, juin 2014, p.3.

appareils et qui les configure pour un usage professionnel. Le salarié peut en faire un usage privé. Dans les deux cas, même si les problématiques liées aux risques de sécurité de l'entreprise sont réduites, il semble que rien ne permette de protéger la perte ou le vol de l'objet connecté²¹.

Avec l'utilisation du BYOD, la politique de l'entreprise concernant cette pratique se doit d'être rigoureuse. Il est nécessaire de sensibiliser le salarié aux risques que cette pratique peut engendrer, que ce soit pour lui ou pour l'entreprise. Les règles ne doivent pas être définies au hasard. Il est impératif de trouver un juste équilibre afin d'éviter à la fois une surveillance quasi totalitaire et une trop grande liberté du salarié.

Le BYOD concerne davantage des objets connectés déjà utilisés depuis un certain nombre d'années comme les ordinateurs ou les Smartphones.

La sécurité de l'entreprise est également source de transformation lorsque de nouveaux objets connectés sont sur le point d'être intégrés dans le fonctionnement de l'entreprise. Ces nouveaux objets génèrent donc une quantité de données susceptibles de faire l'objet de piratage. Le risque est basé sur le « détournement de l'objet connecté ». Ainsi, il a été prouvé par des experts informatiques qu'il était possible de contrôler les freins d'un véhicule à distance ou encore d'avoir accès aux données personnelles des consommateurs (noms, adresses, numéros de téléphones, codes bancaires) d'un site de livraison. Comme nous l'avons cité précédemment la collecte ou le traitement des données personnelles sont protégés par la loi du 6 janvier 1978.

Néanmoins, les recours de l'entreprise qui est victime de piratage semblent restreints. Il en va de la responsabilité de celui qui utilise ce type de données. Un système d'obligations pèse sur lui afin de limiter ce risque de piratage. L'employeur doit notamment déclarer à la CNIL le système de collecte ou de traitement de données.

Des puces RFID (Radio Frequency Identification) sont également intégrées dans ces objets connectés. Le risque est que les sociétés fabricant ces appareils aient accès aux données personnelles des consommateurs. C'est ainsi que certains préconisent un droit à la désactivation de la puce. Ce droit doit être prévu par les fabricants eux mêmes.

Etant donné que le risque d'intrusion dans la vie privée des utilisateurs des objets connectés ne peut être contrôlé avec précision, un appel à l'éthique des fabricants est lancé. En effet, afin de préserver la confiance des consommateurs avec les nouvelles technologies, l'entreprise devra respecter un engagement de respect à la vie privée de ces derniers. Ce sera une manière de fidéliser son client.

²¹ PERNODET (T.), « BYOD, CYOD, COPE & Co : meilleurs « ennemis » du DSI ? », *Journaldunet.com*, 4 mars 2014.

L'employé aura donc tout intérêt à intégrer ces systèmes de protection au sein de ses objets connectés²².

Depuis le début de cette année 2015, se tient le salon des nouvelles technologies à Las Vegas qui permet aux entreprises de présenter leurs nouvelles innovations. On constate qu'au sein de ce salon, le risque de collecte des données personnelles par ces entreprises fabricantes est d'ores et déjà envisagé. La confiance avec les consommateurs qui détiennent leurs objets connectés est un point essentiel pour ces dernières. Pour la préserver, le concept de « security by design » apparaît. Il consiste à utiliser le recueillement de données personnelles des futurs clients seulement si nécessaire et à mettre en œuvre une politique de transparence et d'information de ces derniers²³.

c) La rupture du contrat de travail

Encore une fois, la connexion à outrance va accentuer les risques d'atteinte à la vie privée et d'enregistrement des données personnelles du salarié. Ce qui pourra à terme avoir pour but un licenciement trouvant sa source dans des causes discriminatoires.

En effet, une des conséquences de ces immixtions dans le recueillement des données personnelles que va causer ces objets connectés est la rupture du contrat de travail. Bien qu'une réglementation en matière d'usage excessif des TIC au travail est déjà prévue puisque par exemple le fait de se connecter de manière excessive à des fins personnelles est considéré comme une faute grave, justifiant un licenciement pour cause réelle et sérieuse²⁴.

Les objets connectés vont donc permettre une meilleure connaissance des faits et gestes du salarié. Au final, la conséquence de ces risques est que l'objet connecté va déceler encore plus facilement le moindre manquement du salarié. Les caméras portatives vont par exemple permettre de savoir que le salarié prend un appel personnel à son travail.

Certains objets connectés pourront donc servir à établir la preuve de la faute du salarié plus facilement. Ces objets qui à la base sont conçus dans le but d'améliorer la productivité d'une entreprise ou les conditions de travail, pourront se retourner contre son utilisateur et entraîner des conséquences qui sont néfastes pour ce dernier. Envisageons le cas des caméras portatives. Elles permettent d'assister le salarié et de collaborer avec plusieurs personnes en temps réel. Elles ont la faculté de s'accrocher à tout objet tels que les lunettes, les casques, les vêtements. Ainsi, suite à une

²² SILGUY (S.), « Les objets connectés, un risque pour la protection de nos données personnelles », *Revue Lamy Droit Civil*, 1^{er} octobre 2014, n°119, pp. 67-69.

²³ AUFFRAY (C.), « CES 2015 – Objets connectés : et les données personnelles dans tout cela ? », *Zdnet.fr*, 8 janvier 2015.

²⁴ TRICOIT (J-P), *op. cit.*, p. 14.

bavure filmée par un policier, Barack Obama dans un discours du 2 décembre 2014 a déclaré sa volonté de vouloir équiper tous les policiers de caméras portatives.

Mais attention, il faut être prudent car le recueillement de la preuve est très encadré. Si les formalités prévus par le droit du travail ne sont pas respectées, le procédé sera considéré comme clandestin et l'employeur ne pourra en aucun cas s'en servir pour licencier son salarié.

Avec toutes les données personnelles qui vont être récoltées, l'employeur pourra procéder à un licenciement discriminatoire. Par exemple, comme on a pu le constater précédemment avec le bracelet connecté du salarié qui permet de récolter ses données de santé, le licenciement sera basé sur une discrimination qui est l'état de santé du salarié.

Mais, si les formalités liées à l'utilisation de ces objets connectés sont respectées et que les causes de sont pas discriminatoires, les licenciements pour faute sont susceptibles de se multiplier.

Ça a pu déjà être le cas aux Etats-Unis avec l'utilisation du BYOD. En effet, une banque à New York a pu procéder aux licenciements de plusieurs de ses cadres au motif qu'ils n'avaient pas déclaré la perte de leurs Smartphones dans les 24 heures, faisant courir d'énormes risques de sécurité pour l'entreprise. De même, en Californie, la géolocalisation du Smartphone d'un avocat, utilisé dans le cadre du BYOD, a pu permettre de découvrir que ce salarié se rendait au golf au lieu d'être sur son lieu de travail²⁵. Les risques liés à la pratique du BYOD sont bien réels puisqu'il peut dans certains cas mener au licenciement de l'employé.

²⁵ SANYAS (N.), « BYOD : la surveillance de l'employé peut mener à un licenciement », *Zdnet.fr*, 4 décembre 2014.

II) L'état des lieux du droit du travail appliqué aux objets connectés

Au regard des nouvelles technologies, le droit du travail dispose d'un arsenal juridique étoffé et précis. Effectivement, depuis plus de vingt ans, les Nouvelles Technologies de l'Information et de la Communication (NTIC) ont envahi l'univers de l'entreprise. De ce fait, la relation de travail telle que conçue au XIX^{ème} siècle et XX^{ème} siècle a considérablement évolué. Les marges de manœuvres accordées aux salariés pour mener à bien leurs missions ont été totalement modifiées, mais, en contrepartie le pouvoir de contrôle de l'employeur s'est élargi. Face à ces phénomènes, le droit du travail semble apporter un certain nombre d'éléments de réponses **(A)**. Cependant, le droit du travail tel que conçu aujourd'hui doit-il être considéré comme suffisamment adapté ou doit-on envisager un droit du travail 2.0 ? **(B)**

A) L'application possible du droit du travail

Les problématiques posées par les objets connectés sont distinctes au regard du droit du travail, mais cinq problématiques essentielles se retrouvent : il s'agit de la géolocalisation facilitée que permet un objet connecté à l'instar des vêtements connectés (a), l'interception des données de santé facilitée à l'instar du bracelet connecté (b) et la surveillance accrue des correspondances professionnelles mais aussi privées à l'instar du bracelet connecté ou encore des lunettes connectées (c). Le droit du travail prévoit également des normes afin que le salarié soit protégé de l'utilisation des TIC dans l'entreprise, car celui-ci sera confronté à des problématiques telles que « technostress » (d) et le brouillage entre sa vie privée et sa vie professionnelle (e).

a) Application du droit concernant la problématique de la géolocalisation

La géolocalisation²⁶ est une technologie qui a pour but de déterminer la localisation plus ou moins précise d'un objet ou d'une personne par le biais d'un système GPS, d'un téléphone mobile et dès aujourd'hui grâce à un objet connecté, que le salarié pourrait porter directement sur lui. C'est l'exemple des lunettes connectées, du bracelet connecté, des vêtements connectés ou encore d'un objet tout à fait anodin comme un stylo connecté. Ce système permet un traitement de données à caractère personnel²⁷. Également, le fait pour un employeur de géolocaliser un salarié s'apparente incontestablement à de la surveillance. Ainsi, à partir des textes existants, il paraît opportun de dégager certains grands principes à respecter, qui pourraient être également appliqués aux objets connectés. En avant propos, il faut rappeler que l'employeur a le droit de contrôler l'activité de ses

²⁶ VIVANT (M.), *ibid.*

²⁷ GEITNER (M.), HERAUD (S.) et KASSAIAN (L.), Rapport « Les données personnelles », Table ronde Iredic 13 février 2015, Aix-en-Provence.

salariés pendant le temps de travail²⁸. Mais les moyens et techniques de contrôle clandestins sont illicites. Au regard du droit du travail, le recours à des moyens techniques de surveillance est licite si les conditions suivantes sont remplies :

Premièrement, l'employeur doit respecter le principe de proportionnalité²⁹. Cela signifie que la mesure de surveillance doit être justifiée par la nature de la tâche à accomplir par le salarié et proportionnée au but recherché (article L.1121-1 Code du travail). L'employeur n'a donc pas le droit de mettre en place une caméra uniquement parce qu'il souhaite contrôler les faits et gestes de ses salariés. Par analogie, il paraît vraisemblable que la même règle s'applique aux objets connectés : l'employeur ne pourra pas offrir à ses salariés un objet connecté « wearable » dans le seul but de contrôler ses moindres faits et gestes. L'employeur doit invoquer une raison précise afin de les équiper pour des raisons de sécurité par exemple. En cas de non-respect de ce principe, le salarié ou les délégués du personnel pourront saisir le juge prud'homal qui peut ordonner toute mesure afin de faire cesser l'atteinte aux droits et libertés individuelles des salariés (article L.2313-2 Code du travail).

L'employeur doit également effectuer une déclaration préalable à la CNIL³⁰. L'article 22 de la loi informatique et liberté du 6 janvier 1978 impose une déclaration préalable à la Commission nationale informatique et liberté (CNIL) des traitements automatisés de données à caractère personnel. L'employeur doit préciser les finalités du traitement qu'il entend mettre en place et doit assurer que la conservation de ces données ne sera pas excessive. L'absence de déclaration à la CNIL rend le dispositif illégal et toutes les sanctions fondées sur le traitement illégal les rendent nulles.

L'employeur doit de plus informer et consulter les représentants du personnel³¹. L'employeur doit informer et consulter le Comité d'entreprise ou à défaut, les délégués du personnel, sur les moyens mis en œuvre pour surveiller les salariés (Article L.2323-32 Code du travail). Tout licenciement prononcé sur la seule base du procédé de contrôle clandestin sera jugé sans cause réelle et sérieuse³². Par ailleurs, l'employé est fortement recommandé de consulter également le CHSCT préalablement à la mise en place du système dès lors qu'il peut avoir un impact sur les conditions de travail des salariés³³ (Article L.4612-8 Code du travail).

²⁸ LE PETITCORPS (K.), *Droit du Travail au Quotidien*, Groupe Liaisons, coll. Vivre le droit, 5218^{ème} éd., UE, septembre 2014, §132-15.

²⁹ LE PETITCORPS (K.), *ibid.*

³⁰ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

³¹ LE PETITCORPS (K.), *ibid.*

³² Cass. Ch. soc., 15 mai 2001, n° 99-42.219, *Société Transports frigorifiques européens c/ M.X et autres.*

³³ LE PETITCORPS (K.), *ibid.*

Finalement, l'employeur a l'obligation d'informer individuellement tous les salariés³⁴. Chaque salarié doit être informé sur le dispositif de surveillance mis en place (article L.1222-4 Code du travail), en vertu du principe de transparence et de loyauté. La Cour de cassation³⁵ a ainsi jugé que l'information doit avoir lieu même si les moyens de surveillance sont matériellement visibles³⁶. Dès lors un simple affichage n'apparaît pas être suffisant puisque l'information délivrée par l'employeur doit être individuelle à chaque salarié.

Concrètement, si l'employeur entend mettre en place un système de géolocalisation par le biais des objets connectés, celui-ci doit obligatoirement respecter les quatre étapes obligatoires détaillées ci-dessus. Autrement dit, l'employeur qui n'informe pas le comité d'entreprise et les salariés de l'existence de ces moyens de contrôle ne pourra pas les utiliser comme moyen de preuve.

La Cour d'appel de Dijon³⁷ a eu l'occasion de juger qu'un employeur ne pouvait pas utiliser les données de géolocalisation d'un salarié pour démontrer que son licenciement était justifié, dès lors que le dispositif en question n'avait pas été porté préalablement et individuellement à la connaissance de ce dernier et qu'il n'avait pas fait l'objet d'une déclaration à la CNIL³⁸.

b) Application du droit concernant la problématique liée aux données de santé

Les données sensibles sont celles qui font apparaître, directement ou indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses et l'appartenance syndicales des personnes. Elles sont relatives à la santé ou à la vie sexuelle de ces dernières³⁹. Ainsi d'après cette définition, les données de santé sont donc des données sensibles. Or, par principe la collecte et le traitement de ces données sont interdits par l'article 8 de la loi du 6 janvier 1978⁴⁰. Ainsi, l'employeur doit respecter le principe de proportionnalité et de pertinence des données⁴¹. Effectivement seules doivent être traitées les informations pertinentes et nécessaires au regard des objectifs poursuivis. En outre, comme le rappelle le Code du travail, la mise en place d'un dispositif de contrôle des salariés ne doit pas conduire à apporter de restrictions aux droits et libertés des personnes qui ne seraient pas proportionnées au but recherché et justifiées par l'intérêt légitime de l'entreprise (article L.1121-1 Code du travail).

De plus, l'employeur doit strictement respecter la place du médecin de travail au sein de son entreprise. Il résulte d'un faisceau d'indices réparti dans le Code de la santé publique et dans le

³⁴ LE PETITCORPS (K.), *ibid.*

³⁵ Cass. Ch. soc., 15 mai 2001, n° 99-42.219, *Société Transports frigorifiques européens c/ M.X et autres.*

³⁶ LE PETITCORPS (K.), *ibid.*

³⁷ CA Dijon, Ch. Soc., 14 sept. 2010, *Mille Services c/ Rémi X*

³⁸ VIVANT (M.), *ibid.*

³⁹ ANONYME, « Qu'est-ce qu'une donnée sensible ? », *cil.cnrs.fr*

⁴⁰ Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

⁴¹ Guides de la CNIL, Guide pour les employeurs et les salariés édition 2010

Code du travail que seul le médecin est habilité à disposer des données de santé dans l'enceinte de l'entreprise. Cela résulte de l'article R.4127-5 du Code de la santé publique que « *le médecin ne peut aliéner son indépendance professionnelle sous quelque forme que ce soit* », autrement dit le travail du médecin au sein de l'entreprise doit s'effectuer en toute indépendance. Egalement, le médecin du travail sera tenu par les mêmes obligations que tout autre médecin, à savoir l'obligation de secret professionnel et d'indépendance de ses décisions (article R.4127-95 Code de la santé publique). Qui plus est le Code du travail précise lui aussi que le médecin doit travailler de manière indépendante (article L.4623-8 Code du travail).

Pour finir, le Code du travail pose un principe de non discrimination, principe qui prévoit qu'aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire en raison de son état de santé (article L.1132-1 Code du travail). Ce principe est crucial concernant les données de santé car même si un employeur réussit à intercepter des données de santé de son salarié, que ce soit au stade de la procédure de recrutement, pendant la période de formation en entreprise ou encore pendant l'exécution du contrat de travail, l'employeur ne pourra pas fonder quelque sanction ou licenciement sur celles-ci.

c) Application du droit concernant les problématiques liées au contrôle des correspondances professionnelles

Les formalités à respecter concernant le contrôle des correspondances sont les mêmes que celles détaillées lors de la mise en place d'un système de géolocalisation à savoir : l'obligation pour l'employeur de respecter le principe de proportionnalité, la déclaration obligatoire à la CNIL, l'obligation pour l'employeur d'informer et consulter les représentants du personnel (CE et CHSCT) et l'obligation pour l'employeur d'informer individuellement tous les salariés. Cependant en plus de ces quatre obligations, l'employeur doit respecter un principe essentiel qui s'applique dès qu'il s'agit de protéger les correspondances, c'est le principe du secret des correspondances. Ce principe a été posé dans un arrêt Nikon du 2 octobre 2001⁴², arrêt considéré comme fondateur en la matière. La Cour de cassation a considéré que le salarié avait droit au respect de l'intimité de sa vie privée, laquelle implique en particulier le secret des correspondances. En application de ce principe, l'employeur ne peut donc, sans violation de cette liberté fondamentale, prendre connaissance du contenu des messages professionnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ce, même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur. A l'inverse, s'il s'agit d'un fichier ou d'un dossier considéré comme professionnel, l'employeur peut librement y accéder avec l'accord et sans la présence du salarié.

⁴² Cass, Ch. Soc., 2 octobre 2001, n° 99-42.942, *Nikon France c/ M.X*

d) Application du droit concernant les problématiques liées au « technostress »

Les TIC ont amplifié le stress au travail. Les salariés ont l'obligation de traiter des informations bien plus nombreuses et plus rapidement. Cela entraîne donc une charge de travail plus lourde, comme on a pu le constater dans les risques liés à l'utilisation de ces objets connectés. Pour protéger la santé et la sécurité du travailleur, un certain nombre de dispositifs a été mis en place.

L'employeur doit respecter une obligation de sécurité. Effectivement, le droit du travail encadre ce qui est relatif à la santé et à la sécurité de l'employé. Il est dit que l'employeur doit prendre les mesures nécessaires pour assurer la santé physique et mentale des travailleurs (article L4121-1 du Code du travail). Ce dispositif fait peser une obligation de sécurité sur l'employeur afin de garantir la protection de la santé et de la sécurité du travailleur. Le stress est pris en compte dans les accidents du travail ou dans la reconnaissance d'une maladie professionnelle.

La Cour de cassation a eu l'occasion de reconnaître la faute inexcusable de l'employeur à la suite d'une surcharge de travail de son salarié ayant provoqué un infarctus.

L'instance représentative du personnel compétence pour connaître les problématiques liées au « technostress » est le CHSCT. Le rôle du CHSCT est de protéger la sécurité et la santé des travailleurs. Pour cela, il analyse les risques professionnels auxquels peuvent être exposés les travailleurs. Il mène des actions de sensibilisation et d'information en matière de harcèlement moral. Il analyse également les causes des accidents de travail ou des maladies professionnelles. Cette instance est donc susceptible de contribuer à limiter voire à éviter le stress du salarié qu'il ressent du fait de l'utilisation nécessairement intense de ces nouveaux objets connectés.

Finalement, il est recommandé que l'employeur mette en place des chartes d'usage des TIC.

Un avis rendu par le Conseil économique, social et environnemental du 14 mai 2013 a précisé la nécessité de promouvoir le bon usage des TIC dans l'entreprise. Pour cela, la mesure la plus rapide et la plus efficace est de mettre en place une charte d'usage des TIC. Elle doit permettre d'encadrer cette utilisation pour notamment éviter un trop grand stress pour le salarié engendré par les TIC.

La Cour de cassation⁴³ a déjà validé l'opposabilité de telle charte du moment qu'elle est intégrée au règlement intérieur de l'entreprise et qu'elle respecte les dispositions légales.

Finalement, le salarié est susceptible de se voir appliquer le droit à la déconnexion potentiellement prévu par l'employeur. Le droit à la déconnexion consiste à une gestion automatisée de déconnexion des appareils électroniques et ce à des heures précises. Il fait l'objet d'une régulation interne à chaque entreprise. Même si les TIC ne sont pas considérées comme une chose négative pour les salariés, il est nécessaire de les encadrer pour éviter ce brouillage entre vie privée et vie

⁴³ Cass. Soc. 15 décembre 2010 n°09-42.691 *M.X c/ société Coca-cola*

professionnelle. Par ce droit à la déconnexion, les instances du travail veulent éviter le « burn out » ou l'immixtion trop forte dans la vie privée du salarié⁴⁴.

Contrairement à ce que l'on pourrait croire cette notion n'est pas nouvelle. En effet, dès l'apparition d'Internet au sein de l'entreprise, le droit à la déconnexion a pu être envisagé pour éviter qu'avec l'utilisation des TIC il y ait une interpénétration entre la vie professionnelle et la vie personnelle. Cela avait pour support l'article 8 de la CEDH et l'article 9 du code civil qui prévoient le droit au respect de sa vie privée. Ce droit n'était pas évoqué de manière explicite dans l'ancien code du travail. Cependant, il était bien prévu un repos quotidien pour les salariés, afin de préserver leurs vies privées. Comme aujourd'hui, il était préconisé d'avoir recours à une réelle réglementation dans l'entreprise à ce sujet⁴⁵.

Un accord vient d'être signé entre le patronat d'ingénierie et de conseil et des bureaux d'études avec la CFDT et la CGT le 1^{er} avril 2014, reconnaissant ce droit à la déconnexion et plus précisément « une obligation de déconnexion des outils de communication à distance ». Cet accord est venu se mettre en conformité avec les règles françaises et européennes relatives aux durées de repos du travailleur⁴⁶.

Toujours est-il que le développement des TIC et notamment des nouveaux objets connectés constitue un risque professionnel établi et non équivoque sur la santé du travailleur.

e) Application du droit concernant les problématiques liées au brouillage entre la vie privée et la vie professionnelle

Comme on l'a vu précédemment, l'usage des TIC a pour conséquence une immixtion de la vie professionnelle du salarié dans sa vie privée et vice versa. Selon une étude récente⁴⁷, les salariés ont de plus en plus de mal à distinguer leur vie privée et leur vie professionnelle. D'après une étude réalisée, 89 % des salariés consultent leurs mails professionnels sur leur temps privé et 93% pendant leurs congés. L'usage des nouvelles technologies engendre cette tendance d'effectuer des tâches professionnelles dans le cadre privé. De ce fait, les demandes de requalification en heures supplémentaires sont nombreuses. Ce brouillage est d'autant plus présent avec l'utilisation du BYOD.

⁴⁴ NICOLET (S.), « Qualité de vie au travail : transformer la contrainte en opportunité », *Les Cahiers du DRH - 2014*, 1^{er} décembre 2014, n°215, p. 17.

⁴⁵ GOURION (P-A.) et RUANO-PHILIPPEAU (M.), *Le droit de l'Internet dans l'entreprise*, L.G.D.J, coll. Systèmes, 1^{ère} éd., Paris, 2003, p. 106.

⁴⁶ ANONYME, « Courriels, SMS, téléphone : Syntec reconnaît le droit à la déconnexion », *RLDI*, 1^{er} mai 2014, n°104

⁴⁷ BENSOUSSANS (A.) « Syntec et le droit à la déconnexion reconnu aux salariés », *alain-bensoussans.com*, 11 septembre 2014.

Pour palier à ce phénomène, les dispositifs mis en place sont les suivants :

Tout d'abord le temps de travail du salarié est encadré, en effet le temps de travail effectif du salarié est encadré par le Droit du travail. L'article L.3121-1 du code du travail dispose que « *la durée du travail effectif est le temps pendant lequel le salarié est à la disposition de l'employeur et se conforme à ses directives sans pouvoir vaquer librement à des occupations personnelles* ».

Puis, le salarié n'a pas d'obligation de répondre à son employeur en dehors de ses heures de travail. Effectivement, la jurisprudence est également venue préciser que ne constitue pas une faute le salarié qui ne réceptionne pas l'appel téléphonique de son employeur pendant son temps de repos. La Cour de cassation dans son arrêt du 17 février 2004 a indiqué que le licenciement pour faute grave basé sur de tels motifs n'est pas justifié.

Ensuite, il est conseillé que l'employeur promeuve les chartes d'usage des TIC, celles-ci permettent de préciser les tâches qui relèvent de la sphère professionnelle et qui doivent être effectuées pendant le temps de travail effectif du salarié. Ce qui est censé permettre d'éviter au mieux ces brouillages.

Finalement, il est conseillé que l'employeur applique un droit à la déconnexion.

Le même sentiment de harcèlement numérique se retrouve dans ce problème de brouillage entre vie professionnelle et vie privée. C'est pourquoi, le droit à la déconnexion s'envisage également en la matière. Ce droit semble permettre d'équilibrer le rapport vie privée et vie professionnelle.

B) Vers l'émergence d'un droit du travail 2.0 ?

En premier lieu, nous pouvons commencer par un constat assez général qui est que tous les secteurs de l'emploi vont être bouleversés par l'apparition de nouveaux objets numériques. Cette transformation va toucher de plus en plus d'entreprises puisque 40 à 70 % d'entre elles sont favorables à ces innovations.

Déjà un groupe de travail « Digiworks » en 2013 était chargé de réfléchir à l'évolution de la place du salarié face aux nouvelles technologies. Le résultat qui en découle est qu'une nouvelle manière de travailler ainsi qu'une nouvelle unité de temps, de lieu et d'espace vont émerger et sont à prendre en considération par les instances du travail.

Un nouveau profil voit le jour. Il s'agit du slasher qui désigne le travailleur qui ne s'épanouit pas dans son travail mais qui permet de le faire vivre et qui trouve une passion qui le motive. Son emploi est davantage perçu comme un gagne pain. C'est la tendance qu'on voit se développer actuellement. Avec ce brouillage entre vie privée et vie professionnelle, ce statut émerge.

Au sein de l'organisation du travail elle-même, de nouveaux changements commencent à apparaître. Tout d'abord, le dialogue avec le personnel ainsi que la régulation interne des entreprises divergent de plus en plus afin de s'adapter au mieux à ce nouveau marché high tech. On constate également qu'avec ces nouvelles formes d'échanges numériques, le mode de valorisation du travail est différent. En effet, est opérée une distinction entre le travail créatif et la simple fonction d'exécution (tâche administrative).

Au regard de cet phénomène de « technostress », une nouvelle tendance a d'ores et déjà été envisagée par les entreprises. Il s'agit de capteurs physiologiques placés sur le salarié permettant d'indiquer son niveau de stress et d'anxiété⁴⁸.

A partir de ces nouveaux phénomènes, nous pouvons constater qu'à travers l'émergence de l'Internet des objets, l'organisation ainsi que les conditions de travail sont susceptibles de connaître de profondes mutations dans les années à venir.

En second lieu, les risques sur les données personnelles du salarié ainsi que sur la sécurité de l'entreprise sont indéniables avec l'apparition de ces nouveaux objets connectés. Cela va avoir pour conséquence d'entraîner un changement considérable dans les habitudes professionnelles des travailleurs.

⁴⁸ SUSSAN (R.) et GUILLAUD (H.), « Quel avenir pour le travail dans un monde numérique ? », *Lemonde.fr*, 19 novembre 2014.

Les objets connectés ne sont pas perçus comme de simples gadgets du moment qu'ils génèrent des contenus à caractère personnel. En effet, ils permettent de renseigner sur la géolocalisation du salarié, sur son état de santé, sur les données personnelles de manière générale qu'il s'agisse du salarié ou de l'entreprise.

Afin de minimiser tous ces risques, la politique de l'entreprise se doit d'être repensée à tous ces égards et de manière sérieuse. « L'internet of things » est considéré comme une véritable révolution à laquelle vont devoir faire face les entreprises⁴⁹.

En dernier lieu, on constate que notre droit du travail est très dense. En effet, le code du travail contient de nombreuses dispositions en matière de protection du salarié, aussi bien concernant la vie privée que les licenciements. Ces dispositions viennent s'ajouter aux formalités que doivent accomplir les employeurs notamment en matière de TIC. Plusieurs acteurs sont sollicités comme la CNIL, le CE et le CHSCT. On ne peut douter que ces nouveaux objets connectés feront aussi l'objet d'un traitement strict, afin de pouvoir être intégrés dans ces entreprises.

⁴⁹ MELIA (L.), « Les objets connectés et l'entreprise, Big Gadget », *lenouveleconomiste.fr*, 8 octobre 2014.

CONCLUSION

Pour conclure, la question qui se pose alors est si avec l'intégration de ces nouveaux objets connectés dans l'entreprise, on doit aller vers la reconnaissance explicite d'un droit à la déconnexion. Au regard des développements en la matière, on constate que les entreprises intègrent déjà ce droit au sein de leur régulation interne, au sein des chartes d'entreprises notamment. Cette mesure est susceptible de se répandre de plus en plus au regard de la multiplication des objets connectés qui commence déjà à apparaître. Ces chartes sont déjà opposables dans un litige. On peut éventuellement envisager que ce droit à la déconnexion fasse l'objet d'une reconnaissance à part entière dans le code du travail.

Après cette étude, nous pouvons constater que les nouveaux usages qu'entraînent inévitablement les objets connectés vont devoir faire l'objet d'une adaptation au sein de l'entreprise. Sa politique interne semble devoir être axée sur l'utilisation précise de ces nouveaux objets. La sensibilisation à tous ces risques va devoir être prise en compte, afin d'en informer le salarié. Le personnel va être obligé de travailler différemment. L'entreprise fabricante doit envisager la conception de l'objet de manière à préserver la sécurité des données personnelles et garantir la confiance avec les consommateurs.

Néanmoins, au niveau du droit, ces chamboulements font naître la question de la nécessité de créer un nouveau droit du travail numérique, qui serait adapté entièrement à l'utilisation de « l'Internet of things ». Il semblerait que depuis l'apparition d'Internet, les problématiques liées à la surveillance des salariés, à leur traçabilité, à la protection des données personnelles, à l'équilibre entre sphère privée et sphère professionnelle soient récurrentes. Il paraît évident que les nouveaux objets connectés vont engendrer le même type de problématiques, qui ne sont en réalité pas nouvelles. C'est ainsi, qu'une refonte totale du droit du travail n'est pas légitime. En effet, le droit social semble paré à répondre à ces problématiques avec le droit existant, qui reste complet dans ces domaines.

En résumé, au niveau interne, la politique des entreprises va devoir être inévitablement repensée. Cependant, si l'adaptation du droit semble évidente, sa réorganisation complète apparaît comme étant inopportune.

BIBLIOGRAPHIE

I. OUVRAGES GENERAUX ET SPECIALISES

GOURION (P-A.) et RUANO-PHILIPPEAU (M.), *Le droit de l'Internet dans l'entreprise*, L.G.D.J, coll. Systèmes, 1^{ère} éd., Paris, 2003, 156 p.

LE PETITCORPS (K.), *Droit du Travail au Quotidien*, Groupe Liaisons, coll. Vivre le droit, 5218^{ème} éd., UE, septembre 2014, 1534 p.

VIVANT (M.) et alii, *Lamy Droit du numérique – 2014*, Wolters Kluwer, 1^{ère} éd., France, 2014, 1972 p.

II. ARTICLES

Articles juridiques

ANONYME, « Courriels, SMS, téléphone : Syntec reconnaît le droit à la déconnexion », *RLDI*, 1^{er} mai 2014, n°104.

FANTONI-QUINTON (S.) et LEBORGNE-INGALAERE (C.), « L'impact des TIC sur la santé au travail », *JCP S*, 26 novembre 2013, n°48, pp. 16-21.

NICOLET (S.), « Qualité de vie au travail : transformer la contrainte en opportunité », *Les Cahiers du DRH – 2014*, 1^{er} décembre 2014, n°215, pp.13-21.

POIDEVIN (B.) et VANCOSTENOBLE (C.), « Drones : Responsabilité pénale, vie privée et données personnelles », *Expertises des systèmes d'information*, Avril 2014, n° 390, pp. 141-144.

SILGUY (S.), « Les objets connectés, un risque pour la protection de nos données personnelles », *Revue Lamy Droit Civil*, 1^{er} octobre 2014, n°119, pp. 66-69.

TILMAN (L.) et FRIMAT (P.), « TIC et santé au travail : la protection des données de santé », *JCP S*, 26 novembre 2013, n°48, pp. 22-26.

TRICOIT (J-P.), « Recrutement, rupture du contrat de travail et TIC », *JCP S*, 1^{er} octobre 2013, n°40, pp. 9-14.

Articles non juridiques

AUFFRAY (C.), « CES 2015 – Objets connectés : et les données personnelles dans tout cela ? », *Zdnet.fr*, 8 janvier 2015.

BENSOUSSANS (A.) « Syntec et le droit à la déconnexion reconnu aux salariés », *alain-bensoussans.com*, 11 septembre 2014

BISEUL (X.), « Demain les salariés seront bardés d'objets connectés », *01net*, 9 décembre 2014

BISEUL (X.), « En 2015, les entreprises seront à l'avant-garde de l'équipement digitale », *www.01net.com*, 5 février 2015

BLOCH (M.), « Cinq usages méconnus des drones », *francetvinfo.fr*, 28 mai 2013

CLAPUD (A.), « PSA s'offre la plus grosse imprimante 3D du marché », *01net.com*, 10 juin 2013

DRAGO (J.), « Les 8 objets connectés qui vont révolutionner le travail » *monkey-tie.com*, 27 juin 2014

GRALLET (G.), « le vêtement connecté, cette nouvelle peau électronique », *lepoint.fr*, 19 novembre 2014

MADJOUB (R.) « Des puces électroniques implantées sous la peau d'employés suédois » *Kobini.com*, 5 février 2015

MELIA (L.), « Les objets connectés et l'entreprise, Big Gadget », *lenouveleconomiste.fr*, 8 octobre 2014.

PERNODET (T.), « BYOD, CYOD, COPE & Co : meilleurs « ennemis » du DSI ? », *Journaldunet.com*, 4 mars 2014.

RONFAUT (L.), « La SNCF équipe ses contrôleurs de Google Glass », *lefigaro.fr*, 24 octobre 2014

ROZIER (U.), « Marissa Mayer offre un bracelet connecté Jawbone Up a ses employés », *frandroid.com*, 13 juillet 2013

SANYAS (N.), « BYOD : la surveillance de l'employé peut mener à un licenciement », *Zdnet.fr*, 4 décembre 2014.

SUSSAN (R.) et GUILLAUD (H.), « Quel avenir pour le travail dans un monde numérique ? », *Lemonde.fr*, 19 novembre 2014.

TARRIERE (M.), « Les vêtements de travail connectés c'est pour demain », *Companeo.com*, 21 mars 2014.

III. RAPPORTS

CHOUX (L.), ESTRUCH (L.) et GONZALVES (S.), rapport sur « La santé connectée », Table ronde Iredic, 13 février 2015, Aix-en-Provence.

GEITNER (M.), HERAUD (S.) et KASSAIAN (L.), Rapport « Les données personnelles », Table ronde Iredic 13 février 2015, Aix-en-Provence.

Guides de la CNIL, Guide pour les employeurs et les salariés édition 2010

Lettre innovation et prospective de la CNIL, n°7, juin 2014, p.1

Lettre innovation et prospective de la CNIL, n°7, juin 2014, p.3.

IV. LOI

Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

V. JURISPRUDENCES

CA Dijon, Ch. Soc., 14 sept. 2010, *Mille Services c/ Rémi X*

Cass. Ch. soc., 15 mai 2001, n° 99-42.219, *Société Transports frigorifiques européens c/ M.X et autres.*

Cass, Ch. Soc., 2 octobre 2001, n° 99-42.942, *Nikon France c/ M.X*

Cass. Soc. 15 décembre 2010 n°09-42.691 *M.X c/ société Coca-cola*

VI. SITES INTERNET

<http://www.legifrance.gouv.fr/>

<http://www.cnil.fr/>

<http://www.lemonde.fr/>

<http://www.01net.com/>

<http://www.zdnet.fr/>

<http://www.lepoint.fr/>

<http://www.lefigaro.fr/>

<http://www.dalloz.fr/>

<http://www.lamyline.lamy.fr/>

Table des matières

| | |
|--|-----------|
| Remerciements | 1 |
| SOMMAIRE | 2 |
| Introduction | 3 |
| I. L’impact des objets connectés sur l’organisation du travail dans l’entreprise | 5 |
| A. L’impact positif des objets connectés sur l’organisation et les conditions de travail | 5 |
| <i>a) Liste non exhaustive des objets connectés utilisés dans le monde du travail</i> | <i>5</i> |
| <i>b) Les aspects positifs des objets connectés</i> | <i>6</i> |
| B. L’impact négatif des objets connectés sur l’organisation et les conditions de travail | 7 |
| <i>a) L’embauche</i> | <i>7</i> |
| <i>b) L’exécution du contrat de travail</i> | <i>8</i> |
| <i>c) La rupture du contrat de travail</i> | <i>12</i> |
| II. L’état des lieux du droit du travail adapté aux objets connectés | 14 |
| A. L’application possible du droit du travail | 14 |
| <i>a) Application du droit concernant la problématique de la géolocalisation</i> | <i>14</i> |
| <i>b) Application du droit concernant la problématique liée aux données de santé</i> | <i>16</i> |
| <i>c) Application du droit concernant les problématiques liées au contrôle des correspondances professionnelles</i> | <i>17</i> |
| <i>d) Application du droit concernant les problématiques liées au « technostress »</i> | <i>18</i> |
| <i>e) Application du droit concernant les problématiques liées au brouillage entre la vie privée et la vie professionnelle</i> | <i>19</i> |
| B. Vers l’émergence d’un droit du travail 2.0 ? | 21 |
| CONCLUSION..... | 23 |

BIBLIOGRAPHIE 24

Table des matières 27