AIX-MARSEILLE UNIVERSITE

FACULTE DE DROIT ET DE SCIENCE POLITIQUE

INSTITUT DE RECHERCHE ET D'ETUDES EN DROIT DE L'INFORMATION ET DE LA COMMUNICATION

MOBILITÉ, TERMINAUX CONNECTÉS ET HYPER-CONNEXION DES SALARIÉS

Approche en droit comparé français et italien

Mémoire pour l'obtention du Master 2 « Droit des médias et des télécommunications »

PRÉSENTÉ PAR

Sandrina GONCALVES SILVA

SOUS LA DIRECTION DE M. PHILIPPE MOURON

Maître de conférences à l'Université d'Aix-Marseille

Année universitaire 2014/2015

AIX-MARSEILLE UNIVERSITE

FACULTE DE DROIT ET DE SCIENCE POLITIQUE

INSTITUT DE RECHERCHE ET D'ETUDES EN DROIT DE L'INFORMATION ET DE LA COMMUNICATION

MOBILITÉ, TERMINAUX CONNECTÉS ET HYPER-CONNEXION DES SALARIÉS

Approche en droit comparé français et italien

Mémoire pour l'obtention du Master 2 « Droit des médias et des télécommunications »

PRÉSENTÉ PAR

Sandrina GONCALVES SILVA

SOUS LA DIRECTION DE M. PHILIPPE MOURON

Maître de conférences à l'Université d'Aix-Marseille

Année universitaire 2014/2015

« Hyper-connecté, hyper-mobile, il n'est ni d'ici ni d'ailleurs. Homme de réseaux, il se dissout en eux, et n'a d'autres racines que celle de l'algorithme. Il n'est pas du monde des humains mais flotte au-dessus de lui, porté par l'air du temps « Anytime AnyWhere AnyDevice Anycontent[1]. » C'est l'histoire d'un homme « sans territoire » qui n'est plus tout à fait un Homme (….) ; c'est l'histoire d'un Homme…sans histoire.[2] ».

Patrice ADAM

[1] En français : « tout le temps, partout, sur tout support et tout contenu » ou mobiquité, issue de la fusion des termes mobilité et ubiquité, désigne la capacité d'un individu en situation de mobilité qui peut se connecter à un réseau sans contrainte de temps, de terminal ou de localisation.

[2] ADAM (P.), « SMS, vie privée et portable professionnel : histoire (courte) d'un Homme « sans territoire », *Revue Droit du travail Dalloz*, n°3, p.191-194

REMERCIEMENTS

Mon premier remerciement s'adresse à Monsieur Philippe MOURON pour avoir accepté de diriger ce mémoire de fin d'études. Je le remercie pour sa disponibilité, sa gentillesse, son enthousiasme et ses nombreux conseils prodigués au cours de ces deux années de Master au sein de l'université d'Aix-Marseille. Je tiens aussi à remercier l'équipe enseignante de l'IREDIC, en particulier M. Isar et M. Laurie qui m'ont permis d'intégrer ce Master.

Je remercie aussi M. Jean-Luc Molins du syndicat Ugict-CGT qui a accepté de répondre à mes questions sur la thématique de l'hyper-connexion à travers un entretien téléphonique et qui m'a transmis un dossier de presse très complet, afin de compléter ce mémoire.

Par ailleurs, je remercie particulièrement l'ensemble de ma famille qui m'a soutenu tout au long de mon cursus universitaire en France, ainsi que pendant la rédaction de ce mémoire en Italie. Ils ont su trouver les mots justes pour m'accompagner, malgré la distance.

Je remercie aussi les personnes rencontrées au cours de mon expérience à Rome qui m'ont également apporté leur soutien au cours de cette période, ainsi que mes amis en France, qui ont été présents pour moi, particulièrement Mademoiselle Mélanie Da Silva.

Mes remerciements s'adressent ensuite à l'ensemble de l'équipe de la bibliothèque de l'Ecole française de Rome qui m'a permis de m'inscrire au sein de leurs locaux au Palais Farnèse, lieu incroyable chargé d'histoire, au sein duquel j'ai pu avoir l'opportunité de rédiger, en grande partie, ce mémoire.

Enfin, une pensée particulière pour mes très chers italiens et très probablement futurs brillants historiens je l'espère : mon amie Mademoiselle Serena RUBINELLI et Monsieur Dennj SOLERA, à qui je souhaiterai adresser mes derniers remerciements.

TABLE DES ABREVIATIONS

ANACT	Agence Nationale pour l'amélioration des conditions de travail
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
BYOD	Bring Your Own Device
CA	Cour d'appel
Cass.	Cour de cassation
Cass.crim	Cour de cassation, chambre criminelle
Cass.soc	Cour de cassation, chambre sociale
CCE	Communication Commerce Electronique
CEDH	Cour Européenne des Droits de l'Homme
CNIL	Commission Nationale de l'Informatique et des Libertés
CYOD	Choose Your Own Device
COPE	Corporate-Owned-Personally-Enabled
CPI	Code de la propriété intellectuelle
IUT	Union internationale des télécommunications
OIT	Organisation Internationale du Travail
RPS	Risques psychosociaux
SIAE	Società italiana degli Autori ed Editori
TIC	Technologies de l'information et de la communication
UGICT	Union générale des Ingénieurs, Cadres, et Techniciens

SOMMAIRE

PARTIE 1.

La mise en place de terminaux mobiles et connectés dans le milieu professionnel : un choix à hauts risques pour l'employeur face aux enjeux juridiques

Chapitre 1. La remise en cause de la classification et de la sécurité des données personnelles et professionnelles

Section 1. La problématique de la porosité des données personnelles et professionnelles

Section 2. La problématique de la sécurité et de la confidentialité des données personnelles et professionnelles

Chapitre 2. L'atteinte aux droits de propriété intellectuelle du fait de l'usage illicite d'un terminal

Section 1. Les usages en termes de propriété littéraire et artistique

Section 2. Les usages illicites en matière de logiciel

PARTIE 2.

La mise en place de terminaux mobiles et connectés dans le milieu professionnel : la nécessité d'un encadrement juridique face à une politique à risques pour le salarié

Chapitre 1. Vers une dangereuse réduction de la frontière entre les sphères professionnelle et personnelle

Section 1. Le risque d'atteintes à la vie privée accru par la mise en place de terminaux mobiles et connectés

Section 2. Le risque d'atteintes à la vie privée renforcée par la cyber surveillance et la géolocalisation intensive

Chapitre 2. Vers une consécration opportune d'un droit à la déconnexion face aux risques liés à l'exigence d'hyper productivité

Section 1. Les risques psychosociaux

Section 2. La pertinence de la déconnexion : une utopie face à l'hyper-connexion, « mal du siècle »

INTRODUCTION

« Le salon familial n'est pas un bureau professionnel. Le grand changement du 21e siècle est l'irruption des TIC, en particulier Internet qui permet d'avoir le don d'ubiquité. Nombreux sont aujourd'hui les salariés qui travaillent dans ce que les juristes considéraient comme le graal de l'intimité : leur home[3]» écrivait Jean-Emmanuel Ray, il y a quelques années.

Face aux nouvelles pratiques et aux nouvelles formes d'organisation du travail, le terme « ubiquité » qui semblait bien adapté auparavant semble être moins approprié, voir presque « dépassé ». Dorénavant le terme « mobiquité » semble davantage convenir. Ainsi, le terme « mobiquité », issu de la fusion entre les notions de mobilité et ubiquité est maintenant fréquemment utilisé. En effet, on assiste à une « confusion » de plus en plus importante entre la sphère privée propre à chaque salarié et la sphère professionnelle. Les terminaux mobiles et connectés permettent aux salariés de passer des appels « personnels » sur leur lieu de travail, tandis que ces mêmes outils offrent dorénavant aux salariés la possibilité de travailler également depuis leur domicile. Par ailleurs, ces outils accompagnent les salariés fréquemment et quasiment en permanence. En outre, incontestablement aujourd'hui, nous sommes quasiment tous hyper-connectés, non seulement dans notre vie personnelle (par le biais des nombreux réseaux sociaux, du smartphone dont les individus se séparent rarement ainsi que par le biais des applications) mais également dans notre vie professionnelle. Certes, il s'agit bien entendu d'une généralité. Toutefois, dans le cadre de ce mémoire, la problématique de l'hyper-connexion sera abordée, et nous verrons pourquoi celle-ci peut soulever des difficultés. Ainsi, la limite entre les deux sphères personnelle et professionnelle est difficilement établie, et les propos de Jean-Emmanuel Ray cités ci-dessus semblent pouvoir être confirmés de nos jours. En effet, le salarié aujourd'hui ne se contente plus de travailler « entre les murs » de son entreprise.

Par ailleurs, il apparaît également aujourd'hui que l'entreprise peut tenir « dans la poche » du salarié, et ce notamment, par le biais d'outils qui se sont énormément développés ces dernières années, qui ont favorisé cette évolution et qui ont connu une ascension fulgurante : les smartphones ainsi que les tablettes. De nos jours, les salariés travaillent au sein de leur entreprise, mais également parfois au sein de leur domicile comme nous l'avons précédemment évoqué. A ces comportements qui ne sont pas nouveaux, de nouvelles

[3] Home (anglais) : maison

pratiques se sont ajoutées qui aujourd'hui parfois inquiètent. En effet, il convient de souligner que de plus en plus de salariés apportent sur leur lieu de travail, leurs propres terminaux « mobiles » ou « connectés ». Ce phénomène d'actualité est couramment appelé BYOD (Bring Your Own Device) que l'on doit traduire en français par l'expression suivante : « *apportez votre propre matériel* », selon la Commission générale de terminologie et de néologie française[4]. C'est précisément ce phénomène qui m'a particulièrement interpelé. Selon un sondage réalisé en 2011 pour le compte de la CNIL, seulement 44% des possesseurs de smartphones ont un usage « exclusivement personnel » de leur outil. Ainsi, il apparaît que l'usage mixte est de plus en plus fréquent[5]. En outre, dans son rapport annuel en 2014, le Conseil d'Etat a rappelé les principes les plus importants en matière d'outils de travail mobiles et connectés mis à la disposition des salariés[6].

J'ai souhaité consacrer mon mémoire de fin d'études à une problématique qui m'a semblé dans l'actualité et qui me tient à cœur en lien avec l'insertion et l'utilisation des nouvelles technologies dans le milieu professionnel. J'ai donc fait le choix de m'intéresser à la mobilité et à l'hyper-connexion. En effet, dans le cadre de ce mémoire, nous verrons qu'il semble exister un lien fort entre ces deux notions. J'ai choisi d'aborder ce thème car depuis quelques années j'ai pris conscience que de plus en plus fréquemment, les employeurs de nombreuses personnes dans mon entourage mettaient à leur disposition des terminaux mobiles ou connectés ou bien qu'ils leur permettaient d'apporter leurs propres terminaux sur leur lieu de travail. J'ai alors commencé à faire des recherches sur cette problématique, qui comme je m'en doutais, soulève de nombreux problèmes juridiques. Très rapidement, j'ai compris qu'il s'agissait d'un véritable enjeu pour nombreux d'entre nous, à la fois pour les salariés, mais également pour les employeurs. En débutant mes recherches, je me suis principalement intéressée à la problématique du Bring Your Own Device (BYOD). Il s'agit ici d'un acronyme que beaucoup de personnes ne connaissent pas alors que celui-ci est parfois mis en place dans leur milieu professionnel. J'espère pouvoir apporter au sein de mon mémoire des éléments de réponse aux différentes et nombreuses problématiques juridiques soulevées par le BYOD. C'est la démarche que j'ai souhaité menée dans le cadre de ce mémoire.

[4] Avis publié au Journal Officiel le 24 mars 2013
[5] La lettre innovation et prospective de la CNIL, Intimité et vie privée du travailleur connecté : BYOD, capteurs, sécurité des données dans l'entreprise numérique,n°7, juin 2014, p.2
[6] Etude annuelle 2014 du Conseil d'Etat, « Le numérique et les droits fondamentaux », Edition La Documentation Française, Etudes et documents, septembre 2014

Le BYOD est une problématique qui aujourd'hui concerne non seulement les entreprises, mais également le secteur public ou encore les écoles. En effet, dans les pays où les élèves sont équipés, la problématique de la mise en place du BYOD se pose aujourd'hui. Ainsi, c'est déjà par exemple le cas en France, où le « BYOD » fait déjà beaucoup parler de lui. Néanmoins, il existe encore véritablement un manque d'information sur un sujet pourtant d'actualité. Il me semble aujourd'hui impératif de définir un cadre juridique pour ce type de mobilité. Parmi les outils de travail les plus fréquemment utilisés dans le cadre de la mobilité, on trouve bien entendu « le smartphone », qualifié par certains de « prothèse de vie ». Il est possible de s'interroger : comment expliquer le développement de ce type de mobilité ? Comme l'ont souligné certains auteurs, puisque « le bureau peut s'inviter à la maison par le biais d'un appel ou d'un message, la maison doit également pouvoir, dans l'esprit de certains salariés, faire irruption au bureau[7] ».

Préalablement, il me paraît nécessaire de définir les termes du sujet afin de mieux appréhender mon sujet de mémoire. En effet, tout d'abord, je souhaiterais indiquer que le terme « mobilité » peut faire l'objet de nombreuses acceptions. Pour certains, il ne conviendrait pas au BYOD, car dans ce contexte, c'est le salarié qui apporte son propre outil mais la majorité de la doctrine s'accorde à considérer que le BYOD correspond à la « mobilité professionnelle ». Bien qu'au départ le terme de mobilité était traditionnellement utilisé pour faire référence à la « mobilité des personnes », ce terme est désormais également employé eu égard au développement des outils mobiles et connectés[8]. Selon certains, le terme de « mobilité » ne pourrait se justifier car il renvoie davantage à une « sortie d'équipement », tandis que le BYOD correspondrait plutôt à l'accueil d'équipements[9]. Ainsi, il apparait que le terme même de « mobilité » peut diviser. Il est intéressant de souligner que le BYOD a fait l'objet d'une appréhension progressive. En effet, dans un premier temps, les chartes informatiques prohibaient généralement l'utilisation « d'outils » personnels.

Par définition, le **BYOD** est une pratique qui consiste à utiliser ses équipements personnels dans un contexte professionnel. Selon le cabinet Gartner, en 2018, plus d'un terminal mobile et connecté sur deux appartiendra aux employés et non à l'entreprise[10].

[7] ADAM (P.), «SMS, vie privée et portable professionnel : histoire (courte) d'un Homme « sans territoire », *Revue Droit du travail Dalloz*, n°3, p.191

[8] MARRAUD (L.), *De la conception d'une plateforme de télétravail virtualisée et unifiée : analyse socio-techniques du travail « à distance » équipé* , Business administration . Telecom Paris-Tech, 2012, p.22

[9] Clusif , « Consumération de l'IT et la Sécurité de l'information », mai 2012, p.4

[10] TRUJILLO (E.), « Le BYOD : une réalité, mais jusqu'à quand ? », publié le 12 janvier 2015, disponible sur <www.ideas.microsoft.fr >

Toujours d'après ce cabinet, 90% des organisations devraient avoir adopté l'un des aspects du BYOD en 2017[11]. Cette pratique soulève des problématiques sociales, juridiques et relatives à la sécurité de l'information.

Aujourd'hui, trois éléments permettent de caractériser un équipement BYOD : la mobilité, la disponibilité et l'adaptabilité, et l'appartenance à l'utilisateur[12]. Si l'on s'attache particulièrement à définir et à préciser chaque terme : « *Bring* » signifie en français « apportez », il sous-entend toutefois une connexion avec le système d'information, peu importe le moyen utilisé (port USB, réseau Wifi, 3G/4G/ Bluetooth), « *your own* » signifie « ton propre », ce terme renvoie aux outils et terminaux possédés par le salarié, et « *device* » signifie « équipement » c'est-à-dire qu'il renvoie aux smartphones, tablettes etc. Le terme « mobile device » est également très utilisé. Celui-ci fait référence aux équipements dits « mobiles ». Le terme « *mobilité universelle* » est aussi aujourd'hui fréquemment utilisé. Certains n'hésitent pas à affirmer que cette mobilité constitue l'un des moteurs de la technologie[13]. Il est opportun de souligner que la mobilité professionnelle ne se résume plus aujourd'hui simplement au BYOD. En effet de très nombreux acronymes sont ensuite apparus. Ainsi, l'entreprise connectée du 21e siècle a vu se développer plusieurs pratiques. Le **BYOS**, dérivé du BYOD, signifie « *Bring Your Own Software* » c'est-à-dire apportez votre propre logiciel. En effet, les outils liés à la mobilité permettent aux employés d'accéder à des logiciels qui n'appartiennent pas à l'entreprise. Cela peut par exemple inclure l'utilisation de services de stockage dans le Cloud pour collaborer ou partager des documents[14].

Parmi ces acronymes, le **CYOD** (*Choose Your Own Device*) a également fait parler de lui. Par définition, c'est le choix qui est offert à l'utilisateur d'un matériel professionnel au sein d'un catalogue d'équipements nomades ayant reçu l'agrément de l'entreprise. Il semblerait que le CYOD vienne en complément du BYOD. En effet le CYOD présente un avantage incontestable pour l'entreprise : les terminaux mobiles sont paramétrés, approuvés et intégrés

[11] CASETTA (R.), « Les défis du BYOD en entreprise sont à relever dès maintenant », publié le 10 décembre 2014,< www.lesechos.fr>
[12] PASSET (M.), VERDEL (C.), NAUGES (L.), *BYOD : réussir son intégration dans l'entreprise*, Ed.ENI, 2014 p.41
[13] Livre blanc Aerohive Networks, Au-delà du BYOD : comment transformer le BYOD en productivité, 2012, p.2
[14] Livre blanc Sophos de M. ESCHELBECK Gerhard, Les risques et avantages du BYOD , Juillet 2013, disponible sur www.sophos.com, p.4

à l'entreprise[15]. Le CYOD a pu être présenté comme l'une des tendances de l'année 2014 avec les objets connectés et la thématique du Big Data.

Enfin, je souhaiterai également évoquer le **COPE** (*Corporated Owned Personnaly Enabled*). Par définition, il s'agit de la mise à disposition dans un cadre privé d'un matériel professionnel, propriété de l'entreprise et sélectionné par elle. L'ensemble de ces politiques de mobilité sont aujourd'hui fréquemment accusés d'inciter les salariés à « l'hyper-connexion ». Par définition, celle-ci peut se définir comme la « *volonté croissante dans notre société d'être toujours connecté, toujours joignable et disponible à tout moment*[16] ».

Pour mieux appréhender la notion « d'entreprise mobile et connecté », il convient de présenter certains éléments de cette mobilité. Ainsi, le marché des technologies mobiles est aujourd'hui très dense. Depuis plusieurs années, des changements économiques, juridiques, sociaux et technologiques se sont imposés aux entreprises. Parmi ces changements technologiques, la « mobilité informatique » est un véritable enjeu pour toutes les entreprises[17]. Les chiffres relatifs aux taux d'équipements sont impressionnants. Ainsi en 2016, le nombre de smartphones et de tablettes devrait atteindre un milliard tandis que le nombre de téléchargements d'applications devrait atteindre 305 millions et le nombre de terminaux connectés en 2020 est estimé à 50 milliards[18].

Il est possible d'opérer une classification entre les différents objets qui contribuent à la mobilité de l'entreprise. Parmi ces outils, il est possible de distinguer :

- **Le téléphone mobile et plus récemment le smartphone** :

D'un point de vue historique, les premiers téléphones portables sont apparus dans les années 1980 mais leur démocratisation auprès du grand public ne date que des années 1990. La baisse des prix des terminaux mobiles a notamment permis de favoriser la tendance du multi-équipement que l'on peut constater aujourd'hui. Ces téléphones ont progressivement évolués, et dorénavant ceux qui connaissent le succès le plus important sont les smartphones, appelés aussi « téléphones intelligents ». Une grande partie des français est maintenant équipée.

[15] GERAY (L.), « Choose Your Own Device : le vrai débat pour travailler autrement ? », publié le 5 mars, <www.lesechos.fr>
[16] MADEROU (T.), Mémoire d'étude, Mémoire de projet, sur l'hyperconnexion, Ecole Boulle, 2013, p .20
[17] BESSEYRE DES HORTS (C-H.), *L'entreprise mobile : comprendre l'impact des nouvelles technologies*, Pearson, coll. ENTREPRISES/MAN, avril 2008, p.16
[18] ANONYME, « Le CYOD, première étape vers le BYOD ? », publié le 5 novembre 2014, www.itforbusiness.fr

Ainsi, le smartphone est devenu un objet de consommation courante[19]. Cet outil est aujourd'hui répandu non seulement dans la sphère professionnelle mais également dans la sphère personnelle. C'est pourquoi, il est possible d'affirmer que celui-ci est maintenant devenu un véritable outil de travail[20]. Le smartphone réunit un ensemble de fonctionnalités qui étaient présentes dans des outils mobiles distincts. Il présente un avantage certain : les informations peuvent également se synchroniser avec d'autres types d'outils mobiles. En outre, sa fonction principale est de moins en moins celle de passer des communications. Enfin, le smartphone présente aujourd'hui de nouvelles fonctions comme par exemple la géolocalisation[21]. Selon le reportage très pertinent intitulé « *Digital Detox* » de Pierre-Olivier Labbé, aujourd'hui, un français sur deux possède un smartphone. En France, on compte plus de 28 millions de smartphones. En moyenne toujours selon ce reportage, un individu consulte son smartphone 150 fois par jour. L'usage addictif de cet outil est souvent critiqué et soulève également des problématiques juridiques que j'évoquerai dans le cadre de ce mémoire. Le smartphone est en général le terminal mobile le plus souvent utilisé dans le cadre du BYOD. Toutefois, il existe certaines divergences entre les pays. Ainsi, par exemple en Chine, pays où le BYOD est bien implanté : 90% des salariés utilisent leur terminal mobile (smartphone) personnel pour travailler, tandis que 81% des salariés aux Etats-Unis et 72% des salariés au Royaume-Uni utilisent également leur smartphone dans un contexte professionnel[22].

- **L'ordinateur portable et la tablette** :

Le PC traditionnel a progressivement été remplacé par les tablettes, particulièrement dans le milieu professionnel. Il me semble qu'il est également important de souligner que de nombreuses entreprises n'hésitent plus à équiper leurs salariés. Depuis la mise sur le marché de l'iPad, le marché des tablettes est devenu un véritable marché de masse. Il est possible néanmoins de s'interroger sur les risques, les conséquences et les répercussions de ces usages mixtes sur la vie personnelle du salarié. Selon le reportage « Digital Detox » de Pierre Olivier Labbé, on compte en France, plus de 9 millions de tablettes. Ainsi, 1 foyer sur 3 est aujourd'hui équipé. D'après IDC, société de conseil et d'études, près de 100 millions de tablettes ont été vendues depuis le début de l'année 2015, dont 7.5 millions en France. Ainsi,

[19] PASSET (M.), VERDEL (C.), NAUGES (L.), *BYOD : réussir son intégration dans l'entreprise*, *op.cit*, p .22
[20] BESSEYRE DES HORTS (C-H.), *L'entreprise mobile : comprendre l'impact des nouvelles technologies*, Pearson, coll. ENTREPRISES/MAN, avril 2008, p.38
[21] BESSEYRE DES HORTS (C-H.), *L'entreprise mobile : comprendre l'impact des nouvelles technologies*, Pearson, *ibid.*, p.45
[22] Rapport d'étude CISCO IBSG Horizons, BYOD : une perspective mondiale, 2012, p.7

on assiste à un véritable engouement des français à l'égard de cet outil[23]. Par ailleurs, la tablette et le smartphone sont des outils fréquemment utilisés car en général on estime qu'ils permettent d'améliorer la productivité des employés, dès lors que ceux-ci ont une bonne connaissance de leur fonctionnement. Cela est d'autant plus vrai quand les salariés financent leur propre terminal, ils ont alors tendance à en prendre davantage soin, ce qui semble véritablement compréhensible[24]. Aux Etats-Unis, 60 % des salariés environ utilisent une tablette personnelle pour travailler, tandis qu'au Royaume-Uni, « seulement » 54% des travailleurs utilisent une tablette personnelle pour un usage professionnel[25].

- **La clé USB** :

Outil lié à la mobilité par excellence qui a très récemment fait l'objet de l'actualité jurisprudentielle en 2013. Pour une grande partie de la doctrine, la jurisprudence relative à une clé USB connectée à un ordinateur professionnel constitue l'une des premières liée à la mobilité, et plus particulièrement au BYOD. Aujourd'hui, de nombreux salariés ne sont plus réticents à stocker de nombreuses informations sur ce type de support.

Aujourd'hui, le BYOD qui a connu une évolution exponentielle ces dernières années semble s'être imposé comme un problème de société. Il soulève des problèmes techniques, sociaux, et principalement juridiques[26]. Avec l'accroissement considérable du nombre de terminaux connectés, l'individu entre autre le salarié exprime fréquemment le souhait de pouvoir être connecté de façon quasiment permanente. Nous verrons toutefois dans le cadre de ce mémoire, que ce souhait est remis en cause aujourd'hui pour certains qui prônent la « déconnexion ».

Le BYOD et le CYOD s'imposent parfois pour les plus jeunes comme une évidence. Pour les générations Y, selon une étude réalisée en 2012 par JobTeaser pour Deloitte, « 86% des jeunes arrivant sur le marché du travail s'attendent à être équipés de terminaux mobiles par leur

[23]ANONYME, Mobilité, digital et entreprise, la loi des tablettes, publié le 13 novembre 2014, <www.lenouveleconomiste.fr>
[24] LEVY-ABEGNOLI (T.), « Terminaux IT personnels (BYOD) : impacts et impératifs pour l'entreprise », publié le 3 mai 2012, disponible sur <www.zdnet.fr>
[25]Rapport d'étude CISCO IBSG Horizons, BYOD : une perspective mondiale, 2012, disponible sur www.cisco.com, p.7
[26] Rapport d'étude Club EBIOS, BYOD : Elements de réflexion pour gérer des risques, sous la direction de M.GRALL Matthieu, responsable des travaux, 11 février 2014, p.4

entreprise[27] ». Si le BYOD est aujourd'hui au cœur de l'actualité, il ne semble toutefois pas convaincre tout le monde, et les réticents à ce type de mobilité semblent nombreux.

Bien que le sujet de la mobilité interroge et divise certains, il semblerait que les français portent néanmoins un intérêt de plus en plus important à l'égard de ces solutions. Ainsi, je souhaiterais illustrer ce propos en citant quelques chiffres issus d'une étude pour le compte de VMware[28]. Selon cette étude, « 62% des salariés français pensent que leur entreprise ne leur procure pas les outils et applications mobiles nécessaires à leur productivité et à leurs missions ». Cette étude révèle aussi « qu'un salarié sur cinq se dit stressé sans accès à ses données professionnelles en dehors de son lieu de travail. Un tiers des salariés se dirait même prêt à quitter l'entreprise à défaut de pouvoir utiliser ses outils mobiles pour travailler.

Le multi-équipement est aujourd'hui un constat. Ainsi 63% des salariés utilisent un PC portable et 55% un smartphone. Quant à l'utilisation des tablettes par les salariés, le chiffre a doublé en 2013 et a atteint 19%[29]. Un salarié est équipé en moyenne de près de 2, 5 équipements mobiles. L'augmentation de l'équipement mobile s'explique en grande partie par l'acquisition d'outils personnels utilisés à titre professionnel.

Le BYOD présente un certain nombre d'avantages qui sont les suivants : « une disponibilité immédiate des équipements, un accroissement de la productivité, une liberté et un confort lié à l'utilisation d'un terminal connecté que le salarié connaît et une plus grande autonomie des collaborateurs[30] ». Le BYOD est une problématique véritablement d'actualité. A cet égard, il est possible d'illustrer ce propos par un exemple d'outil mobile et connecté qui connaît aujourd'hui un fort succès. Cet outil peut potentiellement rassurer les réticents à la pratique du BYOD. Ainsi, une entreprise française propose désormais une clé USB intelligente qui permet de travailler en mobilité en sécurité. Le principe de cette clé est simple et séduit de plus en plus : une fois connectée, l'utilisateur peut accéder à un réseau privé virtuel qui lui permet de sauvegarder, partager et transférer des données, et ce en sécurité. En

[27] VALLEJO (J-L), « Digital : chronique d'une mutation du travail », L'Expansion Management Review 2/2014 (N° 153), p. 120-128

[28] SANYAS (N .), « Byod et mobilité : les salariés français mécontents de la politique de leur entreprise », publié le 14 juin 2013, <www.zdnet.com>

[29] Livre blanc IDC, BAHLOUL Karim et BRINDAVOINE Florent, Télétravail et ultra-mobilité un nouvel environnement de travail pour les salariés, de nouvelles problématiques pour les entreprises, janvier 2014, p.2

[30] PASSET (M.), VERDEL (C.), NAUGES (L.), *BYOD : réussir son intégration dans l'entreprise, op.cit,* , p.58

outre, cette clé présente un avantage important : elle peut être rendue inutilisable sur simple demande.

Dans le cadre de ce mémoire, j'ai également souhaité mettre à profit mon expérience professionnelle en Italie acquise dans le cadre de mon master 2 professionnel, afin d'analyser ma problématique également sous un autre angle européen. C'est pourquoi au sein de ce rapport, je ferai régulièrement des comparaisons afin d'analyser de quelle manière la « mobilité professionnelle » ou « la mise en place de terminaux mobiles et connectés » est appréhendée en France et en Italie. Ainsi, j'évoquerai différents aspects juridiques en droit comparé mais également d'autres aspects plus économiques ou sociaux. Cette approche comparée me semble pertinente dès lors que la problématique traitée au sein de ce mémoire dépasse nos frontières. Le BYOD ou le CYOD dépasse également les frontières entre le public et le privé, et nombreux sont ceux qui y sont aujourd'hui confrontés. Selon un report d'Oracle- Byod Index[31], « près de la moitié des entreprises européennes s'oppose encore au modèle BYOD ou ne l'acceptent que dans des circonstances exceptionnelles, 22% interdisent fermement la possibilité que les informations et les données de l'entreprise se trouvent sur ces dispositifs, et 20% n'ont défini aucune règle spécifique à cet égard ». Toutefois, il est intéressant de souligner que les entreprises italiennes semblent en retard par rapport au reste de l'Europe. La principale préoccupation en Italie est la suivante : la sécurité des dispositifs. Au niveau européen, la sécurité des informations est la principale préoccupation.

Après avoir évoqué quelques chiffres relatifs au BYOD au niveau européen, je souhaiterai faire un focus sur la situation du BYOD plus particulièrement en Italie, pays dans lequel j'ai réalisé mon stage de fin d'études. En effet, selon une étude InTel Sécurity réalisée sur 2500 professionnels dont 200 italiens relatifs à l'impact des nouvelles technologies sur l'activité professionnelle : « 86% des professionnels apportent et utilisent leurs terminaux personnels en entreprise : 72% apportent leur smartphone, 32% un ordinateur portable ». Par ailleurs, « 79% admettent utiliser leur terminal professionnel pourun usage personnel, 76% pensent que l'entreprise est responsable de la protection de données personnelles conservées sur les terminaux professionnels, 63% pensent que leur entreprise protège leur propre identité et

[31] ANONYME, « Il BYOD fa paura alle aziende italiane », publié le 18 mars 2014, < www.corrierecomunicazioni.it>

données[32]. » Malgré ces chiffres qui semblent témoigner d'une implantation du BYOD chez nos voisins, le BYOD semble malgré tout demeurer un phénomène parfois encore marginal en Europe. La situation devrait néanmoins évoluer. Selon la société de recherche GARTNER, la moitié des salariés devrait demander aux employeurs de pouvoir utiliser leur propre dispositif [33]. Toutefois, certains auteurs ont souligné de façon pertinente une difficulté. En effet, une entreprise avec des filiales dans plusieurs pays européens doit prendre en compte les différentes règles applicables dans les pays en matière de droit à la protection de la vie privée ou encore en droit du travail. En outre, dans de nombreux pays européens (parmi lesquels l'Italie), toute forme de contrôle à distance du salarié est interdite sans autorisation. Selon Roberto Scano, fondateur d'Iwa Italy, la norme italienne interdit employés du secteur public, d'utiliser leur propre dispositif personnel[34] ».

Historiquement, on constate que l'intérêt porté au BYOD a débuté à partir de 2012 en France, comme en témoigne le nombre de recherche sur Google Trends[35]. Il est intéressant de souligner que les anglo-saxons sont les premiers à avoir introduit le BYOD dans les entreprises. En outre, il me semble important de rappeler que préalablement à l'obligation qui s'impose par le Code du travail à l'employeur de fournir aux salariés les outils de travail, les salariés apportaient leurs outils pour travailler[36]. En juillet 2015, j'ai utilisé le logiciel Google Trends proposé par Google afin de connaître la fréquence à laquelle le terme « BYOD » a été tapé sur le moteur de recherche, en vue de définir l'intérêt pour ce sujet. J'ai effectué cette recherche à la fois pour la France et pour l'Italie afin de comparer l'évolution de l'intérêt pour cette recherche. S'agissant du BYOD, on constate un intérêt pour cette recherche en France à partir de décembre 2011. L'intérêt pour cette recherche a été le plus important en octobre 2012 et en juillet 2013. Enfin, l'intérêt pour cette recherche a diminué, puis a de nouveau augmenté en novembre 2014 et en mars 2015. En Italie, on constate un intérêt pour cette recherche à partir d'avril 2012, en général croissant jusqu'à décembre 2012, puis cet intérêt a diminué en mars 2013. Entre novembre 2013 et mai 2015, l'intérêt apparaît constant**. (cf. voir Annexe n°1)**

[32] ANONYME, « BYOD in Italia e all'estero: i nuovi dati Intel », publié le 30 janvier 2015, <www.techeconomy.it>
[33] ODDO (I.), « ADAPTability/14 BYOD : la nuova frontiera del lavoro « mobile », publié le 29 mai 2014, <www.ilsole24ore.com>
[34] LONGO (A.), « Il BYOD si diffonde senze regole in aziende e PA », <www.Digital4.biz>
[35] PASSET (M.), VERDEL (C.), NAUGES (L.), *BYOD : réussir son intégration dans l'entreprise*, *op.cit*, p.22
[36] OLSEN (M.), *BYOD Sans stress* , Institut Supérieur d'Electronique de Paris, 2011-2012, Master management et protection des données personnelles, p .5

Dans le cadre de ce rapport, j'ai choisi d'apporter des limites à ce sujet. Je limiterai mes analyses techniques, économiques et sociologiques. Néanmoins, j'aborderai certains aspects, indispensables à une meilleure compréhension du sujet.

Le BYOD est aujourd'hui un phénomène mondial, bien qu'ignoré ou largement sous-estimé par les entreprises. Néanmoins, on constate quelques divergences, avec un fort développement en Asie et en Amérique latine, et une progression difficile en Europe, tandis qu'il est fortement adopté aux Etats-Unis[37]. Par ailleurs, il convient de rappeler que le BYOD est une pratique que l'employeur est libre d'organiser ou d'interdire[38]. En France, bien que la mobilité interroge, inquiète et divise les entreprise, trois grandes entreprises françaises ont déjà fait le choix de la mobilité. Ainsi, « sur terre » la SNCF a décidé d'équiper 10 000 chefs de bords et contrôleurs de smartphones en 2010. « Dans les airs » Air France a également lancé un projet de mobilité. En effet, la société a équipé en 2012 plus de 4000 pilotes d'iPad. Enfin, chez Renault, plusieurs milliers d'employés équipés auparavant de BlackBerry utilisent désormais leurs propres terminaux. Certains ont toutefois préféré le CYOD[39].

Ma démarche dans le cadre de ce mémoire est la suivante : identifier et définir les risques en particulier juridiques, en vue de pouvoir mettre en place ce type de mobilité, sans exposer l'employeur ni le salarié à trop de risques. La problématique que j'ai donc choisie dans le cadre de ce mémoire est la suivante :

Dans quelle mesure l'ultra-mobilité de l'entreprise et la mise en place de terminaux connectés personnels ou professionnels nécessite-t-elle un encadrement spécifique face à l'hyper-connexion du salarié et aux risques juridiques ?

Bien que la « mobilité de l'entreprise » soit souvent présentée comme pertinente et opportune, la mise en place de terminaux connectés dans le milieu professionnel apparaît comme étant un choix à risques pour l'employeur face aux enjeux juridiques (**Partie I**). Elle semble nécessiter un encadrement juridique face aux risques auxquels les salariés sont également exposés (**Partie 2).**

[37] Rapport d'étude CISCO IBSG Horizons, BYOD : une perspective mondiale, 2012, disponible sur <www.cisco.com>, p.3

[38] Rapport d'étude, Les Terminaux personnels en Entreprise- FAQ, Forum des Compétences, étude menée avec Caprioli&Associés, Société d'avocats, disponible sur <www.forum-competences.com>, p.9

[39] SANYAS (N.), « Mobilité en entreprise : les cas Renaut, Air France et SNCF », publié le 30/01/2015, <www.zdnet.fr>

PARTIE 1.

LA MISE EN PLACE DE TERMINAUX MOBILES ET CONNECTÉS DANS LE MILIEU PROFESSIONNEL : UN CHOIX À HAUTS RISQUES POUR L'EMPLOYEUR FACE AUX ENJEUX JURIDIQUES

A priori, il semblerait que le choix de la mobilité en entreprise ne puisse se faire sans risques. Avec le développement des nouvelles formes de mobilité citées en introduction, les risques ont tendance à se multiplier. A titre d'illustration, par exemple, selon une enquête récente : un salarié sur 5 mettrait en ligne des données sensibles de son entreprise via des applications de cloud pour les partager à l'extérieur[40]. Dès lors, la question suivante peut se poser : comment parvenir à concilier les enjeux et les risques liés à la mobilité ? En effet, « par le biais du développement des nouvelles technologies, tout salarié peut aujourd'hui accéder aux ressources de son entreprise, peu importe l'endroit où il se trouve [41] » et cela pose des problèmes en terme de sécurité.

Le choix de solutions de « mobilité » a véritablement tendance à accroître la porosité entre les données d'une part personnelles et d'autre part professionnelles. La protection des données personnelles et professionnelles doit ainsi en principe être assurée de manière effective**.** Dans le cadre de ce mémoire, je tenterai d'apporter des éléments de réponse à cette problématique, qui me semble être l'une des plus pertinentes, soulevée notamment par le BYOD. En effet, la porosité entre les différentes données a tendance à engendrer des risques nombreux qui peuvent être internes et externes à l'entreprise. (**Chapitre 1**).

[40] Enquête « Market Pulse Survey » de Sail Point

[41] ASSING (D.), CALE (S.), *La sécurité des accès mobiles : au delà du BYOD*, Hermes Science Publications, coll. Management et informatique, septembre 2012, p.15

Toutefois, les solutions de mobilité n'entraînent pas seulement des risques à l'égard de la distinction et de la gestion des différents types de données. En effet, elles peuvent également avoir une influence sur les droits de propriété intellectuelle **(Chapitre 2).**
La première partie de mon mémoire a donc pour objectif d'identifier les principaux risques juridiques liés aux solutions de mobilité en vue d'apporter des informations pertinentes à tout employeur qui serait intéressé par ces solutions de mobilité.

Chapitre I. La remise en cause de la classification et de la sécurité des données personnelles et professionnelles

Le choix de solution de mobilité dans le milieu professionnel présente comme nous l'avons précédemment vu des risques en matière de protection des données. Ces risques concernent en grande partie les données professionnelles et donc par conséquent l'employeur. L'absence de prise en compte de ces risques peut dans certaines hypothèses avoir pour conséquence une « cessation d'activité ou bien une condamnation de l'entreprise[42] ». Toutefois, les données personnelles peuvent également présenter des risques pour cette dernière, car l'employeur se voit imposer un certain nombre de règles en vue d'assurer leur protection. A défaut, il peut voir sa responsabilité engagée. C'est pourquoi, la problématique de l'identification de la nature et de la séparation des données personnelles et professionnelles me paraît très importante.

La protection des données apparaît être le défi le plus conséquent[43]. Dans le cadre de cette sous-partie, je ferai une approche en droit comparé relative à la gestion et au traitement de données d'une part en France et d'autre part en Italie **(Section 1)**.

En outre, les solutions de mobilité semblent également accroître les risques en matière de sécurité et de confidentialité, toujours au regard des données personnelles et professionnelles **(Section 2)**.

[42] PASSET (M.), VERDEL (C.), NAUGES (L.), *BYOD : réussir son intégration dans l'entreprise*, Ed.ENI, 2014, p.85
[43] Livre Blanc Microsoft, GRASSET (J.), Bring Your Own Device, Vision sécurité et approche des solutions, Microsoft France, septembre 2013, p.6

Section I. La problématique de la porosité des données personnelles et professionnelles

Les solutions de mobilité ont généralement pour conséquence d'augmenter la porosité entre les données (**paragraphe 1**). Toutefois, certains types de mobilité se sont développés ces dernières années afin de protéger l'employeur de ce risque et peuvent apparaître aujourd'hui comme des alternatives pertinentes pour ceux qui seraient encore réticents au BYOD (**paragraphe 2**).

§1 - La porosité croissante des données personnelles et professionnelles par l'utilisation d'un terminal privé à des fins professionnelles

La frontière entre les données personnelles et professionnelles semble de plus en plus mince eu égard aux nouvelles formes de mobilité. Cela entraîne une confusion entre les données personnelles qu'il convient d'identifier précisément (A), et les données professionnelles (B) afin de les protéger**.** En effet, l'identification des données apparaît véritablement nécessaire en vue également d'assurer la sécurité de l'entreprise.

A) Les données personnelles

Les outils utilisés dans le cadre de la mobilité sont de plus en plus souvent utilisés pour un usage mixte, c'est-à-dire à la fois personnel et professionnel. Par conséquent, il est très fréquent que des données dites « personnelles » se trouvent au sein de ces outils. Il y a peu, la présidente de la CNIL affirmait *« les données personnelles sont le pétrole de l'économie numérique »*. Ces propos peuvent être confirmés aujourd'hui. En effet, il existe un véritable

commerce qui représente plus de 800 milliards de dollars autour de ces données. Ces chiffres témoignent donc de la nécessité d'assurer la protection de ces données, qui peuvent exister au sein des outils mobiles et connectés.

1) L'identification des données

Il est important de souligner que le smartphone est souvent appréhendé comme étant un outil personnel, hébergeant par conséquent des données personnelles. Certains d'entre nous entretiennent un rapport véritablement addictif à l'égard du smartphone. C'est pourquoi l'expression « prolongement de soi » est parfois utilisée, et l'hyper-connexion inquiète de plus en plus tant dans la sphère personnelle que professionnelle. Or, il s'avère que parfois le smartphone est également ou le devient un outil de travail. Eu égard à cette qualification, la frontière entre la sphère professionnelle et personnelle du salarié a tendance à se réduire, dès lors que le smartphone se présente comme un outil à usage mixte.

La question qui se pose alors est la suivante : Comment réussir à distinguer les données personnelles et les données professionnelles au sein de ces outils à usage mixte ? La problématique des données stockées sur ces outils apparaît difficile à appréhender. En effet, ces données peuvent être qualifiées de données personnelles au sens de l'article 6 de la loi de 1978, de données relevant de la vie privée au sens de l'article 9 du code civil, ou il peut s'agir de données professionnelles. Préalablement, il me semble donc pertinent de revenir sur la notion de « données personnelles ». Selon l'article 2 de la loi du 6 janvier 1978, par définition, il s'agit de « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* ». Ces données sont donc, entre autres, « le nom, le prénom, le sexe, les appartenances politiques, les activités syndicales, les aspirations philosophiques et religieuses, le numéro de sécurité sociale, le numéro de carte bancaire[44] ». En outre, les éléments suivants permettent aussi l'identification de manière indirecte d'un individu : les photographies, l'adresse IP, les « traces informatiques », l'ADN, le numéro d'immatriculation, l'empreinte digitale, le lieu de résidence, la profession ou encore le numéro d'identifiant national étudiant. Ainsi, la liste est loin d'être exhaustive.

[44] LANDREAU (I), « Le téléphone portable : instrument angélique ou diabolique lors d'un usage mixte professionnel et personnel ? », *Revue Lamy Droit de l'immatériel*, n°95, juillet 2013, p.69

Selon la CNIL, la protection des données à caractère personnel est aujourd'hui l'un des sujets les plus importants sur le lieu de travail en 2015. Ainsi, la CNIL a pour objectif, entre autres, de s'assurer que les employeurs et employés soient informés de leurs droits et de leurs obligations en matière de protection des données à caractère personnel. En effet, il est intéressant de souligner qu'en 2012, plus de 10% des plaintes reçues par la CNIL concernaient le monde professionnel. Parmi ces plaintes, 17 ont eu pour conséquence des mises en demeure. Les principaux manquements allégués étaient les suivants : « absence ou mauvaise information des employés, absence de déclaration, collecte excessive ou non pertinente de données personnelles ». En 2014, la CNIL a enregistré environ 11 000 demandes dont 5825 plaintes, ce qui représente une hausse de 3%.

En Italie, en matière de risques relatifs à la protection des données, il apparaît que seulement 1 entreprise sur 4 a mis à jour sa politique sur le BYOD (17%), tandis que 10% prévoit de le faire[45]. Après avoir évoqué la définition des données personnelles, il me semble important de faire un rappel sur le cadre juridique qui s'applique à ce type de données. C'est pourquoi, je souhaiterai évoquer les obligations qui incombent au responsable du traitement (souvent l'employeur) et les droits dont peuvent se prévaloir les salariés. En effet, dans le cadre du BYOD, les données personnelles qui se trouvent au sein d'outils mobiles et connectés peuvent être très importantes et très nombreuses. Dès lors, la connaissance et l'information à propos de la gestion de ces données me paraît très importante.

2) Les obligations de l'employeur et les droits des salariés

a) Les obligations de l'employeur

Le traitement de données personnelles implique un certain nombre d'obligations pour l'employeur, non seulement en France mais également en Italie.

- ***Le traitement de données personnelles en France***

L'information des représentants du personnel par l'employeur de la mise en place d'un dispositif gérant des données personnelles est nécessaire. En effet, chaque salarié doit avoir connaissance de l'identité du responsable de l'outil en question, des finalités poursuivies avec son installation, des destinataires ou des personnes ayant accès aux informations collectées et

[45] RUSCONI (G.), « Il Byod è sinonimo di produttività. Ma anche una sfida ancora da vincere », publié le 1er novembre 2014, <www.ilsole24ore.com>

des conditions d'exercice de ses droits. En France, c'est la loi Informatique et Libertés du 6 janvier 1978, modifiée par la loi du 6 août 2004, qui a défini les principes qui doivent être respectés dans l'hypothèse d'une collecte, d'un traitement et de la conservation de données à caractère personnel. Elle évoque également les droits pour les personnes dont les informations sont collectées. Le respect des règles par l'employeur permet également de s'assurer la confiance des employés. La CNIL distingue un certain nombre de principes à respecter : le principe de finalité (les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime), le principe de proportionnalité, le principe de pertinence des données (les données personnelles doivent être adéquates, pertinentes et non excessives au regard des objectifs poursuivis, une durée de conservation doit être établie en fonction de la finalité de chaque fichier, l'employeur est tenu à une obligation de sécurité). Enfin, il est tenu de garantir l'intégrité et la confidentialité des données. Le principe de transparence s'impose également[46].

Ainsi, s'agissant des données personnelles, il est important de rappeler que l'entreprise pourra voir sa responsabilité pénale engagée dans l'hypothèse où un salarié pourrait accéder à des fichiers professionnels de données à caractère personnel depuis un environnement informatique non sécurisé ne permettant pas de maîtriser les risques[47]. Enfin, la CNIL est également intervenue en matière de protection des données personnelles à travers une délibération Cnil n°2005-019 en date du 3 février 2005. Cette délibération est importante dès lors qu'elle porte création d'une « norme simplifiée concernant les traitements automatisés de donnés à caractère personnel mis en œuvre dans le cadre de l'utilisation de services de téléphonie fixe et mobile sur les lieux de travail ».

- ***Le traitement de données personnelles en Italie***

Après avoir évoqué les principaux principes en matière de protection des données personnelles en France, il me semble opportun de faire un focus sur la situation en Italie afin de mettre en évidence les ressemblances qui peuvent exister entre ces deux droits.

La collecte de données personnelles peut s'avérer souvent indispensable dans le milieu professionnel. Néanmoins, il est nécessaire de se montrer vigilant. Ce propos général s'applique également en Italie. C'est pourquoi la législation sur ce que les italiens appellent la

[46] CNIL, Guide pratique pour les employeurs, p.3-5
[47] CULLAFROZ-JOVER (S.), et LUBET (P.), « La souplesse du droit face à l'usage croissant du BYOD : étude sur la gouvernance des données au sein de l'entreprise connectée », *Revue des Juristes de Sciences Po*, 1 Mars 2015

« Privacy» ou relative à la « vie privée » reconnaît la possibilité pour le salarié d'avoir le contrôle des informations qui sont récoltées par l'employeur et de pouvoir consentir à leur utilisation. Ce contrôle des informations apparaît opportun dès lors qu'il permet véritablement de renforcer la protection de la vie privée (notion à laquelle les italiens sont très attachés) mais également « d'accroître la protection de l'identité personnelle du salarié, qui dans le cadre de son milieu professionnel a le droit de limiter la diffusion d'informations le concernant[48] ». Il est important de souligner que ces informations peuvent être nombreuses et sensibles. A cet égard, le 23 novembre 2006, le Garant de la Privacy a adopté un « acte juridique » relatif au traitement des données personnelles dans le cadre du rapport entre le salarié et l'employeur[49]. L'objectif est de fournir des indications et des recommandations relatives aux opérations de traitement effectuées avec des données personnelles mais également des données sensibles des salariés. Ce texte évoque entre autres plusieurs points importants tels que : le comportement de l'employeur qui doit traiter ces données du salarié en respectant les principes de licéité, transparence, pertinence et finalité. Ensuite, la diffusion de ces données peut être autorisée seulement pour l'exécution d'obligations résultant du contrat de travail. L'employeur doit aussi informer son salarié et identifier précisément les personnes pouvant traiter les données. En l'espèce, il est possible d'affirmer que sur ce point le droit français et le droit italien convergent dès lors que comme nous l'avons vu précédemment, un certain nombre de principes (licéité, transparence, pertinence et finalité) sont communs.

S'agissant de l'acquisition des données et du traitement : l'employeur est tenu d'informer le salarié de manière claire sur les modalités d'utilisation des instruments mis à sa disposition qui le contrôle. Les informations peuvent figurer dans une sorte de règlement interne adopté par l'employeur. Par ailleurs, certaines ne peuvent pas être diffusées à moins que cela soit prévu par un contrat ou qu'il s'agisse de l'exécution d'une obligation légale.

Le BYOD en Italie divise et interroge à cet égard. En effet, l'employeur pourrait de manière involontaire avoir connaissance de données personnelles violant ainsi l'article 8 de la loi du 20 mai 1970 n.300 qui interdit à l'employeur de mener des enquêtes sur les données personnelles.

[48] ANONYME, « La privacy nei rapporto di lavoro », www.diritierisposte.it
[49] Linee guida sul trattamento di dati personali dei lavoratori privati – 23 novembre 2006 [1364939]

Au niveau du droit de l'Union européenne, l'adoption du projet de règlement européen[50] relatif aux données à caractère personnel apparaît très pertinente, car ce projet influencerait également la gestion du BYOD, dès lors que la problématique des données personnelles est omniprésente. Ce projet est important à plusieurs égards. En effet, tout d'abord, il présente un ensemble de règles pouvant s'appliquer directement dans tous les Etats membres. Par conséquent, il concernera la France et l'Italie. Par ailleurs, il prévoit non seulement un renforcement des obligations et de la responsabilité du responsable du traitement de données personnelles mais également des autorités nationales en charge de la protection des données.

b) Les droits des salariés

- **En France**

La CNIL, autorité garante pour la protection des données personnelles a notamment publié un guide à l'attention des employeurs et des salariés afin de les « orienter » et de les guider dans la gestion de la « problématique des données personnelles en entreprise ». Un certain nombre de principes importants sont énoncés au sein de ce guide. Parmi ces principes, il est important de relever l'exigence de l'information des salariés à propos de l'informatisation de leurs données, des objectifs poursuivis, du caractère « obligatoire ou facultatif » de leurs réponses, des destinataires des données et des modalités d'exercice de leurs droits. En vertu de la loi Informatique et Libertés de 1978, le salarié dispose d'un certain nombre de droits, parmi lesquels :

- **Le droit d'accès et de rectification** (article 35) : toute personne peut demander au détenteur d'un fichier de lui communiquer toutes les informations la concernant dans un fichier. Toute personne peut également demander le droit de rectification ou de suppression d'informations erronées. Cette disposition législative s'applique bien entendu dans le cadre de la relation entre salariés et employeurs. En effet, l'employeur a de plus en plus régulièrement accès aux données personnelles du salarié, entre autres par le contrôle de la connexion internet et géolocalisation. A cet égard, certains ont pu dénoncer des lacunes dans la rédaction du texte et l'absence de prise en compte

[50] Proposition de règlement européen sur la protection des données à caractère personnel (COM25(2012)11 final) 25/01/2012

de cette problématique dans le cadre du projet de règlement européen sur la protection des données personnelles[51].

- **Le droit d'opposition** : toute personne a le droit de s'opposer, pour des motifs légitimes à ce que des données à caractère personnel la concernant soient enregistrées dans un fichier informatique, sauf si celui-ci résulte d'une obligation légale ou réglementaire.

Les autorités européennes ont veillé à rappeler le droit de chacun à la protection de ses données personnelles, lors des journées européennes de la protection des données personnelles et de la vie privée. L'objectif de ces journées est de sensibiliser les citoyens au traitement de leurs données personnelles. Cela permet de témoigner de l'intérêt qui est porté à la protection des droits des individus en matière de protection des données personnelles.

Parallèlement à ces « droits », le salarié peut également avoir « des devoirs » notamment à l'égard de la protection des données « professionnelles ». Ainsi, certains auteurs de doctrine insistent sur la nécessité de prise de conscience de « ces devoirs » par le salarié. Parmi ces « devoirs », le salarié doit être conscient de l'importance de la nature des données et des informations qui sont soumises par exemple au principe de confidentialité de l'entreprise. Certains auteurs préconisent d'inscrire ce principe au sein de chartes dites « informatique et internet » en vue déterminer et de préciser l'encadrement de l'utilisation d'outils personnels à des fins professionnels. Ainsi, le salarié doit être conscient du fait de la porosité entre les données sur ce type d'outils. En effet, il peut exister des problèmes liés à la confidentialité sur ce type d'outil à usage mixte. En outre, il appartient aussi aux salariés d'être vigilant s'agissant de ses données personnelles. A titre d'illustration, il est possible d'évoquer l'anecdote suivante : en 2012, le dirigeant d'une compagnie américaine en congés avec sa famille a été confronté à une problématique pouvant être soulevée lors de l'usage mixte d'un terminal. Ainsi, sa fille a bloqué son smartphone après avoir indiqué 5 codes PIN incorrects. L'entreprise a supprimé à distance les données, et le dirigeant a perdu ses informations personnelles sur ce terminal[52].

- **En Italie**

[51] RENARD (I.), « L'employeur face au droit d'accès du salarié à ses données informatiques », publié le 20 mai 2015,<www.usine-digitale.fr>
[52] Livre blanc, Cabinet d'avocats Mathias, Livre blanc BYOD : un défi juridique à anticiper, septembre 2013, p.10

Le droit à la protection des données personnelles dit « droit élémentaire » en droit européen, est reconnu comme un droit fondamental de l'individu en Italie. Celui-ci est ainsi protégé par le Code en matière de protection des données personnelles (« decreto legislativo » du 20 juin 2003, n°196). Ainsi, selon ce Code : toute personne peut protéger ses propres données personnelles en exerçant les droits prévues par l'article 7 du Code. Toute personne peut demander à un sujet (personne physique ou entreprise) de lui fournir les informations sur un éventuel traitement de ses propres données personnelles. En particulier, il est possible de demander : l'origine du traitement, la finalité et les modalités du traitement, si les données sont traitées avec des instruments électroniques, l'identité du titulaire du responsable et du représentant désigné sur le territoire, les sujets et les catégories de sujets auxquels les données personnelles peuvent être communiquées. Enfin, les salariés en Italie disposent également d'un droit à la mise à jour, à la rectification ou à la suppression de données personnelles. En outre, ils disposent aussi d'un droit d'opposition qui leur permet de s'opposer au traitement de données personnelles : pour des motifs légitimes ou alors sans motifs dès lors que les données sont traitées pour des finalités de commerce ou de marketing. Ainsi, il est possible de constater à cet égard de nombreux points communs entre le droit français et le droit italien.

Toutefois, les données personnelles ne sont pas les seules à pouvoir être mises en danger par le BYOD. En effet, les données professionnelles sont également concernées. Dans le cadre du BYOD, des informations ou données professionnelles pourront se trouver sur un terminal personnel appartenant au salarié. Dès lors, il est possible de s'interroger sur la protection, l'accès à ce type de données et plus globalement, la gestion de ces données dont la sécurité peut être compromise. Ainsi, les interrogations des employeurs à l'égard de cette problématique peuvent sembler dans un premier temps pertinentes car la méfiance peut apparaître réelle face à une absence d'informations à ce sujet.

B) Les données professionnelles

Comme nous l'avons précédemment vu, les outils de mobilité peuvent hébergés de nombreuses données personnelles ou privées. Toutefois, ces équipements portent également des données professionnelles, qui sont tout autant importantes pour l'entreprise. De nombreuses questions ont pu être soulevées. La coexistence de données personnelles et

professionnelles au sein d'un même équipement n'est pas sans risque[53]. La problématique principale concerne ainsi le stockage des données. Il est véritablement important pour l'employeur de déterminer s'il accepte que les données professionnelles soient stockées sur le terminal[54].

Il me semble opportun dans un premier temps de définir ce que l'on entend par « données professionnelles » avant d'envisager les problématiques qui peuvent être soulevées. En effet, les données professionnelles peuvent être des données sensibles et des données stratégiques. Les données sensibles peuvent correspondre à des fichiers clients, à des documents relatifs à la stratégie de l'entreprise, au budget ou bien au chiffre d'affaire. Elles peuvent aussi se référer au patrimoine dit « immatériel de l'entreprise » qui comprend les marques, les brevets et les logiciels[55]. Les données professionnelles peuvent également correspondre aux « e-mails, déplacements professionnels, données de géolocalisation d'un véhicule ». Il est important que ces données figurent au titre de données confidentielles au sein d'une charte informatique signée**.** Quant aux données stratégiques, il s'agit de données en rapport avec certains secteurs importants par exemple celui de la sécurité intérieure ou la défense. La divulgation de données relevant de ces secteurs est réprimée par le Code pénal[**56**].

Les risques en matière de données professionnelles ont récemment fait l'objet de l'actualité. A titre d'illustration, il me semble pertinent d'évoquer ici une étude financée par IBM qui certes peut sembler alarmiste, mais dont les chiffres sont très intéressants pour illustrer mon propos. En effet, cette étude a mis en évidence que les entreprises du « Fortune 500 », qui sont les 500 entreprises les plus fortunées aux Etats-Unis, n'investissent que très peu dans la sécurité de leurs applications. Dès lors, elles sont victimes de nombreuses « cyber attaques » qui mettent en danger les données des entreprises.

Ainsi, selon une étude de l'Institut Ponemon commandée par IBM du 20 mars, elles consacrent seulement 5,5% de leur budget à la sécurité quand elles développent des applications mobiles. Cette étude révèle aussi l'insécurité dans le domaine de la mobilité. Toujours, selon cette étude, 33% des entreprises ne testent jamais les applications qu'elles fournissent à leur client et nombreuses sont celles qui ne vérifient que rarement les failles de

[53] Rapport d'étude Club EBIOS, BYOD : Elements de réflexion pour gérer des risques, sous la direction de M.GRALL Matthieu, responsable des travaux, 11 février 2014, p.6
[54] Rapport d'étude Club EBIOS, BYOD : Elements de réflexion pour gérer des risques, *op.cit*, p.12
[55] LANDREAU (I), « Le téléphone portable : instrument angélique ou diabolique lors d'un usage mixte professionnel et personnel ? », *Revue Lamy Droit de l'immatériel*, n°95, juillet 2013, p.69
[56] LANDREAU (I), « Le téléphone portable : instrument angélique ou diabolique lors d'un usage mixte professionnel et personnel ? », *op.cit*., p.69

sécurité de leurs applications[57]. Avec l'essor de la mobilité, les entreprises doivent aujourd'hui être en capacité de gérer de très nombreux nouveaux appareils apportés par les employés ou qu'elle leur met à disposition. A cet égard, le BYOD peut être une source de danger pour les entreprises, surtout à cause des nombreuses applications que les employés installent et qui peuvent accéder aux données sensibles. Par ailleurs, une étude de la société Appthority a permis de soulever un autre point important en matière de sécurité de données professionnelles. En effet, cette étude a mis en évidence que de nombreuses applications dites « zombies », présentant un risque pour les entreprises, existaient dans des terminaux mobiles utilisés dans un cadre professionnel. En outre, cette même étude révèle que de nombreux salariés ne prennent pas le soin de mettre à jour les applications au sein de leurs terminaux personnels. Or, il est important de rappeler que les mises à jour permettent également de corriger les dispositifs de sécurité[58].

Par ailleurs, la problématique de la responsabilité à l'égard des données, en particulier professionnelles se pose également. Ainsi, la « fuite » de données sensibles et professionnelles constitue le risque principal pour l'entreprise. Certains affirment que « les nouveaux modes d'accès aux données professionnelles constitueraient de nouvelles portes d'accès aux données dites sensibles de l'entreprise »[59]. Ainsi, certains préconisent de mettre en place un système de responsabilité conjointe, qui me semble personnellement pertinent, afin qu'en cas de litige ou de conflit sur la perte de données, la direction informatique et la direction métiers de l'entreprise soient conjointement responsables. Ceux qui sont réticents au BYOD allèguent en général que cette pratique augmente les risques à l'égard de programmes malveillants en cas de perte, de vol, du mobile du salarié, des données confidentielles[60]. S'agissant des données à caractère professionnel, en principe, elles sont la propriété de l'entreprise. Par conséquent, l'entreprise est responsable de leur conservation, sauvegarde et restauration[61]. Enfin, l'entreprise est responsable de la sécurisation des données professionnelles.

§2 – La porosité limitée de la frontière entre données personnelles et professionnelles par la mise en œuvre de solutions techniques

[57] PEPIN (G.), « Selon une étude d'IBM, tous les utilisateurs de smartphones sont en danger », publié le 1er avril 2015, disponible sur www.nextinpact.com
[58] ELYAN (J.), « BYOD : les apps zombies hantent les terminaux mobiles », publié le 29 avril 2015, <www.lemondeinformatique.com>
[59] PASSET (M.), VERDEL (C.), NAUGES (L.), *BYOD : réussir son intégration dans l'entreprise*, *op.cit*,, p.90
[60] Rapport d'étude EPITA/SOLUCOM, Comment sécuriser les usages du BYOD ?, p.13
[61] PASSET (M.), VERDEL (C.), NAUGES (L.), *BYOD : réussir son intégration dans l'entreprise*, *ibid.*, p.10

De nouvelles politiques de mobilité tels que le CYOD ou le COPE ont connu une nette évolution ces dernières années face aux doutes soulevés par le BYOD (A). En outre, des interrogations relatives à la thématique du « Cloud », dit « nuage » en français existent également dans ces trois types de mobilité (B).

A) L'émergence de nouvelles politiques de mobilité et les solutions techniques : des alternatives pertinentes pour la protection et la distinction des données

Le CYOD présente un avantage par rapport au BYOD. En effet, avec le CYOD, la problématique de la propriété du terminal ne se pose plus. Avec le CYOD, les terminaux mobiles et connectés fournis par l'entreprise appartiennent à l'entreprise[62]. La problématique de la propriété de l'outil se pose dans le cadre de l'adoption du BYOD. Toutefois, il est généralement admis que les outils appartiennent aux salariés, que les applications appartiennent généralement aux salariés, tandis que les applications professionnelles appartiennent à l'employeur[63]. Ce modèle est traditionnellement opposé à celui où les outils et applications appartiennent à l'employeur et où l'utilisation de ces derniers est présumée professionnelle. L'employeur ne peut en principe interdire un usage personnel dit résiduel.

A propos des solutions techniques, le Mobile Device Management (MDM) est souvent évoqué dans le cadre de la mobilité. Par définition, il s'agit de solutions de gestion du « parc mobile » qui permettent d'identifier et de contrôler des équipements. Ainsi, le MDM installe une application qui permet à l'administrateur de contrôler l'équipement mobile. Par conséquent, « l'utilisateur cède le contrôle de l'équipement BYOD à l'entreprise[64] ». Toutefois, il est important de souligner que cette problématique lié à la « gestion de terminaux mobiles » qui sous-entend l'installation d'un logiciel peut poser certaines difficultés, dès lors que ce type de logiciel implique une collecte de données à caractère personnel des salariés qui sont les propriétaires des terminaux mobiles. L'employeur a donc l'obligation de se

[62] FILIPONE (D.), « CYOD : pourquoi ça va décoller en 2014 », publié le 5 mars 2014, <www.journaldunet.com>
[63] MAGNIEZ (A.), « BYOD : que dit la loi ? », publié le 24 janvier 2013, IT-expert magazine, <www .alain-bensoussan.com>
[64] OLSEN (M.), *BYOD Sans stress* Institut Supérieur d'Electronique de Paris, 2011-2012, Master management et protection des données personnelles, p.33

conformer à la loi Informatique et Libertés du 6 janvier 1978 que j'ai évoqué précédemment[65].

Il est important de souligner que la CNIL, autorité garante pour la protection des données personnelles en France veille à ce que les principes en matière de protection de ces données soient respectés. C'est pourquoi, la CNIL a pu parfois, à certains égards, se montrer méfiante à l'égard notamment du BYOD. Ainsi, la CNIL a publié un certain nombre de « conseils ». Parmi ces nombreux conseils, la CNIL veille notamment à rappeler que l'entreprise doit protéger ses données, et ce peu importe, que ces données se trouvent au sein d'outils mobiles et connectés qui lui appartiennent ou bien au sein d'appareils mobiles qui sont la propriété des employés. Les solutions MDM offrent aujourd'hui la possibilité aux employeurs d'effacer à distance les données hébergées dans l'appareil. Or, à cet égard, la CNIL s'est prononcée en affirmant que : « l'employeur peut mettre en place un tel système, à condition que la partie visée de l'appareil ne soit que celle spécifiquement dédiée à l'accès distant aux ressources de l'entreprise. L'employeur ne peut pas effacer l'ensemble des données présentes sur le terminal[66]. » En outre, le MDM peut soulever une autre problématique juridique : l'absence de distinction entre l'usage privé et professionnel. Par conséquent, ils permettent en principe un contrôle total du terminal personnel[67].

En résumé, les autres formes de mobilité tels que le CYOD et le COPE ainsi que la mise en place de solutions MDM peuvent être une solution mais il convient de véritablement les encadrer eu égard aux risques juridiques.

B) L'opportunité de la mise en place de mesures techniques face au Cloud

Il apparaît que le « Cloud » est beaucoup plus connu que le BYOD. Présenté comme une « révolution », il a beaucoup fait parler de lui en 2014 ainsi qu'en 2015. Il m'a paru important dans le cadre de cette sous-partie d'y faire référence. En effet, les données personnelles et professionnelles se retrouvent fréquemment au sein de ces « nuages informatiques ». Par définition, le « Cloud » peut être traduit en français par la notion suivante « informatique en nuage » qui signifie « un modèle d'organisation informatique permettant l'accès à des

[65] FERRAH (R.), « BYOD & Protection des données », publié le 10 octobre 2013, <www.village-justice.com>
[66] SANYAS (N.), « BYOD : les conseils de la CNIL », publié le 23 mars 2015,< www.zdnet.fr>
[67] LEVY-ABEGNOLI (T.), « BYOD : les outils de Mobile Device Management, la solution technique ? », publié le 11 juin 2012, <www.zdnet.fr>

ressources numériques dont le stockage est externalisé sur plusieurs serveurs[68] ». Ainsi, il me semble nécessaire de distinguer d'une part les services de « cloud computing » et d'autre part le « cloud personnel ». Ainsi, le cloud personnel peut être défini comme « la porte d'entrée de la vie virtuelle et de l'expérience numérique de chacun[69] ». En 2012, IBM a interdit l'utilisation de deux applications à 400 000 employés en raison de problèmes de sécurité. L'une des applications était Dropbox, un service renommé de stockage dans le cloud.[70] Dans le cadre du cloud, les données sont en effet stockées en dehors du périmètre physique de l'entreprise et deviennent alors accessibles depuis de nombreux terminaux et systèmes d'exploitation. Le principal risque qui peut exister en termes de cloud est le suivant : une fuite de données fréquemment confidentielles et stratégiques de l'entreprise[71]. Si le Cloud pouvait au départ apparaître réservé à un usage pour particulier initialement, les services de cloud aujourd'hui se sont énormément développés dans le milieu professionnel dans différents secteurs. Ces services peuvent toutefois mettre en danger les données de l'entreprise[72].

La problématique du Cloud dans le cadre d'une politique BYOD doit nécessairement être prise en compte, non seulement au regard de la sécurité des données, mais également au regard de leur « localisation ». En effet, la problématique de la localisation des données est parfois oubliée dans le cadre du BYOD. Or, il est important de rappeler que bien que selon le droit européen et français, les données confiées « à un tiers restent la propriété du client et que la loi interdit au prestataire de les divulguer », dans certains pays, comme dans les pays anglo-saxons, le prestataire devient le propriétaire des informations, et il n'existe pas d'obligation de protection.

Une partie de la doctrine s'interroge depuis quelques temps sur la thématique du cloud et des problèmes que celui-ci peut soulever. Ainsi, à cet égard, certains auteurs soulignent notamment la nécessité pour une entreprise française qui souhaiterait opter pour une solution

[68] Définition donnée par le Larousse
[69] OLSEN (M.), *BYOD Sans stress* Institut Supérieur d'Electronique de Paris, 2011-2012, Master management et protection des données personnelles, p.13
[70] Livre blanc Sophos de M. ESCHELBECK Gerhard, *Les risques et avantages du BYOD* , Juillet 2013, disponible sur www.sophos.com, p.4
[71] ZERBIB (R.), « Cybersécurité: le Cloud, talon d'Achille? », publié le 13/01, <www.lesechos.fr>
[72] DEDENIS (L.), « Byod et Cyod, Cloud ou encore télétravail : la synchronisation met les données en danger », publié le 21/01/14, <www.lesechos.fr>

cloud de toujours vérifier que les offres qui lui sont faites répondent aux contraintes légales qui s'imposent en sa qualité de « responsable de traitement[73] ».

En conclusion, il apparaît que le Cloud pose principalement donc des problèmes en matière de sécurité et de confidentialité des données. Toutefois, à cet égard le cloud n'est pas le seul qui est dans la ligne de mire des entreprises.

Section 2. La problématique de la sécurité et de la confidentialité des données personnelles et professionnelles

Préalablement, il est intéressant de rappeler ce que l'on doit entendre par la notion de « risques » en entreprise. Par définition, il existe un risque quand il y a une « probabilité pour qu'un évènement nuisible ou préjudiciable arrive et produise un effet négatif sur la performance de l'entreprise[74] ».

Dès lors que le salarié utilise son propre terminal personnel à des fins professionnelles, les risques internes à l'entreprise semblent s'accroître **(paragraphe 1)**. Toutefois, ces risques ne sont pas seulement internes. En effet, de plus en plus souvent, les entreprises sont concernées par des risques externes **(paragraphe 2).** Les usages mobiles et connectés sont dorénavant essentiels et apparaissent incontournables dans le milieu professionnel. Toutefois certains mettent en évidence l'absence de changements nécessaires dans la « construction des politiques de sécurité[75] ». En effet, le BYOD soulève de nombreuses problématiques relatives à la sécurité : 1 terminal sur 8 en moyenne est perdu ou volé. La protection des données est donc nécessaire[76]. Ainsi, les entreprises doivent aujourd'hui protéger non seulement leurs données, ainsi que celles de leurs clients et de leurs salariés, tout en se protégeant contre les attaques cybercriminelles[77]. Certains ont déjà pu mettre en évidence que le BYOD en 2015 pourrait soulever encore plus d'inquiétudes dès lors que les attaques et malware ont tendance à se multiplier et face à l'absence de politiques de sécurité à l'égard des données « sensibles

[73] POGGI (A-S), « Les offres Coud pour entreprises et la protection des données à caractère personnel : les recommandations dont les entreprises doivent tenir compte lorsqu'elles choisissent une offre cloud », *Lamy Droit de l'immatériel,* 1er juillet 2014, n°105, p.44

[74] Définition donnée par M.Jean-Paul Laberge, consultant en gestion

[75] ASSING (D.), CALE (S.*), La sécurité des accès mobiles : au delà du BYOD*, Hermes Science Publications, coll. Management et informatique, septembre 2012, p.13

[76] CASETTA (R.), « Les défis du BYOD en entreprise sont à relever dès maintenant », publié le 10 décembre 2014, <www.lesechos.fr>

[77] Livre blanc Sophos de M. ESCHELBECK Gerhard, Les risques et avantages du BYOD , Juillet 2013, disponible sur www.sophos.com, p.2

des compagnies » ou « des informations personnelles des salariés ». Cela témoigne donc de la nécessité urgente d'appréhender les risques internes et externes à l'entreprise dorénavant.

§ 1 – Les risques internes à l'entreprise

Les risques internes à l'entreprise peuvent faire l'objet d'une sous-division. En effet, si parfois, le salarié expose son entreprise à des risques de façon non-intentionnelle (A), la malveillance interne s'est également développée ces dernières années, et l'origine intentionnelle du risque causé est de plus en plus souvent caractérisée (B). Bien que les entreprises soient semble-t-il plus sensibles aux risques externes, la menace interne commence à être progressivement appréhendée. Ainsi dans le cadre de cette sous-partie, nous verrons qu'il est fréquent de constater des atteintes aux systèmes d'informations dont les employés sont parfois étonnement à l'origine[78].

A) L'origine non-intentionnelle du risque : la négligence ou la maladresse

Les principaux risques en interne qui peuvent aujourd'hui être identifiés (1), peuvent faire l'objet de sanctions (2).

1) L'identification des risques

Selon certains auteurs de doctrine, le facteur humain apparaît être le facteur de le plus important pouvant compromettre la sécurité de l'entreprise. Ainsi, notamment Jean-François Funke au sein d'un article juridique consacré au BYOD affirme que les risques liés à la pratique du BYOD en réalité sont plutôt liés « à l'utilisation ou au comportement social d'un individu, dès lors que les comportements de ces derniers se révèlent fréquemment être imprévisibles ou aléatoires ». Ainsi, l'entreprise ne peut en aucun cas se limiter à mettre en place des solutions techniques, car le comportement humain semblerait le plus difficile a appréhendé. « *La technologie peut toujours être dépassée* », affirme Jean-François Funke[79]. Ce principe a parfois tendance à être oublié par les dirigeants tant qu'ils ne sont pas directement confrontés à ces risques.

[78] MATIGNON (E.), *La cybercriminalité : un focus dans le monde des télécoms*, Sorbonne, 25 juin 2012, p.12-13

[79] FUNKE (J-F.), « La pratique du BYOD (Bring your own device) », JCP S (édition sociale), n°4, janvier 2015, p.3

Aujourd'hui, il est un fait : la cybersécurité est susceptible de concerner la totalité des entreprises. Par définition, elle peut être définie comme *« une politique de réduction de la surface des menaces criminelles, inhérentes à l'usage des nouvelles technologies dans l'entreprise*[80] *»*. Comme certains auteurs l'ont souligné, dorénavant la « vulnérabilité est située entre la chaise et le clavier » et « il semble inutile d'ériger de belles défenses en château fort, au coût élevé de solutions techniques, si l'édifice peut s'écrouler par celui qui, de sa chaise, aura abaissé le pont-levis de son clavier[81] ». Certes, il s'agit ici d'un propos « fort et percutant», qui semble avoir un véritable impact, mais il permet véritablement ainsi d'illustrer l'importance du risque interne en entreprise.

Une définition officielle de la cybersécurité a également été donnée par l'Union internationale des télécommunications. Ainsi, selon l'UIT, la cybersécurité correspond à « *l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyber environnement et les actifs des organisations et des utilisateurs*[82] *»*. A titre d'illustration, selon une étude GLOBAL Sécurity Study de Blue Coat, aujourd'hui, les cybermenaces dues aux employés sont constitutives d'une véritable problématique[83]. Ainsi, les chiffres issus de cette étude peuvent sembler dans un premier temps, édifiants : « 51% des employés utiliseraient des appareils personnels au travail et 20% ouvriraient des e-mails provenant de sources inconnues ». De manière incontestable, ces comportements constituent donc des risques pour la sécurité. Cette même étude s'est intéressée à la prise de conscience de la part des employés de ces risques. L'étude révèle que les employés sont conscients globalement d'exposer leur employeur à un risque de cyber-attaques. Ainsi, d'après cette étude, « 73% sont conscients du danger lié à l'ouverture d'une pièce-jointe d'une source inconnue pour l'entreprise et 65% pensent qu'utiliser une nouvelle application à défaut d'obtenir l'accord du service informatique est une menace sérieuse ». A certains égards, les employés sont conscients des cyber-risques bien qu'ils n'ont prennent pas toujours compte.

En outre, il me semble important de rappeler que si les outils liés à la mobilité se sont développés, c'est également grâce au développement très rapide des réseaux. Les salariés sont toutefois parfois négligents s'agissant de la sécurité de ceux-ci et n'hésitent pas à en faire

[80] SOUVIRA (A.), « La cyber sécurité des entreprises », Lamy Droit des affaires, novembre 2013, n°87, p.95
[81] SOUVIRA (A.), « La cyber sécurité des entreprises », Lamy droit de l'immatériel, 2013
[82] MERAV (G.), « La cyber sécurité des entreprises », Cahiers de droit de l'entreprise, septembre 2014, n°5, p.62
[83] SANYAS (N.), « L'employé, la première faille de sécurité », publié le 25 mai 2015, <www.zdnet.com>

abstraction au détriment de la sécurité de l'entreprise. Parmi ces réseaux, il convient de citer particulièrement :

- **Les réseaux mobiles :** Il convient d'évoquer ici non seulement le développement des réseaux de type Wi-Fi mais aussi développement de la 3G, 4G et 5G imminente. Aujourd'hui, le salarié peut se connecter au moment où il le souhaite à partir du lieu qu'il veut. Il est également intéressant de souligner ici que selon un rapport sur le trafic des données de juin 2012, Ericsson a pu estimer que le trafic des données devrait être multiplié par 15 entre 2011 et 2017.

- **Les réseaux Bluetooth :** Ce type de réseau permet de connecter entre eux les outils mobiles.

- **Les réseaux wifi :** L'utilisation de ce type de réseau est fréquente dans l'entreprise. Toutefois, il est à noter que les employeurs se montrent particulièrement vigilants. Néanmoins, les salariés font parfois preuve de moins de méfiance à l'égard de ces types de réseaux. Par conséquent, les risques pour l'entreprise peuvent être plus importants dès lors que les réseaux auxquels les salariés se connectent ne sont parfois pas sécurisés.

Ainsi, au-delà de la méconnaissance de la sécurité des réseaux par certains employeurs, d'autres risques internes peuvent se manifester lors de la perte ou d'un vol par exemple d'un terminal mobile et connecté sur lequel des informations professionnelles seraient stockées. En conclusion, il est possible d'affirmer que les risques internes semblent donc être très importants et nécessiter un véritable cadre juridique. C'est pourquoi, certains types de comportements font déjà l'objet de sanctions.

2) Un comportement, objet de sanctions

Le salarié fautif qui par une négligence impardonnable aurait porté atteinte aux données de l'entreprises peut faire l'objet d'un licenciement pour faute grave. A cet égard, il est important de souligner que d'après la jurisprudence, la faute grave résulte « d'un fait ou d'un ensemble de faits imputables au salarié qui constitue une violation des obligations résultant du contrat de travail ou des relations de travail d'une importance telle qu'elle rend impossible le maintien du salarié dans l'entreprise pendant la durée du préavis[84] ».

[84] Cass.soc.,26 février 1991, n°88-44.908

Le risque non-intentionnel qui se traduit en général par un comportement négligent de la part des salariés n'est pas le seul que les entreprises craignent. En effet, les dirigeants semblent de plus en plus s'interroger sur la malveillance intentionnelle de leurs propres « subordonnés ».

B) L'origine intentionnelle du risque : la malveillance interne, entre cyber criminalité et cyber vengeance

Il convient dans un premier d'identifier quels peuvent être les risques internes intentionnels (1) avant d'évoquer les sanctions dont peuvent faire l'objet les subordonnés qui se livreraient à des actes compromettant la sécurité de l'entreprise (2).

1) L'identification des risques

Lors de mes recherches sur le risque « intentionnel » en entreprise, j'ai pris connaissance d'une étude mondiale Fortinet dont les chiffres m'ont véritablement surpris. En effet, cette étude met en évidence les défis de sécurité posés par les salariés ayant adopté le BYOD. Elle révèle aussi le manque de prise de conscience de certains salariés à l'égard des problèmes liés à la sécurité. Selon cette étude qui me semble alarmante, « plus d'un tiers des interrogés se disent prêts à transgresser la politique de l'entreprise interdisant l'utilisation d'appareils personnels au travail ou à des fins professionnelles ». Toujours selon cette étude, « plus de 30% des personnes interrogées se disent prêtes à transgresser les règles posées par l'entreprise dans l'hypothèse d'applications non-autorisées[85] ».

Néanmoins, il me semble important de souligner qu'en France, il semble exister une véritable prise de conscience progressive de ces risques et de l'absence de prise en compte de ces derniers par certains organismes et salariés. En effet, l'ANSSI a publié un guide pour les salariés qui partent en mission ou en déplacement professionnel avec une tablette par exemple. Ce guide prend la forme d'un « passeport de conseils aux voyageurs ». Il s'agit ici d'une forme de sensibilisation aux risques de vol, de prise de contrôle ou de détournement d'un terminal mobile et connecté. L'objectif principal de l'ANSSI est de prévenir le risque. Cette intervention me semble pertinente et mérite d'être évoquée selon moi.

Par ailleurs, la jurisprudence s'est déjà prononcée sur la problématique de l'utilisation de périphérique dans le but de nuire de manière intentionnelle à l'entreprise. Ainsi, dans un arrêt

[85] LELOU (P.), « La génération Y adepte du BYOD pose des défis de sécurité », <finyear.com>, publié le 22 juin 2012

rendu par la Cour d'appel de Riom, le 12 février 2013[86], les juges ont considéré que le salarié qui consulte des données de nature confidentielles et qui les transfère sur une clé USB commet une faute grave. Cette jurisprudence met de nouveau en exergue les difficultés et les risques pouvant être entrainés par l'utilisation de supports ou d'outils mobiles et connectés, ou connectables. En outre, une cour d'appel, dans un arrêt rendu le 17 novembre 2008 a également reproché à un salarié d'avoir emporté chez lui une clé USB. Par ailleurs, la jurisprudence a aussi considéré que la rupture du contrat de travail est justifiée quand le salarié au moyen de clés USB professionnels transfère sur son ordinateur des films ou musiques téléchargées par lui illégalement. En outre, il a été également souvent été reproché à des salariés d'avoir copiés des documents appartenant à l'entreprise sur des clés USB[87] ».

Comme ces exemples permettent de l'illustrer, les outils liés à la mobilité sont au cœur d'importantes problématiques juridiques au sein de l'entreprise.

2) Les sanctions à l'égard du salarié

Le salarié qui soumet son entreprise à des risques par un comportement « intentionnel » et « malveillant » peut donc être sanctionné sur certains fondements. Ces derniers sont divers. Les notions de « vol de données » et « d'abus de confiance » sont toutefois fréquemment invoquées. Ainsi, un exemple permet d'illustrer mon propos.

Les juridictions ont jugé que l'information est susceptible de faire l'objet d'un vol, si celle-ci est reproduite sur un support, dont la soustraction serait l'objet du délit. Ainsi, l'article 323-3 du code pénal permet de poursuivre l'introduction, l'extraction, la détention, la reproduction ou la transmission frauduleuse de données contenues dans un système de traitement automatisé[88]. Traditionnellement, les juridictions françaises exigent « l'appréhension d'un support ». Ainsi, selon certaines juridictions l'une des conditions nécessaires à la caractérisation de l'infraction est la soustraction d'une chose. Ainsi, par exemple, une cour d'appel avait rejeté dans un arrêt du 24 juin 1987, le vol d'une onde hertzienne, en raison de sa nature immatérielle et en l'absence d'un quelconque support.

Toutefois, certaines juridictions dissocient le support matériel de l'information. Le vol de données informatiques est reconnu par la jurisprudence. Ainsi, dans un arrêt rendu le 9

[86] CA Riom, chambre civile 4, 12 février 2013, n°11-01.747
[87] CA Bourges, 15 octobre 2010 n°09/01531 – CA Paris 28 juin 2011 n°09/09327
[88] CULLAFROZ-JOVER (S.), et LUBET (P.), « La souplesse du droit face à l'usage croissant du BYOD : étude sur la gouvernance des données au sein de l'entreprise connectée », *Revue des Juristes de Sciences Po*, 1 Mars 2015

septembre 2003, la Cour de cassation a retenu la qualification de vol de données informatiques.

En 2008, la Cour de cassation s'est encore prononcée à propos du vol de fichiers informatiques, considérant que « peut-être condamné pour vol, celui qui soustrait non pas le support d'une information, mais celle-ci en la reproduisant sur son propre support[89] ».

Par ailleurs, dans un arrêt rendu par le TGI de Clermont Ferrand, le 26 septembre 2011[90], les juges ont apporté des précisions pertinentes sur la notion de « vol d'informations ». En effet, la loi du 5 janvier 1988 relative à la fraude informatique qui incrimine les atteints aux données informatiques comportait des lacunes sur la problématique du vol de données informatiques alors que les technologies de l'information semblent accentuer les risques[91].

En l'espèce dans l'arrêt du 26 septembre 2011, les faits étaient les suivants : une salariée avait transféré des informations confidentielles appartenant à son employeur à des fins personnelles. Dans cette décision, les juges ont considéré que l'infraction de vol pouvait être caractérisée. Cet arrêt a été confirmé par un arrêt rendu par la CA de Paris le 5 février 2014 qui reconnaît que l'infraction de vol peut s'appliquer à des fichiers informatiques même s'ils n'ont pas été copiés sur un support ayant également fait l'objet d'une soustraction.

Le TGI de Versailles a également condamné il y a quelques années une stagiaire chinoise pour abus de confiance. En l'espèce, la stagiaire avait accédé et téléchargé sur son disque dur des fichiers confidentiels appartenant à la société[92]. Enfin, la Cour de cassation a également par le passé condamné un salarié pour usager personnel d'un matériel mis à sa disposition par l'employeur en vue de la consultation de sites pornographiques. En l'espèce, la Haute-juridiction a caractérisé « l'abus de confiance[93] ».

§2- Les risques externes à l'entreprise

L'entreprise est également exposée à des risques externes (A), qu'elle peut toutefois tenter d'éviter en respectant un certain nombre d'obligations en vue de prévenir ces risques (B).

[89] Cass. Crim 4 mars 2008, n°07-84.002
[90] TGI Clermont-Ferrand, ch.corr., 26 septembre 2011
[91] CAPRIOLO (E.), « Condamnation pour vol et abus de confiance d'une ex-salariée ayant transféré des fichiers sur une clé USB », *CCE*, mars 2012, n°3, p.39-42
[92] TGI de Versailles du 18 décembre 2007
[93] Cass.crim, Nortel, 15 mai 2004

A) L'identification des risques

Le fait d'adopter une solution « BYOD » peut avoir pour conséquence de favoriser les risques externes à l'entreprise et les menaces provenant de l'extérieur.

Ainsi, ces risques externes sont également appelés « risques invisibles ». Il peut s'agir entre autres de virus, de malware, de « vols de fichiers et de documents, d'usurpations d'identités numériques », d'enregistrements téléphoniques, du « pillage informationnel » du patrimoine immatériel de l'entreprise ou bien « d'une entrave des systèmes d'information ».

B) Les obligations en vue de la prévention des risques

Il est important de rappeler ici qu'en amont, l'entreprise, et plus précisément le responsable du traitement de données se voit imposer un certain nombre d'obligations, parmi lesquelles : l'obligation de sécurisation des réseaux et des systèmes afin de protéger les données contenues ou y transitant. Ces obligation sont notamment posées entre autres par l'article 34 de la loi du 6 janvier 1978 ainsi que par l'article 226-17 du Code pénal qui dispose : « *Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n°78-17 du 6 janvier 1978 est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende* ». Cette obligation sous-entend entre autres la prise en compte des risques d'hébergement en cloud que nous avons vu précédemment.[94] En outre, il appartient également à l'employeur de s'assurer de la sécurité des réseaux, notamment de l'accès à internet.

Par ailleurs, la problématique de la cybercriminalité est également prise en compte au niveau européen. A titre d'illustration, il est possible d'évoquer la proposition de directive concernant des mesures destinées à assurer un niveau élevé de sécurité des réseaux et de l'information dans l'Union[95]. Ce projet prévoit notamment entre autres une extension de l'obligation de notification à tous les types de données. De plus, il évoque également l'obligation pour certains types d'infrastructures critiques d'adopter des mesures nécessaires pour gérer les risques de sécurité. Enfin, le projet de règlement européen relatif aux données personnelles de

[94] SOUVIRA (A.), « La cyber sécurité des entreprises », *Lamy droit de l'immatériel*, *op.cit*, 2013
[95] Proposition de directive COM(2013) 48 final) 07/02/2013

2012 quant à lui prévoit une obligation de notification dans les meilleurs délais à l'autorité nationale compétente des violations graves de données personnelles[96].

Comme nous l'avons vu dans le cadre de ce premier chapitre, la mise en place de terminaux mobiles et connectés soulève de nombreuses problématiques relatives d'une part à la gestion des données personnelles et professionnelles par l'employeur ainsi que s'agissant de la confidentialité et de la sécurité des données face aux risques internes et externes. Toutefois, ce ne sont pas les seules problématiques que l'employeur doit gérer puisque celui-ci doit également s'informer précisément sur les règles relatives à la propriété intellectuelle, en vue d'éviter que sa responsabilité soit engagée du fait d'un usage illicite d'un terminal.

Chapitre 2. L'atteinte aux droits de propriété intellectuelle du fait de l'usage illicite d'un terminal

L'utilisation de terminaux connectés et mobiles peut également avoir une influence en matière de droits de propriété littéraire et artistique. C'est pourquoi, j'ai choisi d'évoquer dans une première sous-partie deux thématiques qui peuvent se poser relativement à ce droit : d'une part, le téléchargement illicite en entreprise qui comme on le verra peut présenter un risque également pour l'employeur de voir sa responsabilité engagée. En outre, les principes relatifs à la problématique de la création sur un terminal connecté seront également évoqués puisqu'il s'agit d'une question qui peut également être soulevée dans le cadre du développement des outils mobiles et connectés (**Section 1**). Par ailleurs, la problématique de la gestion des licences se pose également pour l'employeur afin d'éviter des risques d'engagements de sa responsabilité. C'est pourquoi, dans le cadre d'une seconde sous-partie, j'évoquerai des solutions possibles en vue de la prévention de ces risques (**Section 2**).

[96] JOLY(C-R.), «CYOD/BYOD : Quels outils pour une gestion maîtrisée de la mobilité en entreprise ? », 16/06/2013,<www.ulys.net> , p.10

Section 1. Les usages en termes de propriété littéraire et artistique

Les enjeux en matière de gestion des droits de propriété littéraire et artistique concernent aujourd'hui particulièrement la gestion du téléchargement illicite. Il s'agit ici d'une problématique qui n'est pas nouvelle, et qui se posait déjà. Toutefois, avec le développement de la mobilité, les enjeux et risques semblent aujourd'hui plus importants (**paragraphe 1**).

La gestion de la propriété de l'œuvre réalisée sur un terminal connecté est également une problématique importante pour l'employeur (**paragraphe 2**).

§1 - Le téléchargement illicite

Le téléchargement illicite est une pratique qui pose également problème dès lors qu'il a lieu sur le lieu de travail ou sur des terminaux appartenant à l'entreprise. Par conséquent, nous verrons que les risques qui peuvent exister semblent parfois exacerbés par le développement du BYOD ou des autres formes de mobilité (A). Ainsi, la pratique du téléchargement illicite

fait peser le risque d'une condamnation pénale, pouvant être très lourde pour l'employeur. C'est pourquoi, l'entreprise doit se montrer particulièrement vigilante (B).

A) L'augmentation des risques en matière de respect des droits de propriété intellectuelle des tiers

Le téléchargement illicite représente une véritable problématique à gérer pour l'employeur en France. Ce phénomène tend à augmenter avec le développement des différents types de mobilité (1).

L'Italie est également un pays qui tente de faire face à ce problème, bien que la problématique ne se limite pas simplement au cadre professionnel. En effet, la répression de cette pratique même est au cœur d'un véritable débat que nous évoquerons dès lors que la problématique du téléchargement illicite revêt une importance considérable. Son appréhension par le droit connaît toutefois des difficultés (2).

1) Le téléchargement illicite en entreprise en France

L'employeur se doit d'être attentif à la problématique du téléchargement illicite en entreprise. En effet, il est important de rappeler que l'employeur est responsable du réseau Internet qu'il met à disposition de ses salariés[97].

Ainsi, c'est à lui de s'assurer que les salariés ne téléchargent pas de contenus illicites. A défaut, il lui appartient de s'expliquer devant la Commission de Protection des Droits de l'Hadopi[98].

Selon un rapport très récent remis au Sénat en juillet 2015, la moitié des téléchargements illicites émane aujourd'hui d'IP professionnelles. Ce rapport souligne notamment que « le risque d'exposition à une suspension d'abonnement pour une entreprise est proportionnel au nombre de collaborateurs qui sont connectés dans l'entreprise ». Ce rapport dénonce

[97] PASSET (M.), VERDEL (C.), NAUGES (L.), *BYOD : réussir son intégration dans l'entreprise, op.cit,* 2014, p.113

[98] ACATRINEI- ALDEA (T.), « Le BYOD et le droit : le couple mal assorti », publié en mars 2014, www.connect.ed-diamond.com

également certaines lacunes de la loi HADOPI 2, notamment le fait que cette loi s'intéresserait plutôt au téléchargement à partir d'IP de particuliers et que les entreprises ignorent parfois les principes en vigueur. Ainsi, une obligation de sécurisation de l'accès internet pour la protection de la propriété littéraire et artistique sur internet s'impose dès lors que l'employeur peut être poursuivi pour négligence caractérisée. La contravention de négligence caractérisée, selon l'HADOPI, peut être constituée dès lors « qu'un abonné s'est abstenu sans motif légitime de mettre en place un moyen de sécurisation ou a manqué de diligence dans la mise en œuvre de ce moyen ». Ainsi, il peut s'agir par exemple du fait pour une entreprise de ne pas avoir mis en place des « spécifications organisationnelles » telles que des chartes ou des sessions de sensibilisation[99].

Face au développement du BYOD et du CYOD, le salarié peut être amené à télécharger des contenus illicites sur son terminal personnel ou sur le terminal qui lui a été confié par son entreprise.

A cet égard, Pierre Poggi, dirigeant d'une société informatique interrogé sur la problématique du téléchargement illicite en entreprise soutient que l'augmentation du nombre de téléchargements illicites au sein du milieu professionnel peut s'expliquer par le fait que « de nombreux salariés après avoir été avertis une première fois à la suite d'un téléchargement dans un milieu personnel sont tentés de se cacher derrière le réseau de leur entreprise », car bien souvent ils ignorent les risques qu'ils peuvent encourir et faire encourir à leur employeur. Les fichiers téléchargés sont ensuite, selon lui, soit transférés vers le cloud ou bien enregistrés sur une clé USB par exemple. En outre, il souligne que ce phénomène concerne maintenant également les smartphones[100].

2) Focus sur la situation du téléchargement illicite en Italie

Dans le cadre de l'approche en droit comparé que j'ai souhaité suivre dans le cadre de ce mémoire, j'ai souhaité faire un focus sur la situation du téléchargement illicite en Italie, appelé « download illegale ». L'Italie est l'un des pays qui est souvent montré du doigt eu égard à sa législation en matière de protection des droits de propriété intellectuelle. Elle fait partie des pays où le téléchargement illicite est le plus important et elle connaît des difficultés

[99] LOIC (H.) et BOUCHOUX (C.), « Loi HADOPI : totem et tabou », rapport d'information n°600 (2011/2015) du 8 juillet 2015 fait au nom de la Commission de la culture, de l'éducation et de la communication, p. 55
[100] CALIXTE (L.), « Téléchargement illégal en entreprise : quels risques pour les salariés et pour l'employeur ?, publié en février 2014, <www.challenges.fr>

pour endiguer ce phénomène. Ainsi, nombreux sont les détracteurs des différentes réformes face aux résultats qui n'ont pas été satisfaisants. Certains se montrent très critiques et n'hésitent pas à qualifier le peuple d'italiens, de « peuple du téléchargement illicite ».

En effet, il apparait que les principes régissant ce phénomène sont encore parfois flous, et également surtout méconnus par les individus. A cet égard, la jurisprudence s'est par exemple fréquemment montrée hésitante sur le fait de savoir si le téléchargement illicite était une activité devant être punie quand bien même il n'y aurait pas un but lucratif, dès lors que certains juges ont énoncé que le téléchargement illicite dès lors qu'il n'a pas un but lucratif n'est pas puni(voir en ce sens, décision de la cour de cassation italienne 149/2007). Certains soulignent qu'il est important de rappeler l'existence de la loi du 21 mai 2004 sur la protection du droit d'auteur dite « Urbani » entrée en vigueur en 2005 qui met en cause la responsabilité des auteurs de téléchargement, ainsi que la loi n°633 du 22 avril 1941 sur la protection des droits d'auteurs et des droits voisins. L'article 174 ter dispose : « *Chiunque abusivamente utilizza, anche via etere o via cavo, duplica, riproduce, in tutto o in parte, con qualsiasi procedimento, anche avvalendosi di strumenti atti ad eludere le misure tecnologiche di protezione, opere o materiali protetti, oppure acquista o noleggia supporti audiovisivi, fonografici, informatici o multimediali non conformi alle prescrizioni della presente legge, ovvero attrezzature, prodotti o componenti atti ad eludere misure di protezione tecnologiche è punito* ». Cet article signifie que : toute personne qui utilise également, même par voie de câble ou hertzienne qui duplique, reproduit, en tout ou partie, par n'importe quel procédé en utilisant par exemple des outils permettant de contourner les mesures techniques de protection des œuvres ou d'autres objets protégés doit être punie. Lé décision jurisprudentielle rendue en 2007 a été très critiquée. Toutefois la SIAE qui est la société en charge de la protection des droits d'auteur en Italie est intervenue et a rappelé que les faits datant de 1999, date à laquelle la directive européenne de 2001 n'avait pas été transposée, cette décision ne pourrait plus s'appliquer de nos jours.

Face à ces hésitations, il est également possible de souligner un manque d'informations et de connaissances des italiens sur les risques qu'ils prennent face à une telle pratique, y compris au sein du milieu professionnel. A titre d'illustration, il est possible de citer une étude menée par l'observatoire Lorien Consulting[101] très récemment portant sur la pratique du téléchargement illicite en Italie. Menée sur 1000 adultes italiens, elle révèle que seulement 14% affirment savoir que « le téléchargement d'œuvres protégées par le droit d'auteur et

[101] Lorien Consulting, avril 2015

téléchargées sur internet sans l'autorisation du titulaire des droits constitue une violation de la loi, 22% ignorent qu'il s'agit d'un comportement contraire à la loi, et plus étonnant encore, 39 % le considère comme un « comportement illicite mais tolérable ». Cette étude est intéressante dès lors qu'elle révèle que 10 à 12 % des personnes interrogées disent savoir que « quelqu'un télécharge illicitement au sein de leur entreprise », « 1,4% dit savoir que quelqu'un télécharge illicitement de la musique, 1,6% des films, et 2,7% des software ». Ainsi, le téléchargement de logiciels est le type de téléchargement le plus important selon cette étude au sein des entreprises italiennes. En effet, il apparaît que le téléchargement de musique ou bien de films peut sembler plutôt réservé à un usage « dans un cadre personnel ». A cet égard, il peut de nouveau être opportun de faire une comparaison avec la situation en France. En effet, selon Pierre Poggi, directeur d'une société informatique, en France les salariés n'hésitent pas à télécharger des films également « pendant leur pause déjeuner ».

C'est pourquoi, il me semble important de revenir sur les principes régissant la responsabilité de l'employeur face à ces faits qui se révèlent de plus en plus fréquents au sein des entreprises.

B) Les risques en matière de responsabilité

Le droit du travail qui est un droit en faveur de la protection du salarié encadre le licenciement d'un salarié pour faute grave en raison de la violation par un salarié sur son lieu de travail de la propriété intellectuelle. En effet, il est de plus en plus fréquent que les salariés commettent des délits en utilisant les outils mis à disposition par l'employeur.

L'article L336-3 du Code de propriété intellectuelle prévoit une obligation de surveillance de l'accès à internet. Ainsi, l'article dispose : « *La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise* ». Par conséquent, la responsabilité de l'employeur peut être engagée dans ce type d'infraction. En cas d'une utilisation illégale d'Internet, l'entreprise reçoit l'injonction de mettre fin au manquement qui est constaté et doit en rendre compte à l'HADOPI. Il est

nécessaire que l'entreprise mette en place des solutions de protection. Or, il s'avère aujourd'hui que nombreuses sont les entreprises qui sont négligentes à cet égard.

La jurisprudence s'est également déjà prononcée sur ce type de litige. Ainsi, dans un arrêt rendu le 31 mars 2011, qui concernait le licenciement d'un salarié pour téléchargement illicite, la Cour d'appel de Versailles[102] a déclaré que « *la violation de la propriété intellectuelle par un salarié sur son lieu de travail en utilisant les ressources de l'entreprise constitue une faute grave* ». En l'espèce, le salarié avait effectué à partir du poste mis à sa disposition par l'employeur, des téléchargements illicites. Dans cet arrêt, la Cour d'appel a déclaré la solution justifiée.

Il est intéressant de souligner que cet arrêt a été confirmé puis précisé par un arrêt rendu le 29 octobre 2014. En l'espèce, l'arrêt rendu par la Cour de cassation le 29 octobre est important car il est venu préciser dans quelles conditions la faute grave peut être caractérisée dans l'hypothèse de téléchargements illicites au sein d'une entreprise.

Les faits étaient les suivants : un salarié avait été licencié pour faute grave en raison de téléchargements illégaux et répétitifs au sein de son entreprise. Le salarié licencié a saisi le conseil des Prud'hommes. Au sein d'un arrêt très médiatisé, les juges de la Haute-juridiction ont estimé que le licenciement était « sans cause réelle et sérieuse » dès lors « qu'aucune preuve du téléchargement n'était apporté ». Par conséquent, la Cour de cassation a confirmé la décision des juges d'appel.

En résumé, le téléchargement illicite fait peser sur le salarié un risque de licenciement pour faute grave à condition toutefois d'apporter la preuve du téléchargement comme l'a rappelé très récemment la jurisprudence. Par ailleurs, il peut également faire peser un risque sur l'employeur. Ce dernier pouvant en effet voir sa responsabilité engagée s'il ne sécurise pas son réseau et s'il ne veille pas à éviter l'usage illicite de celui-ci.

L'HADOPI est un système qui fait l'objet de vives critiques, toutefois certaines initiatives méritent d'être soulignées et sont importantes pour l'employeur. Ainsi, un accompagnement est aujourd'hui offert aux professionnels qui ont été victimes de « piratage » avec des solutions techniques pour éviter la réitération de ces faits illicites au sein de leurs locaux ainsi que des messages de sensibilisation à faire circuler pour les salariés[103].

[102] CA de Versailles, 5e ch., 31 mars 2011, Michael P.C./Mireille B.P.
[103] LOIC (H.) et BOUCHOUX (C.), « Loi HADOPI : totem et tabou », rapport d'information n°600 (2011/2015) du 8 juillet 2015 fait au nom de la Commission de la culture, de l'éducation et de la communication, p.56

Ainsi, la problématique concernant le respect des droits de propriété intellectuelle n'est pas nouvelle mais il me semble important de l'évoquer puisqu'elle se pose également avec le BYOD et le CYOD, dès lors que l'entreprise met à la disposition des salariés des outils mobiles et connectés ou qu'elle leur permet d'apporter leurs propres outils. En effet, l'entreprise doit se protéger face au risque de téléchargements illicites pouvant dans certains cas conduire à l'engagement de sa responsabilité.

§2 - La problématique annexe relative à la propriété de la création réalisée sur un terminal connecté

Il convient préalablement de rappeler les principes généraux relatifs à la création d'œuvre sur un terminal appartenant à l'entreprise (A) avant d'évoquer plus particulièrement les problématiques qui peuvent se poser dans le cadre de l'adoption de solutions de mobilité (B).

A) Le rappel des principes généraux

Le BYOD et les politiques de mobilité peuvent soulever d'autres problématiques liées à la propriété littéraire et artistique. L'une qui peut se poser est celle relative à la propriété d'un contenu ou d'un logiciel crée sur un matériel personnel ou mis à disposition par l'employeur.

Au sein d'un livre blanc consacré au BYOD, le cabinet d'Avocats Mathias a entre autres mis en évidence cette problématique. Le Cabinet a souligné que le BYOD rendrait plus complexe l'attribution des droits dans certaines hypothèses.

Selon le Code de la propriété intellectuelle, le titulaire des droits d'auteurs sur une œuvre est son auteur. Par ailleurs, l'auteur même salarié reste titulaire des droits sur son œuvre créée dans le cadre du contrat de travail. En effet, c'est la fameuse jurisprudence Nortene du 16 décembre 1992 qui a posé le principe de neutralité du contrat de travail.

Dans certaines hypothèses, l'employeur peut être titulaire des droits. Ainsi, ce sera le cas dès lors que l'œuvre est un logiciel. Il s'agit ici d'un régime dit « spécial » dans lequel le principe de « neutralité » du contrat de travail n'a plus vocation à s'appliquer. L'existence du contrat de travail influence dans cette hypothèse la titularité des droits.

L'article L113-9 du code de la propriété intellectuelle vise les logiciels créés par des salariés dans l'exercice de leur fonction ou d'après les instructions de leur employeur. Il s'agit ici d'une formule très large, souvent présentée comme plutôt favorable à l'employeur. Ainsi, si le salarié souhaite revendiquer la titularité de ses droits, il doit parvenir à prouver que le logiciel a été créé sur son temps de pause ou qu'il n'a pas utilisé les moyens mis à sa disposition par son employeur[104].

Ce sera également le cas si l'œuvre a été réalisée par plusieurs salariés ou bien s'il y a eu cession des droits.

B) La problématique soulevée par le BYOD

Auparavant, il semblait donc beaucoup plus simple de déterminer la propriété d'un contenu sur les appareils appartenant à l'entreprise et mis à la disposition des salariés. Il était alors beaucoup plus facile pour l'employeur de revendiquer la titularité des droits.

Or, avec le BYOD, la situation est devenue beaucoup plus compliquée et il est possible de s'interroger sur l'hypothèse d'un salarié qui aurait créé un contenu ou un logiciel par le biais d'un outil personnel en dehors des heures de travail sur son temps et lieu de travail par exemple. [105]

Toutefois, en application des principes énoncées ci-dessus, dans l'hypothèse où le logiciel serait créée dans le cadre d'une politique « COPE », le salarié pour revendiquer la titularité des droits devra prouver que le logiciel a été créé pendant son temps de pause car en effet le CYOD implique la mise à disposition d'un terminal par l'employeur.

S'agissant du BYOD, il s'agit ici d'une problématique ici à laquelle il conviendrait d'apporter rapidement une réponse car elle soulève de nombreux enjeux.

[104] Cours de droit de la propriété littéraire et artistique dispensé par M. Nicolas BRONZO dans le cadre du Master I Droit et management de la culture et des médias, Université Aix-Marseille
[105] Livre Blanc « BYOD, un défi juridique à anticiper », cabinet d'Avocats MATHIAS, *op.cit*, p.10

Section 2. Les usages illicites en matière de logiciel

Face au BYOD et aux autres formes de mobilité, la gestion des licences de logiciel peut apparaître problématique (**paragraphe 1**). Toutefois, nous verrons que des solutions émergent et semblent se dessiner (**paragraphe 2**).

§1- La problématique de la gestion des licences de logiciel

Par définition, une licence est un contrat qui permet de définir les conditions d'utilisation, de diffusion et de modification d'un programme. Le suivi des licences est plus compliqué dès lors que le terminal mobile et connecté n'est pas la propriété de l'entreprise. Le risque de se voir poursuivi en raison de mauvais usages est présent[106] et pourtant souvent ignoré par les employeurs. En outre, il est opportun de rappeler que la gestion des licences ne doit pas être une problématique laissée de côté par l'entreprise, car les éditeurs font de plus en plus de contrôle et d'audit à l'égard de leurs clients.

La problématique de la gestion des logiciels est souvent sous-estimée par les entreprises qui ne prennent pas en compte l'impact que peut avoir le BYOD sur les licences de logiciels. En principe, l'entreprise devrait s'assurer qu'elle est en possession de licences suffisantes pour chaque logiciel sur son réseau.

Il incombe donc à l'entreprise d'effectuer un inventaire des applications qui sont utilisées dans le cadre professionnel ainsi que de procéder à la vérification des conditions d'utilisation de chaque licence[107].

Il est également important de vérifier si les licences autorisent ou non un accès à distance aux applications par le biais des appareils personnels des salariés, dès lors que certaines le permettent tandis que d'autres peuvent le prohiber. La problématique qui se pose est la suivante : parfois, les licences ne sont valables que pour les outils qui sont la propriété de l'entreprise. Par principe, régulièrement elles ne peuvent pas s'étendre aux smartphones ou tablettes qui sont la propriété des salariés. Le BYOD présente donc un risque : certaines

[106]DESJARDINS (C.), « BYOD : Panorama des risques juridiques pour l'entreprise », publié le 1 mars 2013, www.business.lesechosfr

[107] Livre Blanc Microsoft, GRASSET (J.), Bring Your Own Device, Vision sécurité et approche des solutions, Microsoft France, septembre 2013, p.11

pratiques peuvent caractériser une contrefaçon de logiciel.[108] Historiquement, il été constaté que les fournisseurs de solutions de gestion des licences ne se sont pas intéressés à la pratique du BYOD. Ainsi, cela a renforcé les difficultés rencontrées par les entreprises pour assurer la conformité de l'utilisation des licences[109]. Il est très important de distinguer d'une part l'usage personnel et d'autre part, l'usage professionnel. En effet, en cas de litiges relatifs à la gestion de logiciels, la responsabilité pèsera sur l'entreprise[110].

L'employeur doit aussi envisager l'hypothèse où un employé utilise son propre ordinateur pour travailler depuis son domicile. En effet, dans le cas où le salarié utilise une version « Familiale et étudiant », la licence en principe exclut une utilisation à visée commerciale. [111] En outre, dès lors qu'un logiciel de l'entreprise est installé sur l'équipement propriété du salarié, si le salarié quitte l'entreprise et que le logiciel continue d'exister sur son terminal, il apparaît que la société ne respecte probablement plus le contrat qui a été signé.

La Haute-juridiction française s'est prononcée très récemment sur la problématique de la gestion des licences dans un arrêt M.X c/ Fico graphie rendu le 16 juin 2015 relatif au licenciement d'un salarié pour usage de logiciels sans licence. L'analyse de cette jurisprudence me semble importante dans le cadre de ce mémoire, dès lors que cette problématique peut concerner le BYOD. Le principe qui a été posé par cet arrêt est le suivant : l'utilisation et la modification d'un logiciel sans licence par un salarié dans le cadre de son travail peut être une cause réelle et sérieuse de licenciement, toutefois il faut que que cela n'ait pas été demandé par l'employeur. En l'espèce, le salarié affirmait que l'utilisation du logiciel s'était faite au vu et au su de l'employeur, et même à sa demande. Le salarié a été licencié pour faute grave pour avoir téléchargé et utilisé sans droit le logiciel. La CA d'Aix n'a pas retenu la faute grave du salarié, en l'absence de preuve sur le fait qu'il ait procédé lui-même au téléchargement illicite. Les juges d'appel ont cependant estimé qu'il avait eu un comportement fautif, constituant une cause réelle et sérieuse de licenciement pour avoir procédé à la modification du logiciel et l'avoir utilisé. La décision des juges d'appel est censurée par ceux de la Haute-juridiction.

[108] Livre blanc, Cabinet d'avocats Mathias, Livre blanc BYOD : un défi juridique à anticiper, *op.cit,* p.10
[109] Popihn (P.Y), « BYOD : Bring Your Own Disaster ? Comment le rêve de toute organisation peut tourner au pire cauchemar », publié le 15 octobre 2014, www.smart-webzine.com,www.infodsi.com
[110] PASSET (M.), VERDEL (C.), NAUGES (L.), *BYOD : réussir son intégration dans l'entreprise*, *op.cit*, p.138
[111] GILMORE (G.), BEARDMORE (P.), *Sécurité mobile et BYOD pour les nuls*, Kaspersky lab, John Wiley & Sons, Ltd., p.35

§2- Des solutions potentielles pour la gestion des licences de logiciels

Aujourd'hui, face au succès rencontré par les nouvelles formes de mobilité, les sociétés spécialistes dans le domaine du management des risques et de la sécurité de l'information se montrent particulièrement actives. Ainsi, celles-ci n'hésitent pas à prodiguer un certains nombres de conseils à l'égard de l'employeur en matière de gestion de logiciels. A titre d'illustration, la société WIDE ANGLE par exemple préconise aux employeurs : de respecter les accords de licence, de garantir aux utilisateurs un accès aux logiciels dont ils ont besoin et d'acheter uniquement le nombre de licences nécessaires. En effet, certains entreprises font le choix de licences collectives alors qu'elles n'ont ont pas besoin. En outre, les éditeurs quant à eux réfléchissent aussi à l'adoption de nouvelles solutions. C'est le cas par exemple de Microsoft qui a récemment lancer un nouveau modèle de licence qui permet de couvrir plusieurs terminaux par utilisateurs afin de permettre un accès à des terminaux privés.

Face aux difficultés soulevées en matière de gestion des logiciels, il est à noter que de nouvelles idées ont pu émerger ces dernières années : c'est le cas notamment des licences dites « *open hardware* », en français « licences matériels libre ». « L'open hardware » renvoie aux « matériaux dont la conception peut être reproduite car toutes les informations nécessaires à leur construction sont en libre accès ». La piste des licences « open hardware » pourrait donc être envisagée dans la mise en œuvre d'une politique BYOD. Elles peuvent être utiles aux salariés qui travaillent sur des projets personnels et professionnels. Elles favorisent aussi l'échange des données.

En résumé, comme nous l'avons vu dans le cadre de la première partie de ce mémoire, les solutions de mobilité qui aujourd'hui prennent de plus en plus d'importance au sein des entreprises présentent de nombreux risques pour l'employeur. Ce dernier est très souvent réticent à accepter ces politiques de mobilité malgré les avantages qu'elles peuvent présenter. Il me semble donc important de renforcer l'information relative aux risques juridiques qui ont été énoncés au sein de cette première partie. Ces risques sont importants en matière notamment de protection des données personnelles qui est un thème au cœur de l'actualité, de cybercriminalité, thème très important pour la sécurité des entreprises face aux attaques de plus en plus nombreuses et en matière de propriété intellectuelle.

Par conséquent, la crainte de certains dirigeants eu égard aux nombreux risques peut donc être justifiée. Néanmoins, il est important de souligner que ce type de « mobilité » présente aussi

des risques pour les salariés. C'est pourquoi, il me paraît plus opportun « d'appréhender, d'anticiper » et d'encadrer ces risques au lieu d'interdire formellement ces nouvelles formes de mobilité qui ont vocation à s'implanter peut-être durablement au sein des entreprises françaises et qui s'inscrivent dans l'évolution du numérique et du milieu professionnel.

PARTIE 2.

LA MISE EN PLACE DE TERMINAUX MOBILES ET CONNECTÉS DANS LE MILIEU PROFESSIONNEL : LA NÉCÉSSITÉ D'UN ENCADREMENT JURIDIQUE FACE À UNE POLITIQUE A RISQUES POUR LE SALARIÉ

Le développement de solutions de mobilité semble de manière incontestable accroître la porosité entre la sphère privée et la sphère publique alors que le « *Privacy Paradox* » peut parfois être constaté aussi bien en France qu'en Italie. L'approche en droit comparé que j'ai choisie de suivre dans le cadre de ce mémoire nous permettra de mettre en exergue l'appréhension de la notion de « vie personnelle » dans ces deux pays, avant d'étudier les problématiques qui se posent dorénavant liées à l'utilisation des outils permettant la mobilité, notamment celle du contrôle de ces outils. Nous verrons dans le cadre de cette partie que la notion de « vie privée » apparaît floue tant en droit français qu'en droit italien. (**Chapitre 1**).

Les outils liés à la mobilité semblent également accroître l'intensité de la connexion des salariés. Ainsi, les revendications liés à un « droit à la déconnexion » qui puisse être véritablement consacré sont de plus en plus nombreuses. Progressivement, le nombre de défenseurs de ce droit augmente de façon exponentielle. Si ce droit n'a pas encore fait l'objet d'une appréhension juridique en Italie, nous verrons qu'en France, les problématiques liées à l'hyper-connexion prennent de plus en plus d'importance et s'imposent aujourd'hui de plus en plus dans le milieu professionnel (**Chapitre 2).**

Chapitre 1. Vers une dangereuse réduction de la frontière entre les sphères personnelle et professionnelle

Le développement d'outils de mobilité dans un premier temps peut conduire à ce que les atteintes à la vie privée des salariés soient de plus en plus fréquentes. En effet, la présence croissante du numérique dans les relations de travail peut avoir des conséquences sur les droits et libertés qui régissent celles-ci, notamment : le droit au respect de la vie privée des travailleurs[112]. C'est pourquoi, il semble nécessaire de délimiter le cadre juridique et principalement de définir les règles s'agissant du contrôle par l'employeur de ces outils, en vue de protéger la vie « personnelle » du salarié. Dans le cadre de cette sous-partie, nous verrons que la loi et la jurisprudence ont à cet égard évolué en vue de trouver un équilibre qui peut s'avérer plus ou moins « juste » entre le respect des droits fondamentaux du salarié et la

[112] Etude annuelle 2014 du Conseil d'Etat, « Le numérique et les droits fondamentaux », Edition La Documentation Française, Etudes et documents, septembre 2014, p.384

reconnaissance du pouvoir de contrôle de l'employeur. Nous verrons dans le cadre de cette sous-partie que ce juste équilibre fait aujourd'hui débat. **(Section 1**).

Il semble également important de délimiter de façon plus précise les règles applicables en matière de géolocalisation et de surveillance. En effet, les outils de mobilité peuvent soulever de nombreuses problématiques juridiques auxquelles il convient d'apporter des éléments de réponse. Dans ce cadre, j'ai souhaité au sein de cette sous-partie faire une approche en droit comparé des règles applicables dans ce domaine en France, puis en Italie afin de mettre en exergue les ressemblances ou les différences entre ces deux droits (**Section 2**).

Section 1. Le risque d'atteintes à la vie privée accru par la mise en place de terminaux mobiles et connectés

Les terminaux mobiles et connectés sont souvent accusés de mettre en danger la vie « personnelle » du salarié dès lors que l'employeur exerce son pouvoir de contrôle sur ces outils. Le salarié en vue de garantir ses libertés est protégé par le droit du travail et bénéficie d'un droit à la « vie personnelle » consacré par des textes, qui en principe se doit d'être le plus effectif. Toutefois, selon certains, les TIC et les outils liés à la mobilité favoriseraient le « *fil à pattes* », c'est-à-dire l'intrusion dans la vie privée des salariés[113] (**paragraphe 1**). Ainsi, la liberté du salarié n'est toutefois pas absolue et peut se voir encadrée par le pouvoir de contrôle dont dispose l'employeur (**paragraphe 2**).

§1 - Le droit à la vie privée du salarié consacré

[113] ANONYME, « Qualité de vie au travail : transformer la contrainte en opportunité », *Les Cahiers du DRH* 2014, n°125, 1 décembre 2014, p.18

La consécration du droit à la vie privée qui semble « glisser » progressivement vers la notion de vie personnelle a été progressive tant en France comme en Italie (A). Aujourd'hui, l'effectivité de ce droit est réduite selon certains en raison du développement de l'utilisation des terminaux mobiles et connectés (B).

A) L'affirmation du droit à la vie privée

La vie privée est une notion qui a été appréhendée en France (1) mais également en Italie (2).

1) En France

Par principe, l'exercice d'une activité professionnelle conditionne le salarié à l'obligation de se soumettre au pouvoir de l'employeur[114]. Toutefois cette subordination ne lui retire pas le droit au respect de sa vie privée. Ainsi, comme le rappelle très justement Monsieur Stéphane Bouche au sein d'un mémoire consacré au pouvoir de l'employeur en droit comparé français et italien qui cite le juriste Jean Savatier : *« Le progrès de la liberté des travailleurs, c'est tout d'abord le refus du paternalisme de l'employeur et de ses ingérences dans la vie privée du salarié »*.[115] Le respect de l'intimité de la vie privée du salarié s'impose à l'employeur sur le temps et le lieu de travail. Ainsi, il est important de rappeler que le salarié qui se trouve dans un lien de subordination à l'égard de l'employeur demeure un citoyen. C'est pourquoi, les atteintes à ses droits et libertés ne sont légitimes que si elles sont proportionnées au but recherché. [116]A cet égard, le développement des NTIC a pu soulever des problématiques dès lors qu'elles ont offert à l'employeur des « nouveaux moyens de surveillance », parfois très critiqués.

La notion de « vie privée » du salarié est souvent au cœur de l'actualité. Très fréquemment, les nouvelles technologies dans le milieu professionnel sont pointées du doigt car on les accuse de porter atteinte à la vie privée des salariés eu égard à leur caractère fortement intrusif. Le droit du travail évolue très rapidement mais certains ont pu mettre en évidence que les juristes semblent fréquemment dépassés par cette évolution très rapide[117], comme en témoigne aujourd'hui l'absence d'encadrement des solutions de mobilité pouvant

[114] PANSIER (F-J.), *Droit du travail,* 6e edition, LexisNexis, p.128
[115] BOUCHE (S.), *Droits et libertés du salarié comme limites au pouvoir disciplinaire de l'employeur en droit français et en droit italie*n, consultable en ligne sur le site <www.juripole.com>
[116] MOULY (J.), *Droit du travail*, 6e edition, Lexifac DROIT, p.117
[117] PIZZIO – DELAPORTE (C.), *Droit du travail*, 2e édition, VUIBERT Droit, p.16

être adoptées en entreprise. La protection de la vie privée a quant à elle été affirmée en 1948 par l'article 12 de la Déclaration universelle des droits de l'homme des Nations Unies qui dispose « *nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* ». Au niveau du droit interne, cette notion est également protégée par l'article 9 du Code civil en France qui dispose : « *Chacun a droit au respect de sa vie privée* ».

Toutefois, il me semble important de souligner que la notion a beaucoup évolué. C'est pourquoi elle peut apparaître aujourd'hui difficile à définir. L'opposition traditionnelle de la sphère privée à la sphère publique semble véritablement de nos jours, obsolète. Selon Antoinette ROUVROY, docteur en sciences juridiques, certaines tendances remettent en cause la notion traditionnelle de sphère privée, parmi lesquelles : « l'irréversibilité croissante des dispositifs, la confusion croissante des temps sociaux et intimes et des temps de travail ». Celle-ci n'hésite pas à affirmer : *« Le travail se déterritorialise, le temps de travail se décloisonne. Avec l'immersion permanente que cela implique, c'est la notion de sphère privée qui devient problématique »*. [118] En outre, selon une partie de la doctrine, la vie d'une personne « *ne peut faire l'objet d'un morcellement et force est de constater qu'à l'occasion de l'exécution de la prestation de travail, l'individu ne peut faire abstraction de sa personnalité et de certains attributs de sa vie privée* ».[119]

Il est très fréquent que la vie privée des salariés se retrouve au cœur d'affaires juridiques. Ainsi, la Haute-juridiction depuis un fameux arrêt du 16 décembre 1997[120] réaffirme fréquemment la nécessité de protéger la vie privée du salarié. Il est important de rappeler que la finalité du droit du travail est orientée vers la protection des salariés. [121] Que doit-entendre par respect de la vie privée du salarié et comment en assurer l'effectivité ? Il convient de rappeler que le salarié a droit au respect de l'intimité de sa vie privée, sur son lieu et son temps de travail[122]. Selon la jurisprudence qui a posé ce principe : *« l'employeur ne peut (…) prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un*

[118] Rapport de la CNIL, Vie privée à l'horizon 2020, Cahier IP n°1, www.cnil.fr, p.44
[119] ARNAUD Stéphanie, « Analyse économique du droit au respect de la vie personnelle : application à la relation de travail en France ? », *Revue internationale de droit économique*, avril 2007, n°2, p.129-156
[120] Cass. 16 décembre 1997, n°95-41.326, Delamaere c/ Office notarial Ryssen et Blondel
[121] DUQUESNE (F.), *Droit du travail*, 2014, Lextenso Editions, 4 editions, Gualino, p.22
[122] Cass.soc. 2 octobre 2001

outil informatique mis à sa disposition pour son travail ». Cette formulation sous-entend entre autre par exemple, le respect du secret des correspondances[123].

Néanmoins, le droit à la vie « personnelle » ne peut se limiter simplement au respect de l'intimité de la vie privée. Ainsi, progressivement le droit à la vie privée s'est étendu à de nombreux autres aspects de la vie sociale, notamment sous l'impulsion de la jurisprudence de la Cour Européenne des droits de l'Homme. Le respect par l'employeur de la vie personnelle du salarié inclut dorénavant des aspects de la vie professionnelle du salarié, ce qui semble logique. C'est pourquoi, le respect du droit à une vie personnelle est maintenant très large. Par conséquent, le respect de la vie privée ou « personnelle » » du salarié s'impose à l'employeur. A cet égard, certains auteurs de doctrine rappellent toutefois les limites du pouvoir de l'employeur en expliquant que « *Le pouvoir patronal n'est pas un pouvoir total, ni totalitaire, une part de l'individu salarié lui échappe* ».[124] La notion de « vie privée » ou « personnelle » a largement été appréhendée et précisée par la jurisprudence en France ainsi qu'au niveau de l'Union européenne.

Ainsi, dans un arrêt Niemetz c/ Allemagne du 16 décembre 1992, la CEDH a affirmé qu'il serait « trop restrictif de limiter la vie privée à un cercle intime où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle et qu'il n'y a aucune raison de principe d'en exclure les activités professionnelles ou commerciale ». Ainsi, la Cour « ne juge ni possible ni nécessaire de chercher à définir de manière exhaustive la notion de vie privée ».

Par la suite, dans un arrêt Schuth contre Allemagne[125], elle a adopté une conception très large de la notion de vie privée, en affirmant que celle-ci recouvre « *l'intégrité physique et morale de la personne et englobe parfois des aspects de l'identité physique et sociale d'un individu* ». Ainsi, il semble opportun de souligner qu'il apparaît qu'il n'existe pas une seule et unique définition de la vie privée, mais que cette notion revêt plusieurs acceptions qui peuvent être très différentes.

A cet égard, nombreux sont les auteurs de doctrine qui se sont interrogés sur la pertinence de la définition de la notion de vie privée. Ainsi, François Rigaux a mis en exergue les difficultés à définir cette expression. Pour ce dernier, « réduire la définition à l'opposition entre public et privé exclut tout questionnement relatif à la vie privée au sein de l'entreprise, elle-même

[123] CHENEDE (O.) et JOURDAN (D.), *Contrat de travail du recrutement à la rupture*, 6e édition, 2005, p.173
[124] AUZERO (G.) et DOCKES (E.), *Droit du travail*, Dalloz, Précis, 2014, 28 édition, p.689
[125] CEDH, 23 septembre 2010

espace de pouvoir privé ». C'est pourquoi, certains font le choix d'évoquer plutôt le concept de « vie personnelle » qui me semble également plus adapté. Elaborée au cours des années 1990, cette notion permet de désigner tout ce qui, chez la personne du salarié, relève de la protection de ses libertés et droits fondamentaux. Cette notion comprend donc la vie privée, mais également l'ensemble des libertés et droits individuels et collectifs jugés inaliénables, y compris au sein de l'entreprise lorsqu'un lien de subordination s'exerce[126].

La protection de la vie privée des salariés semble ainsi véritablement apparaître au cœur du droit du travail. Toutefois, si le droit assure cette protection, on peut s'interroger : celle-ci n'est-elle pas remise en cause progressivement par le comportement même et les agissements de certains salariés aujourd'hui ? En effet, au cours de mes recherches dans le cadre de ce mémoire sur la notion de vie privée et personnelle au travail, la problématique du « *privacy paradox* » était très souvent évoquée. Ce « *privacy paradox* » a semble-t-il marqué le 21e siècle[127]. Il devrait selon moi, marquer également les années à venir, dès lors que les individus sont de plus en plus connectés. Que doit-on entendre par cette notion ?

Bien que les individus semblent de plus en plus inquiets à l'égard des informations qui peuvent être récupérées par l'entreprise en lien avec leur vie privée, il est possible de constater qu'en réalité dans la pratique, ces derniers n'hésitent pas à s'exposer sur Internet toujours plus et à mettre ainsi à disposition leurs nombreuses données, malgré les conseils de la CNIL. Cette notion témoigne donc d'une véritable contradiction apparente. Le « *privacy paradox* » est très important en matière d'usage du smartphone. En effet, le fait que le smartphone accompagne le salarié quasiment en permanence dans ses déplacements pose problème, car celui-ci permet de « surveiller » presque en continu le salarié, d'autant plus que selon une étude Net-Iris en 2011, 7 personnes sur 10 n'éteignaient jamais leur smartphone[128]. Le privacy paradox inquiète aujourd'hui. La CNIL s'est également interrogée sur cette notion dans son rapport consacré aux données personnelles et plus globalement à la vie privée. Ainsi, au sein d'un rapport qu'elle a rendu, elle affirme que le « Privacy paradox » est devenu un « passage obligé dans toute réflexion sur les questions relatives à la vie privée ». Selon l'autorité garante de la protection des données en France, « *il y aurait une incohérence*

[126] ARNAUD Stéphanie, « Analyse économique du droit au respect de la vie personnelle : application à la relation de travail en France ? », Revue internationale de droit économique, avril 2007, n°2, p.129-156
[127] PRAS (B.), « Entreprise et vie privée », *Revue française de gestion* 5/2012 (N° 224) , p. 87
[128] PRAS (B.), « Entreprise et vie privée », *Revue française de gestion* 5/2012 (N° 224), *op.cit.*, p. 87

apparente des personnes qui se dévoilent malgré la crainte qu'elles exprimeraient fréquemment d'une perte de contrôle de la gestion de leur vie privée ». [129]

La protection du droit à la vie privée, dont certains tel Jean-Emmanuel Ray s'interroge sur le fait de savoir s'il ne s'agirait plutôt dorénavant d'une liberté est toujours au cœur de l'actualité. A titre d'illustration, une recommandation a été adoptée sur le droit au respect de la vie privée des salariés sur leur lieu de travail par le Conseil des ministres du Conseil de l'Europe très récemment en avril 2015. La France n'est toutefois pas le seul pays qui se préoccupe de la protection de la vie privée ou vie personnelle des salariés. Ainsi, c'est aussi le cas en Italie.

2) En Italie

L'Italie est l'un des pays qui semble aujourd'hui avoir une vision très protectrice de la notion de vie privée. Toutefois, il est intéressant de souligner que ce pays ne s'est doté d'une loi que très tardivement par rapport aux autres pays. Par ailleurs, les textes n'évoquent pas cette notion, mais plutôt celle de « droit à l'image » toutefois elle a été énoncée par la jurisprudence. Ainsi, l'Italie a été l'avant dernier pays au sein de l'Europe à se doter d'une loi sur la protection « des données personnelles de la vie privée ». Par ailleurs, au cours de mon expérience professionnelle en Italie, j'ai très rapidement pris conscience que les entreprises sont très vigilantes et veillent à assurer toujours l'effectivité des principes relatifs à la protection de la vie privée.

Dans un premier temps, la loi n°675 du 31 décembre 1996 a été très importante pour les italiens. Selon cette loi, aucune autorisation n'est requise pour le traitement de données n'ayant qu'un but exclusivement personnel, ainsi que pour les données dites anonymes à condition toutefois qu'elles ne permettent pas de révéler l'identité du sujet concerné[130]. Cette loi a aussi mis en place d'un double-système d'autorisation pour le traitement licite des informations. Ainsi, le consentement de l'intéressé est requis pour les données personnelles. Néanmoins, pour les données dites sensibles, l'autorisation du « garant » est nécessaire en plus de l'exigence du consentement de l'intéressé pour les données personnelles.

En outre, il est intéressant de souligner que le développement de l'institution garante en matière de protection notamment des données personnelles s'est véritablement inspiré de modèles étrangers. Enfin, depuis juin 2003, le Code pour la protection des données

[129] Rapport de la CNIL, Vie privée à l'horizon 2020, Cahier IP n°1, www.cnil.fr, p.36
[130] RICCIO (G-M), « La protection de la vie privée : brève analyse de la situation italienne », Lex eletronica, vol. 6, n°2, 2001

personnelles réunit l'ensemble des lois relatives à la notion de vie privée et de données personnelles. Avec la rédaction de ce code, approuvé par le « décret-loi » n°196 du 30 juin 2003, la loi n°675 a été abrogée.

Il me semble opportun d'évoquer quelques décisions jurisprudentielles afin d'illustrer comment la notion de vie privée est appréhendée par le droit italien.

En effet, la problématique du droit à la vie privée s'est posée en Italie dans les années 1950. La jurisprudence Caruso du 22 décembre 1956 doit à cet égard être citée. Il s'agit de l'une des premières décisions rendues en matière de droit à la vie privée en Italie. Ainsi, c'est une décision qui est très importante. Au sein de cette décision, la Cour de cassation italienne a rejeté l'existence d'un droit à la vie privée. Les faits étaient les suivants : le fils et les petits-enfants du ténor italien Caruso avaient intenté une action contre la maison de production du film « *Légende d'une voix* », qui racontait sous forme de fiction, des épisodes et des évènements liés à l'enfance, à la jeunesse de la carrière d'Enrico Caruso. Cette affaire soulevait la question de savoir si le droit à la vie privée « *diritto alla riservatezza* » o « *privatezza* » qualifié en anglais de « *right of privacy* » devait faire l'objet d'une protection.

Le principe qui a été posé par cette décision est le suivant : « dans l'ordre juridique italien, il n'existe pas de droit à la vie privée. Pour autant, sont reconnus et protégés les droits de la personnalité ». Par conséquent, « il n'est pas interdit de communiquer que ce soit de manière privée ou publique, des informations mêmes imaginaires, quand l'information n'a pas été obtenue par des moyens illicites ou qui imposaient le secret ». Au sein de cette décision, les juges ont en effet jugé que *« nell'ordinamento giuridico italiano non esiste un diritto alla riservatezza, ma soltanto sono riconosciuti e tutelati, in modi diversi, singoli diritti soggttivi della persona, pertanto non è vietato comunicare, sia privatamente sia pubblicamente, vicende, tanto più se immaginarie, della vita altrui, quando la conoscenza non ne sia stata ottenuta con mezzi di per sé illeciti i che impogono l'obbligo del segreto* [131] ».

Une autre jurisprudence permet d'illustrer la consécration progressive du droit à la vie privée en Italie. Il s'agit de la jurisprudence Petacci/Palazzi et Tafarell[132]. Dans cette décision, les juges considèrent que les « questions afférentes à la vie privée doivent demeurer protéger de

[131] Cassazione civile – 22 dicembre 1956 n.4487 ; Soc.produzione associata Tirrena Asso Film c.Caruso
[132] Cassazione civile- 20 aprile 1963 n.990

toute atteinte lorsque l'intéressé n'a pas donné son consentement préalable à la diffusion de ces dernières ou qu'il n'existe pas d'intérêt général à leur révélation ». La Cour trouve le fondement du droit à la vie privée dans l'article 2 de la Constitution italienne. « Sebbene non sia ammissibile il diritto tipico alla riservatezza. viola il diritto assoluto di personalità, inteso quale diritto erga omnes alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito, ed ove non sussista, per la natura dell'attività svolta dalla persona e del fatto divulgato, un preminente interesse pubblico di conoscenza. ». Ce principe posé peut être traduit de la façon suivante : « Bien qu'un droit à la vie privée ne soit pas admissible, viole le droit absolu de la personnalité, entendu comme un droit opposable erga omnes sur la liberté de l'auto-détermination dans l'accomplissement de la personnalité de l' homme en tant qu'individu , la divulgation d'informations relatives à la vie privée , en l'absence d'un consentement , au moins implicite, ou s'il n'y a pas d'intérêt général à leur révélation. »

Finalement c'est en 1975 que la Cour de cassation italienne a proclamé expressément l'existence d'un droit à la protection de la vie privée. Au sein de cette décision, les juges se prononcent et affirment que « le droit à la vie privée est reconnu dans notre ordre juridique[133] ».

B) La mobilité, facteur potentiel de risque pour l'effectivité des libertés du salarié

Le BYOD et les outils liés à a mobilité sont fréquemment associés à la notion de liberté, « liberté d'apporter son propre matériel et ses propres outils mobiles et connectés ». Toutefois, pour certains auteurs de doctrine, il est possible de s'interroger sur l'effectivité de cette liberté et sur l'existence même de « liberté ». Dès lors le salarié connecté aujourd'hui apporte avec lui et utilise son terminal personnel quotidiennement et à tout moment, il est peu probable qu'un salarié n'utilise pas ou peu son terminal au travail. Néanmoins, l'effectivité de la liberté interroge la doctrine, certains auteurs s'interrogent alors : le salarié est-il véritablement libre d'utiliser son terminal mobile et connecté comme il le désire dès lors que

[133] Cass.27 maggio 1975 n.2129

l'objet privé devient un instrument au service de l'employeur et de l'entreprise? [134] Le salarié est-il libre d'utiliser et d'éteindre l'outil mobile et connecté quand il le souhaite ? En effet, la pratique du BYOD est une pratique que l'employeur est libre d'interdire. Il pourrait donc par conséquent exister un risque pour le salarié d'atteinte à ses libertés. La question qui se pose n'est pas nouvelle. Elle renvoie au contrôle et à la surveillance des outils numériques des salariés. Contrairement à la clé USB connectée à un équipement professionnel, la tablette ou le smartphone parfois ne sont pas la propriété de l'entreprise.

A priori, le contrôle par l'employeur des outils personnels du salarié peut apparaître compromis dès lors que ces outils sont en mesure d'héberger des données relevant de la vie privée dont la protection est très importante comme nous l'avons vu dans le cadre de la première partie de ce mémoire. Nous verrons que ce contrôle pourrait à l'avenir devenir effectif eu égard aux jurisprudences qui ont fait l'objet de l'actualité récemment.

§2- Le droit à la vie privé du salarié limité par le pouvoir de contrôle de l'employeur

Le pouvoir de l'employeur consacré par des textes et précisé par la jurisprudence tant en droit français qu'en droit italien (A) a été au cœur de jurisprudences récentes en France (B).

A) Le pouvoir de contrôle de l'employeur

L'employeur dispose d'un pouvoir de contrôle en droit français (1), qui existe également en droit italien (2). Dans le cadre de cette sous-partie, je souhaiterai mettre en évidence les points communs entre ces deux droits.

1) Le pouvoir de contrôle de l'employeur en droit français à travers les textes

Les nouvelles technologies de l'information et de la communication ont connu un fort développement ces dernières années dans le milieu professionnel. Le lien de subordination est omniprésent dans l'entreprise. Ainsi, certains n'hésitent pas à qualifier de *« laisse électronique »* les outils mobiles mis à la disposition des salariés pour assurer leur « suivi » en

[134] FUNKE (J-F.), « La pratique du BYOD (Bring your own device) », *JCP S* (édition sociale), n°4, janvier 2015, p.3

dehors de leur lieu de travail[135]. Aujourd'hui cette mise à disposition d'outils de travail pour le salarié est effective avec le développement du CYOD, dans lequel l'entreprise propose un smartphone ou une tablette au salarié. Il est important de rappeler que les droits du salarié ne sont pas un obstacle à l'exercice des pouvoirs de l'employeur. Aujourd'hui, le pouvoir de contrôle de l'employeur dans le cadre des solutions de mobilité interroge à deux égards : d'une part, s'agissant du contrôle « physique des individus » à travers la cybersurveillance, entre autres par la géolocalisation, et d'autre part, le contrôle des outils mobiles et connectés parfois apportés dans l'entreprise par le salarié ou mis à sa disposition. Ainsi, dans le cadre de son pouvoir de direction et disciplinaire, l'employeur a la possibilité de mettre en place des procédés de surveillance et de se livrer à des contrôles. Ce contrôle par l'employeur reste toutefois très encadré en droit français.

S'agissant du contrôle « physique ou par la géolocalisation », nous verrons dans le cadre de ce chapitre que l'article L432-2-1 du Code du travail évoque la possibilité pour un employeur de mettre en place des moyens ou des techniques permettant un contrôle de l'activité des salariés. Toutefois, ce contrôle ne peut concerner la vie personnelle du salarié et ne peut être que loyal, c'est-à-dire que le salarié doit nécessairement être préalablement informé de ce contrôle si ce contrôle a pour but sa surveillance.» Aujourd'hui, avec le développement des outils liés à la mobilité, la problématique du droit d'accès de l'employeur sur des équipements se pose de nouveau[136]. Il s'agit ici d'une des problématiques les plus importantes. A cet égard, la CNIL notamment s'interroge sur ce contrôle[137].

S'agissant des écoutes téléphoniques, la jurisprudence a également précisé les contours de ce contrôle. Ainsi la Cour de cassation n'hésite pas à rappeler le principe suivant : « *L'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, seul l'emploi de procédés clandestins de surveillance est illicite* ».[138]

En outre, s'agissant du contrôle des outils mis à la disposition des salariés précédemment évoqué, la jurisprudence a posé le principe suivant dans un arrêt Nikon relatif à la consultation du courrier électronique : l'employeur ne peut sans violation de la liberté fondamentale du droit à la vie privée « prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail ».

[135] BELIER (G), *13 paradoxes en droit du travail*, Lamy Axe Droit, p.236
[136] CONTAMINE (A), « La surveillance du salarié », *Lamy droit de la concurrence*, 2013, n°3
[137] MEURIS (F), « Le salarié connecté », *CCE*, 1er octobre 2014
[138] Cass. 14 mars 2000, 98-42.090

2) Le pouvoir de contrôle de l'employeur en droit italien

Il me paraît opportun et pertinent dans le cadre de cette sous-partie de comparer d'une part le pouvoir de l'employeur français, et d'autre part italien, afin de mettre en exergue les ressemblances et les différences pouvant exister entre les deux droits. Ainsi, il est important de rappeler que l'employeur italien dispose également d'un pouvoir de contrôle sur ses salariés s'agissant de l'exécution de leur prestation de travail. En effet, le rapport professionnel qui le lie au salarié lui permet d'exercer un certain nombre de pouvoirs en vue de gérer l'organisation de son entreprise, l'exercice de ses droits et l'accomplissement des obligations des salariés. Avec le développement des nouvelles technologies, les dispositifs mobiles et connectés sont parfois devenus des outils véritablement nécessaires à l'exécution de la prestation de travail. Toutefois, ces mêmes technologies permettent à l'employeur d'effectuer des contrôles pouvant se révéler parfois invasifs et portant atteinte à la vie privée des travailleurs[139]. Dans le cadre son pouvoir de sanction disciplinaire en lien avec le contrôle du salarié, l'employeur doit tout toutefois respecter certains principes entre autres énoncés au sein du « *statuto dei lavoratori* ». Néanmoins, il me semble important de souligner, que le pouvoir de l'employeur n'est pas absolu. En effet, certaines limites viennent encadrer ce pouvoir et l'employeur doit prendre en compte les droits du salarié[140].

Deux théories en matière de justification du pouvoir disciplinaire ont été développées. Ainsi, selon une partie de la doctrine, le pouvoir disciplinaire a pour objectif de « *garantir l'ordre interne du groupe social* », tandis que pour l'autre partie de la doctrine, le pouvoir disciplinaire serait fondé sur un rapport de hiérarchie[141] . Au sein de l'article 7 du « *statuto dei lavoratori* », les conditions dans lesquelles le pouvoir disciplinaire s'exerce sont énoncées. Ainsi, il est prévu que le pouvoir de l'employeur ne peut porter atteinte aux droits fondamentaux du salarié. Entre autres, il ne peut porter atteinte au droit à la dignité et à la vie privée

Les limites qui existent dans le cadre du pouvoir de contrôle de l'employeur sont aussi énoncées dans le « statut des travailleurs », définit par la loi n°300 de 1970 à l'article 4. Le « statut des travailleurs » prévoit notamment les « limites subjectives et objectives » pour que

[139] LAURI (M.), I limiti del potere di controllo del datore di lavoro, Tesi di Laurea, p.8
[140] INDICTALIA, LAVORO, Guide e Soluzion, Ipsoa, 2014, p.699
[141] BOUCHE (S.), *Droits et libertés du salarié comme limites au pouvoir disciplinaire de l'employeur en droit français et en droit italie*n, op.*cit*, disponible en ligne sur le site www.juripole.com

l'employeur puisse exercer son contrôle. Ce statut détermine notamment qui est « le sujet » qui peut faire l'objet du contrôle et aussi les deux formes de contrôle pouvant exister : le contrôle à distance et le contrôle direct.

En résumé, le pouvoir de contrôle de l'employeur constitue l'un des pouvoirs attribués à l'employeur, grâce auxquels celui-ci a la possibilité de vérifier que les salariés accomplissent leur prestation de travail. Avec le développement des TIC sur le lieu de travail, et l'utilisation des mails et d'internet, la forme de contrôle de la part de l'employeur sur les modalités d'utilisation de ces outils doit nécessairement être conciliée avec le droit à la « privacy » des salariés, protégé par le « Decreto legislativo » D.lgs, 2003, n°196[142].

B) Le pouvoir de contrôle de l'employeur au cœur de jurisprudences récentes en France

Un cadre juridique semble progressivement se définir pour les solutions liées à la mobilité professionnelle. En effet, la jurisprudence française s'est prononcée très récemment sur le contrôle de deux types d'outils qui sont utilisés dans le cadre de la mobilité, d'une part : la clé USB (1), et d'autre part, les SMS professionnels (2).

1) Les prémisses d'un pouvoir de contrôle sur les terminaux connectés personnels à travers le contrôle de la clé USB

Selon certains sondages, les salariés consacrent plus de 2 heures par jour à des tâches personnelles sur le lieu de travail. La clé USB, outil de la mobilité par excellence, est parfois perçue comme un outil favorisant ces activités personnelles exercées sur le lieu de travail.[143] Ainsi, la problématique du contrôle des outils personnels du salarié se pose de plus en plus régulièrement.[144]

Un précédent au contrôle de la clé USB s'était déjà posé s'agissant d'un dictaphone personnel, au cœur d'une jurisprudence[145] en date du 23 mai 2012[146]. Le principe qui a été

[142] LUCANTONI (S.), « Controllo sul lavoratre e sulla sua attività » <www.treccani.it>, 2014
[143] PANSIER (F-J.), « La clé USB est présumée contenir des fichiers professionnels », *Cahiers sociaux du Barreau de Paris*, mars 2013, n°250, p.78
[144] CAPRIOLI (E.), « Caractère professionnel d'une clé USB privée connectée à l'ordinateur professionnel », *CCE*, n°5 , mai 2013, comm. 62, p.50
[145] Cass. soc.23 mai 2012,n°10-23.521
[146] CAPRIOLI (E.), Contrôle de l'employeur des données se trouvant sur l'outil personnel d'un salarié, *CCE*, n°9, septembre 2012, comm.104, pp.43-45

posé au sein de cet arrêt est le suivant : un employeur ne peut pas procéder à l'écoute des enregistrements réalisés par une salariée sur son dictaphone personnel en son absence ou sans qu'elle ait été dûment appelée. La preuve apportée par un tel contrôle est déloyale. Cet arrêt apporte une pierre essentielle à l'encadrement du contrôle des outils privés du salarié. Il est toutefois possible de citer ici également un autre précédent relatif au contrôle d'un message laissé par un salarié sur le téléphone portable professionnel d'un autre salarié. La jurisprudence a considéré que « *le message envoyé par le salarié aux temps et lieu de travail, qui était en rapport avec son activité professionnelle ne revêtait pas un caractère privé et pouvait être retenu au soutien d'une procédure disciplinaire à son encontre* ».[147]

La jurisprudence française s'est donc prononcée très récemment sur l'un des outils les plus utilisés dans le cadre de la mobilité : la clé USB. Ainsi, au sein d'un arrêt rendu le 12 février 2013, la Cour de cassation a précisé les conditions du contrôle pouvant être exercé par l'employeur sur cet outil[148]. La chambre sociale a dans le cadre de cette affaire validé ce type contrôle. Cette solution a pu apparaître surprenante. Les faits étaient les suivants : une salariée avait fait l'objet d'un licenciement en raison du fait qu'elle avait enregistré des informations confidentielles concernant l'entreprise sur sa clé USB personnelle. La salariée alléguait que son licenciement n'était pas fondé dès lors que selon celle-ci, le mode de preuve utilisé était illicite. La salarié soutenait qu'en son absence, et sans l'avoir dûment informé de son droit de refuser ce contrôle ou d'exiger la présence d'un témoin, son employeur ne pouvait pas consulter le contenu de sa clé USB[149] en application des jurisprudences antérieures. En effet, la Haute-juridiction dans un arrêt rendu le 17 mai 2005 avait précisé que : « Dès lors que le salarié a identifié comme personnels des fichiers de son disque dur, l'employeur ne peut procéder à leur ouverture que s'il respecte deux conditions : la présence du salarié ou du moins son information ou bien à défaut, l'existence d'un risque ou d'un événement particulier pour l'entreprise ».

Dans un premier temps, les juges de la cour d'appel ont fait droit à sa demande. Selon ces derniers, la salarié était absente quand sa clé USB personnelle a été consultée par son employeur car elle n'a pas été informée de son droit d'en refuser le contrôle ou d'exiger la présence d'un témoin. La décision est toutefois censurée par la Cour de cassation. En effet, selon les juges de la Haute-juridiction « *l'employeur peut, en dehors de la présence du*

[147] Cass. 28 septembre 2011, n°10-16.995
[148] Cass.soc. 12 février 2013, n°11-28.649
[149] FROUIN (C.), « L'employeur peut ouvrir la clé USB du salarié connectée à l'ordinateur professionnel », *La gazette du Palais*, mars 2013, n°81-82, p.29

salarié, avoir accès aux fichiers non identifiés comme personnels que la clé USB contient, dès lors que celle-ci était connectée à un outil informatique mis à la disposition du salarié par l'employeur pour l'exécution de son contrat de travail ».

Comme certains auteurs de doctrine l'ont souligné, il est important de rappeler que le droit d'accès de l'employeur à la clé USB du salarié n'est pas absolu puisqu'il est subordonné au fait que ladite clé puisse être présumée utilisée à des fins professionnelles, ce qui était le cas en l'espèce, dès lors qu'elle était connectée à l'outil informatique mis à la disposition du salarié par l'employeur. En l'espèce, il s'agissait de la première fois que la Cour de cassation se prononçait sur le contrôle par l'employeur de cet outil.

Cet arrêt a donc permis à la jurisprudence de préciser les conditions dans lesquelles le contenu d'une clé USB peut faire l'objet d'un contrôle par l'employeur. La particularité des faits en l'espèce était que la clé USB appartenait au salarié et non à l'employeur. Par conséquent, il ne s'agissait pas ici d'un dispositif mis à la disposition du salarié par l'employeur mais qui était connecté à un outil qui l'était. En résume, si la clé USB est connectée à « un outil informatique mis à la disposition du salarié par l'employeur pour l'exécution du contrat de travail, dans cette hypothèse, le principe qui s'applique est le suivant : l'employeur peut consulter le contenu, hors la présence du salarié, sauf ceux identifiés comme personnels[150]. Enfin, dans l'hypothèse où la clé USB n'est pas connectée à un outil informatique, la clé USB est présumée professionnelle et l'employeur ne pourra l'ouvrir qu'en présence du salarié ou celui-ci dûment appelé. La doctrine a souligné que la « connexion à un système d'information de l'entreprise opère un changement de qualification ».[151] Ainsi, la clé USB objet personnel devient professionnelle du fait de sa connexion.

Pour certains, cet arrêt qui a été très commenté, parfois vivement critiqué et qui se prononce sur le caractère professionnel ou personnel d'une clé USB[152], apporte une nouvelle limite au respect de la vie privée dans l'entreprise, et cette solution serait plutôt en faveur des intérêts de l'entreprise. Par conséquent, cet arrêt s'inscrirait dans la continuité d'un mouvement jurisprudentiel qui tend à étendre la présomption de caractère professionnel des documents ou

[150] LHERNOULD (J-P), « NTIC- les secrets de la clé USB personnelle du salarié accessibles à l'employeur », Jurisprudence sociale Lamy, mars 2013, n°340, p.13
[151] CAPRIOLI (E.), Caractère professionnel d'une clé USB privée connectée à l'ordinateur professionnel, *CCE*, n°5 , mai 2013, comm. 62, pp.50
[152] LALOT (L.), « Une clé usb connectée à l'ordinateur est présumée utilisée à des fins professionnelles », *Lamy droit de l'immatériel*, mars 2013, n°91, p.46

des outils sur le lieu de travail[153]. Personnellement, la solution qui a été donnée par les juges à ce litige par la Cour de cassation me paraît justifiée du point de vue de l'employeur dès lors que la clé USB était connectée à l'outil professionnel. Cet arrêt incite donc les salariés à plus de prudence et les invite également à s'informer davantage.

Il est ici intéressant de souligner qu'en dehors de la problématique du contrôle de la clé USB par l'employeur, l'utilisation de cet outil a fait l'objet d'une jurisprudence importante, comme nous l'avons vu précédemment dans le cadre du début de la première partie de ce mémoire, s'agissant de vols d'informations par exemple stockées sur ce type de support. Par conséquent, les outils mobiles et connectés peuvent se révéler à l'origine de problématiques très diverses.

2) L'affirmation du pouvoir de contrôle de l'employeur sur les SMS professionnels

Une autre problématique pouvant être également rattachée au BYOD s'est posée récemment relative au contrôle d'un autre outil lié à la mobilité : le portable professionnel. Les SMS envoyés ou reçus par cet appareil sont présumés avoir un caractère professionnel, d'après un arrêt rendu très récemment le 10 février 2015. En l'espèce, pour la Haute-juridiction, le portable « mis à disposition par l'employeur » est un outil de travail. Cet arrêt met en évidence les difficultés liées à l'usage « mixte » du smartphone aujourd'hui alors que les entreprises sont de plus en plus nombreuses à mettre à disposition de leurs salariés ce type de téléphones. La Haute-juridiction s'était déjà prononcée en ce sens à propos de courriers privés envoyés à partir de la messagerie professionnelle[154]. Cet arrêt n'a toutefois pas été exempt de critiques. Certains auteurs ont dénoncé ici que cet arrêt était en trop faveur des employeurs, et qu'il semblait exister un risque de rupture de l'équilibre devant être recherché entre les intérêts du salarié et ceux de l'employeur. Le but de la présomption développée par la jurisprudence, de nouveau « étendue » par le présent arrêt était d'établir une règle pratique permettant de résoudre le conflit pouvant exister d'une entre le besoin parfois légitime de l'employeur d'accéder à des contenus sur l'outil professionnel du salarié et d'autre part le

[153] NORD-WAGNER (M.), « Présomption d'utilisation à des fins professionnelles d'une clé USB connectée à l'outil informatique mis à disposition du salarié par son employeur » , *revue droit du travail Dalloz,* mai 2013, n°5, p.339-340

[154] COSTES (L.), « Possibilité pour l'employeur de consulter les SMS du mobile de ses salariés », revue *Lamy Droit de l'immatériel,* mars 2015, n°113, p.34

droit au respect de la vie privée et au secret des correspondances du salarié sur son lieu de travail et donc sur ses terminaux[155].

Désormais, eu égard au renforcement de cette « présomption à caractère professionnelle », il appartient donc au salarié d'être prudent et d'indiquer le caractère personnel pour les soustraire à un potentiel contrôle. Cette solution a été toutefois très critiquée dès lors les SMS ne comportent pas de champ « objet », permettant d'indiquer leur caractère personnel. Ainsi, certains ont pu dénoncer le caractère inadapté de cette présomption.

Par ailleurs, la doctrine a toutefois souligné que cette présomption bien que juste à l'égard des intérêts de l'employeur, n'est plus adaptée aux nouvelles formes d'organisation du travail. Ainsi, de nouveau cela permet d'illustrer le fait que les juristes sont fréquemment dépassés par l'avancée des nouvelles technologies. Certains auteurs de doctrine préconisent d'inclure ces nouvelles formes d'organisation professionnelles dans le champ d'application de la présomption, ainsi, la notion « d'outils mis la disposition du salarié par l'employeur » pourrait être remplacée par une notion un peu plus large permettant d'inclure les nouvelles formes d'organisation de la mobilité nobsostant le critère de la personne qui fournit le matériel. En vue de préserver l'équilibre compromis, il pourrait être nécessaire d'introduire dans l'hypothèse du BYOD, une présomption inverse à celle dégagée par l'arrêt NIKON[156].

Par ailleurs, il est opportun de rappeler que la jurisprudence a précisé que : « si les messages présumés à caractère professionnel peuvent être consultés par l'employeur en dehors de la présence du salarié, le règlement intérieur peut toutefois contenir des dispositions restreignant le pouvoir de consultation de l'employeur, en le soumettant à d'autres conditions ».

L'arrêt rendu par la Cour de cassation le 10 février 2015 s'inscrit dans une tendance à la « responsabilisation » des salariés, comme celle relative au contrôle de la clé USB que nous avons cité précédemment, qui sont à travers cette solution, invités à réserver l'utilisation du smartphone mis à leur disposition à un usage strictement professionnel et non plus mixte. Cette jurisprudence les invite à faire preuve de plus de vigilance[157]. Toutefois, il est important de souligner que le fait d'appliquer la même solution aux courriels et SMS a pu être très

[155] CASANOVA (A.), « Consultation des courriers électroniques et des SMS du salarié : même cause, même combat, même principe aux yeux de la Cour de cassation », *Lamy Droit de l'immatériel*, mai 2015, n°115, p.14
[156] CASANOVA (A.), « Consultation des courriers électroniques et des SMS du salarié : même cause, même combat, même principe aux yeux de la Cour de cassation », *ibid.*, p.15
[157] BARRIERE (F.), « SMS, téléphone professionnel et vie privée du salarié », *La Semaine Juridique Entreprise et Affaires* n°14, 2 avril 2015, p.60

critiqué.[158] Enfin, pour une partie de la doctrine, il est légitime que si les SMS sont émis d'un téléphone professionnel, ils soient présumés ne pas être en rapport à la vie privée du salarié.

Personnellement, cette position du point de vue de l'employeur me parait théoriquement légitime et compréhensible. Toutefois, l'usage mixte de cet outil mis à la disposition des salariés est en pratique une réalité qui n'est pas ignorée par les employeurs et bien souvent qui n'est pas prohibée. A cet égard, il apparait donc qu'il s'agit d'une jurisprudence qui divise non seulement la doctrine juridique mais également les individus.

Section 2. Le risque d'atteintes à la vie privée renforcée par la cybersurveillance et la géolocalisation intensive

Il existe aujourd'hui en France, un certain nombre de principes applicables à la géolocalisation du salarié en droit français. Toutefois, un renforcement des règles semble nécessaire pour faire face au développement des outils mobiles et connectés (**paragraphe 1**). La géolocalisation des salariés est également une problématique d'actualité en droit italien et soulève aussi de nombreuses questions juridiques à résoudre (**paragraphe 2**).

§1 - Les principes généraux relatifs à l'utilisation des nouvelles technologies par l'employeur à des fins de surveillance dans l'intérêt de la protection du salarié en droit français

La géolocalisation en droit français est encadrée par des textes (**A**). La CNIL veille à l'effectivité de l'application des principes (**B**).

A) L'encadrement de la géolocalisation par les textes en droit français

Par définition, la géolocalisation est une « technologie relevant de la catégorie des communications électroniques, à finalités multiples mais qui a pour objet principal de déterminer la localisation plus ou moins précise d'un objet ou d'une personne par le biais d'un terminal. » [159] Le recours à la géolocalisation par l'employeur oblige ce dernier à informer au

[158] BARRIERE (C.), « Les SMS envoyés ou reçus par le salarié sur son téléphone professionnel sont présumés professionnels », *La Semaine Juridique Edition générale*, février 2015, n°8, p.373

[159] BARBIER (H.), *Les enjeux de l'encadrement juridique de la géolocalisation,* Aix-Marseille, année 2013-2014, p.1

préalable les représentants du personnel. En vertu de son pouvoir de contrôle, l'employeur français peut vérifier que le salarié exécute sa prestation de travail dans les conditions qui ont été préalablement délimitées. Par le biais du développement des nouvelles technologies, l'employeur a dorénavant de nombreux dispositifs qui lui permettent de s'assurer entre autres de l'utilisation du smartphone par exemple, par ses salariés. La surveillance du salarié par l'employeur est toutefois strictement encadrée par les textes. Dans un premier temps, le principe de loyauté s'impose, c'est-à-dire que l'employeur doit nécessairement informer ses salariés des moyens de surveillance utilisés. Par ailleurs, le principe de proportionnalité s'impose également, ce qui signifie que l'employeur ne peut faire l'objet d'une surveillance permanente[160]. Ainsi le dispositif de surveillance utilisé doit être conforme à l'article L1121-1 du code du travail qui dispose *« nul ne peut apporter aux droits des personnes et aux libertés individuelles ou collectives, des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché. »*

L'employeur français qui souhaite installer un dispositif de surveillance doit respecter un certain nombre de conditions. Ainsi, il doit informer et consulter le comité d'entreprise (article L2323-32 du code du travail). L'information individuelle est obligatoire quand le dispositif permet la surveillance, le contrôle et l'activité du salarié. Ainsi, l'article L1222-4 dispose *« aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté à sa connaissance »*. L'article L.4612-8 du code du travail prévoit que le CHSCT doit également être informé et consulté sur le recours à la géolocalisation. En outre, l'employeur doit également déclarer le dispositif auprès de la CNIL. En outre, au-delà de la géolocalisation, un exemple peut être cité s'agissant de la cybersurveillance de l'outil de travail: ainsi, dans un arrêt rendu le 9 juillet 2008, la Cour de cassation a précisé que «les consultations de sites Internet pendant le temps de travail et grâce à l'outil informatique mis à sa disposition par l'entreprise, sont présumées avoir un caractère professionnel de sorte que l'employeur peut les rechercher aux fins de les identifier même en dehors de la présence du salarié ».

La géolocalisation des salariés ainsi que la cybersurveillance de leurs activités font donc l'objet d'un encadrement strict.

B) La CNIL, autorité garante de l'application des principes

[160] Cours « Droit des TIC et droit du travail » de Madame Alexandra TOUBOUL, dispensé à l'Université d'Aix-Marseille, dans le cadre du M2 Droit des médias et des télécommunications

La CNIL, en tant qu'autorité administrative a un rôle central sur la problématique de la géolocalisation en entreprise. En effet, la CNIL informe, régule, protège et contrôle, afin de veiller à ce que l'informatique soit au service du citoyen et qu'il n'existe pas de risques d'atteintes entre autres aux droits de l'homme ou à la vie privée. La CNIL se montre particulièrement vigilante. Certains auteurs préconisent de se situer dans la « perspective de recommandations de la CNIL qui incite plutôt à un climat de loyauté et de confiance réciproque ».[161] Ainsi, il apparaît qu'au-delà de l'intervention de la CNIL, il est préférable que l'employeur et le salarié discutent ensemble de ces problématiques pour veiller à l'effectivité des principes qui régissent la géolocalisation.

Il est possible de s'interroger sur le fait de savoir si aujourd'hui la CNIL peut être à elle seule une autorité garante suffisante face au développement des TIC.

§2- Les principes généraux relatifs à la géolocalisation des salariés en droit italien

Un nouveau point commun peut être mis en évidence dans le cadre de ce mémoire, et de l'approche en droit comparé franco-italien que j'ai souhaité suivre dans le cadre de la rédaction de ce rapport. En effet, la « géolocalisation » en Italie, fait également l'objet d'un encadrement par des textes (A). En outre, il existe aussi une autorité garante qui veille à l'application effective des principes régissant la géolocalisation (B).

A) L'encadrement de la « géolocalisation » par les textes en Italie

Dans le cadre d'une approche en droit comparé : en droit italien, l'employeur privé ou public ne peut pas effectuer de traitement de données personnelles en utilisant des systèmes hardware et software qui lui permettent de contrôler à distance le salarié. Ce principe s'applique également dans le cadre de la vidéo surveillance et de la géolocalisation.[162] Ainsi,

[161] MAZEAUD (A.), Droit du travail, 9e édition, LGDJ, Lextenso, p.348

[162] Rapport Garante per la protezione dei dati personali , Privacy e lavoro, Le regole per il corretto trattamento dei dati personali dei lavoratori da parte di soggetti pubblici e privati, avril 2015 , p.10

ces instruments ne doivent pas être utilisés en vue de vérifier l'application des devoirs de diligence s'agissant du respect des horaires de travail ou de la correcte exécution de la prestation de travail. Néanmoins, il est également important de rappeler que l'installation de dispositifs qui permettent le contrôle à distance de l'activité est parfois autorisée pour satisfaire certaines exigences[163].

Par exemple, ce sera le cas dans l'hypothèse où la surveillance ou la géolocalisation sont nécessaires pour l'organisation pour des exigences d'organisation, de production ou de sécurité de l'emploi, conformément à l'article 4 de la loi 300/1970 qui prévoit que la surveillance à distance des employeurs est possible, avec l'accord de la Société des représentants, ou, à défaut, de la commission interne. En outre, dans certains cas, l'emplacement géographique peut être utile pour renforcer les conditions de sécurité. Des précautions adéquates doivent être prises, s'agissant de la localisation de données géographiques captées par une application active sur un smartphone fourni à un employé, comme a pu le préciser le Garant à travers deux décisions récentes.

L'un des textes plus important en droit italien à cet égard est le fameux « *decreto legislativo* » D.Lgs 196/2003. En effet, lorsque la thématique de la géolocalisation en droit italien est abordée, il convient de toujours se référer à ce texte. Ce décret prévoit que les données relatives à la géolocalisation sur des véhicules ou des outils, s'ils sont associés directement ou indirectement aux salariés peuvent être en mesure de révéler un certain nombre de données personnelles et doivent par conséquent respecter les principes suivants : liceità (licéité), finalità (finalité) necessità (nécessité), et proportionalità[164] (proportionnalité).

En résumé, il est important de rappeler à l'égard de cet encadrement législatif que l'article 114 du code de la Privacy renvoie à l'article 4 du statut des travailleurs qui dispose « *E vietato l'uso di impianti audiovisivi e di altre apparechiature per finalità di controllo a distanza dell'attività del dipenti* […], ce qui signifie que le contrôle des travailleurs par le biais d'implants et d'autres appareils ayant pour finalité le contrôle à distance des salariés est en principe interdit. Le principe c'est l'interdiction, l'exception est parfois autorisée comme nous allons le voir à travers les décisions rendues par le « garant pour la protection des données personnelles » en Italie.

[163] DE SANTIS (F.), « Garante Privacy : Geolocalizzare i dependenti per migliorare la qualità del servizio », <www.portolano.it>
[164] RAPICAVOLI (R.), « Geolocalizzazione e Privacy : una convivenza possibile », publié le 24 janvier 2015, <www.fedaiisf.it>

B) Le garant pour la Privacy, gardien de l'application des principes en Italie

En Italie, le garant pour la Privacy est une autorité administrative indépendante instituée par la loi n°675 du 31 décembre 1996. L'objectif du Garant est d'assurer la protection des droits et des libertés fondamentales, et le respect de la dignité dans le traitement des données personnelles. Antérieurement, le Garant pour la privacy avait déjà autorisé le traitement de données relatives à la localisation des salariés dans deux cas,[165] dans lesquels l'employeur avait mis en œuvre tous les prérequis prévus par le Statut des travailleurs, et par le Code de la Privacy.

Dans une décision rendue le 7 octobre 2010[166], le Garant pour la protection de la Privacy a précisé que « l'acquisition de données de localisation peut constituer un traitement de données personnelles dans la mesure où ces informations peuvent être associées à d'autres ». Ainsi, les données obtenues à travers GPS, associées à des données qui permettent d'identifier un individu peuvent être considérés comme des données personnelles, telles qu'énoncées par l'article 4 de la loi D.Lgs 196/2003. En outre, les données de localisation peuvent parfois être des données sensibles, dans l'hypothèse où elles sont associées avec des données qui permettent d'identifier par exemple la croyance religieuse d'un individu, ou l'appartenance à un syndicat.

Le garant pour la Privacy à travers deux décisions importantes du 11 septembre et du 9 octobre 2014 a déclaré que « *la géolocalisation à travers des applications installées sur un smartphone d'entreprise requiert une attention particulière, étant donné que ce type de dispositif mobile a pour caractéristique d'être destiné à suivre la personne qui le détient, et que par conséquent le traitement de données par un tel instrument présente des risques pour la liberté, les droits et la dignité des salariés*. » En l'espèce, les deux décisions évoquées ci-dessus concernent deux sociétés qui ont demandé préalablement à l'autorité garante de la protection des données son avis à propos de leur intention d'utiliser des données provenant d'une application de géolocalisation installée sur les smartphones des salariés pour optimiser le travail et améliorer la gestion et la coordination en entreprise[167] Dans la décision rendue le

[165] Décision du 5 juin 2008 [1531604], disponible sur www.garanteprivacy.it/ Décision du 7 octobre 2010, [1763071]
[166] Décision du 7 octobre 2010 [1763071], disponible sur www.garanteprivacy.it
[167] MAROSCIA (A.), « Privacy : uso dei dati di geolocalizzazione dei lavoratori », publié le 5 novembre 2014, <www.lavoroediritti.com>

11 septembre 2014, le Garant pour la Privacy s'est prononcé sur la problématique de l'installation d'un dispositif capable de communiquer la géolocalisation d'un salarié toutes les 15 minutes. Toutefois, ce dispositif ne permettait pas une géolocalisation permanente. En effet, le dispositif ne permettait l'accès qu'à la dernière position. Ainsi, la nouvelle position annulait l'ancienne. Dans le cadre de cette affaire, l'autorité garante a validé ce dispositif mais elle pose un certain nombre de conditions, parmi lesquelles :

- La société doit adopter des mesures spécifiques afin de garantir que les informations présentes sur le dispositif mobile ne se réfèrent exclusivement aux données de géolocalisation et non à des données relatives aux SMS, boîtes e-mails etc.
- La configuration du système de manière à ce que le dispositif de géolocalisation soit indiqué par une icône, qui permet d'informer l'utilisateur quand la géolocalisation est activée. A cet égard, l'icône doit toujours être clairement visible sur l'écran du smartphone quand bien même l'application serait en *« back-ground* ».
- L'accès aux données doit être seulement réservé aux personnels de la société qui peuvent en prendre connaissance.
- La société doit également notifier au Garant le traitement de données relatives à la localisation.
- La société doit recommander aux salariés d'effectuer périodiquement le nettoyage de données mémorisées localement à travers l'activation de la fonction « *clear stored data* ».
- Une information complète et claire doit être donnée aux salariés de la société sur la nature du traitement de données et sur les caractéristiques du dispositif.

L'autorité garante pour la protection des données personnelles en Italie a rendu une deuxième décision importante, le 9 octobre 2014. Dans cette décision, le Garant pour la Privacy a été amené à se prononcer sur la problématique du traitement de données personnelles des salariés effectuées à travers la géolocalisation par le biais de smartphones. Dans cette affaire, l'opérateur de télécommunication « Wind » a présenté une demande de vérification préliminaire au sens de l'article 17 du code de la Privacy en lien avec le traitement de données personnelles, à propos de l'activation d'un logiciel qui prévoyait entres autres l'utilisation de techniques de géolocalisation des smartphones, fournis par l'entreprise. Il était prévu que les données soient traitées par la société seulement après avoir fourni une information détaillée aux salariés, publiée sur l'intranet de l'entreprise. Dans cette décision, le Garant pour la protection des données personnelles a déclaré légitime l'utilisation d'applications installées

sur des smartphones pour les salariés, qui à travers la géolocalisation des dispositifs pouvaient relever l'exacte position des salariés, pour des finalités d'organisation, de production, et un impératif de sécurité. Toutefois, le Garant pour la protection des données personnelles a néanmoins conditionné la légitimité reconnue au respect d'un certain nombre de principes, parmi lesquels :

- ✓ L'adoption de mesures spécifiques pour garantir que les informations présentes sur les dispositifs mobiles, soient exclusivement celles qui se réfèrent aux données de géolocalisation, et non à d'autres types de données comme les données SMS, mails
- ✓ La configuration du système de manière à ce que le dispositif de géolocalisation soit indiqué par une icône, qui permet d'informer l'utilisateur quand la géolocalisation est activée. A cet égard, l'icône doit toujours être clairement visible sur l'écran du smartphone quand bien même l'application serait en « back ground ».
- ✓ L'accès aux données doit être seulement réservé aux personnels de la société qui peuvent en prendre connaissance.
- ✓ Enfin, la société doit également notifier au Garant le traitement de données relatives à la localisation.

Par conséquent, cette décision confirme la précédente.

Chapitre 2. Vers une consécration opportune d'un droit à la déconnexion face aux risques liés à l'exigence d'hyper productivité et à l'usage intensif du numérique

Aujourd'hui, le droit des technologies de l'information et de la communication et le droit du travail apparaissent véritablement liés l'un à l'autre. Les interférences et les points de convergence entre ces deux droits sont fréquents. Il est important de rappeler préalablement

que les TIC en modifiant les conditions de travail des salariés et les rapports sociaux entre eux et envers l'employeur ont aussi été parfois identifiés comme une source de troubles psychosociaux[168]. Ces risques ont fait l'objet d'une appréhension progressive par le droit. Toutefois, nous verrons que le droit du travail n'a pas encore fait l'objet d'importantes modifications **(Section 1**). Pour répondre à cette problématique des risques ainsi que des troubles psychosociaux, qui semblent aujourd'hui s'accroître avec le développement de la mobilité, nombreux sont ceux qui revendiquent aujourd'hui la consécration d'un « droit à la déconnexion ». Ainsi, l'employeur doit aujourd'hui agir contre ces risques en vue d'assurer la protection de ses salariés (**Section 2**).

Section 1. L'appréhension des risques psychosociaux

L'hyper-connexion, renforcée incontestablement par l'utilisation d'outils mobiles et connectés peut avoir pour conséquence directe une augmentation des risques et des troubles psychosociaux chez le salarié (**paragraphe 1**). Face à cela, l'employeur ne peut rester inactif et il lui appartient d'agir en vue de la prévention de ces risques.

[168] Cours de Madame TOUBOUL Alexandra, dispensé dans le cadre du Master 2 Droit des médias et des télécommunications, Université Aix-Marseille, 2014-2015

En effet, ces risques sont néfastes non seulement pour le salarié qui en est la principale victime mais également pour l'employeur, qui à défaut d'actions pourra voir sa responsabilité engagée (**paragraphe 2**).

§1 – Le salarié, sujet de risques et de troubles psychosociaux

Les risques psychosociaux sont très divers. C'est pourquoi, il est nécessaire préalablement d'identifier précisément ces risques (A) avant d'évoquer l'appréhension juridique progressive dont ils ont fait l'objet (B).

A) L'identification des risques et des troubles psychosociaux

Par définition, les risques psychosociaux peuvent être définis comme « les maux qui menacent la santé mentale du salarié lors de l'exécution de son contrat de travail ». [169] Par ailleurs, selon le Ministère du travail, ces risques recouvrent en réalité « des risques professionnels d'origine et de nature variée, qui mettent en jeu l'intégrité physique et la santé mentale des salariés et ont, par conséquent, un impact sur le bon fonctionnement des entreprises ». En outre, les risques psychosociaux peuvent être également définis de la façon suivante : « l'ensemble des troubles ou des risques de troubles de la santé mentale du salarié, troubles dont le lien avec le travail est établi, et qui résultent principalement d'agissements de harcèlement, de stress, de violences physiques ou verbales, d'épuisement professionnel ou d'un sentiment de mal-être au travail ».[170]

En mai 2015, un guide d'aide à la prévention de l'épuisement professionnel a été publié. Il s'agit ici d'une initiative de l'Anact, l'INRS et du Ministère du travail.

Aujourd'hui, la charge mentale et psychologique qui est imposée aux salariés est de plus en plus importante, et les situations de stress de grande ampleur sont presque devenues « banales », communes et acceptées au sein du milieu professionnel. Ainsi, il apparaît que le « burn-out », appelé en français « épuisement professionnel » n'est plus un tabou dans notre société. Par définition, le « burn-out » est « un processus de dégradation du rapport de

[169] VALLOIS (C.), *L'employeur contre les risques psychosociaux*, Master 2 Professionnel Droit et Pratique des Relations du Travail, 2013-2014, p.7
[170] TOURNAUX (S.), *Droit du travail*, Grand Amphi Droit, p.515

l'individu à son travail au bout duquel l'individu s'écroule »[171]. Parmi les facteurs de RPS et donc de burn-out se trouvent les exigences au travail notamment l'intensité et le temps de travail.

Toutefois, on constate progressivement que le droit cherche à appréhender de plus en plus cette situation[172]. Les risques psychosociaux apparaissent comme une problématique complexe, notamment eu égard à l'absence de définition claire et précise. L'observatoire des risques de l'Agence Européenne pour la santé et la sécurité au travail a néanmoins identifié 42 risques psychosociaux parmi lesquels : l'intensification du travail et le mauvais équilibre entre la vie privée et l'activité professionnelle. S'agissant des facteurs de risques psychosociaux, l'Agence européenne évoque : l'intensité du travail, le contrôle ou pouvoir de décision du travailleur sur son travail, l'équilibre vie privée et vie familiale. Au regard de leur dimension multifactorielle, l'identification des RPS s'avère néanmoins très difficile et les RPS sont au cœur de l'actualité. Ainsi, un avis a été rendu le 14 mai 2013 par le Conseil économique, social, environnemental[173]. Cet avis précise que « l'employeur doit prôner un bon usage des TIC » et conseille de « recourir à des chartes d'entreprises qui peuvent être utilisées par les entreprises pour assurer la protection de la santé et de la sécurité et tracer une frontière entre vie privée et la vie professionnelle ». Il est pertinent de noter que l'avis du Conseil souligne qu'il est important de distinguer d'une part « les risques psychosociaux qui sont les risques professionnelles », et d'autre part « les troubles psychosociaux, qui sont les conséquences sur la santé physique ou mentale ».

B) La reconnaissance progressive des risques et des troubles psychosociaux

L'objectif de protection de la santé mentale existe tant au niveau interne qu'international. Ainsi, il apparaît qu'il s'agit véritablement d'une problématique mondiale, et particulièrement européenne tant à l'échelle nationale qu'en Italie, dont les enjeux sont très importants. En effet, le coût annuel du stress au travail s'élève en Europe à plus de 20 milliards d'euros[174].

[171] ANACT, INRS, Ministère du travail, Guide pratique pour prévenir le syndrome d'épuisement professionnel, 21 mai 2015, p.12
[172] COEURET (A.), GAURIAU (B), MINE (M.), *Droit du travail*, 2006, Syrey, DALLOZ, p.44
[173] Avis du Conseil Economique Social et Environnemental du 14 mai 2013, rapporteur SYLVIE Brunet, disponible sur <www. Lecese.fr>
[174] Risques psychosociaux au travail : une problématique européenne, Eurogip, janvier 2010

D'un point de vue historique, la prise de conscience des risques psychosociaux a commencé au début des années 2000 au niveau international (1). Nous verrons ensuite comment ces risques ont été appréhendés en France (2), avant d'évoquer l'appréhension de ces risques et troubles en Italie (3).

1) L'appréhension internationale des risques psychosociaux

En matière de santé au travail sur un plan international, il est d'usage de faire référence aux textes de l'OIT. Selon l'article 3 de la convention n°155 de l'OIT de 1981 sur la sécurité et la santé des travailleurs, entrée en vigueur le 11 août 1983, le terme « santé » ne vise pas seulement l'absence de maladie ou d'infirmité. Ce terme inclut aussi « les éléments physiques et mentaux affectant la santé directement liés à la sécurité et à l'hygiène du travail ».

Par ailleurs, selon le comité mixte OIT/OMS de la santé au travail en 1950 : « *l'objectif de sécurité et de santé au travail doit être de contribuer à promouvoir et à maintenir le plus haut degré de bien-être physique, mental et social dans toutes les professions*. » Enfin, la recommandation n°164 de 1981 qui complète ce texte préconise, la « prévention de tout stress physique ou mental » préjudiciable à la santé due aux conditions de travail, et au niveau de l'entreprise « de prendre toutes mesures raisonnables et pratiquement réalisables en vue d'éliminer une fatigue physique ou mentale exagérée ».[175]

Au niveau communautaire, la directive 89/391/CEE du 12 juin 1989 énonce des obligations pour les employeurs qui n'excluent pas les RPS : ceux-ci sont inclus de façon implicite dans l'obligation d'assurer la santé et la sécurité des travailleurs dans les aspects liés à leur travail.

En outre, le 8 octobre 2004, un accord-cadre sur le stress a été signé entre les partenaires sociaux européens. L'objectif de cet accord était la sensibilisation des employeurs, des travailleurs et de leurs représentants aux problèmes de stress au travail. Cet accord revêt une importance dès lors qu'il reconnait l'existence du problème du stress au travail, les bénéfices de la prévention et la responsabilité des employeurs dans ce domaine, à exercer en collaboration avec les salariés[176]. Cet accord entre les syndicats européens et les organisations des employeurs définit également le stress au travail comme « un mal être, un

[175] COTTIN (J-B.), MIR (J-M.), « Risques psychosociaux : perspectives internationales », *Les cahiers du DRH*, février 2011, n°173, p.47
[176] Risques psychosociaux au travail : une problématique européenne, Eurogip, *ibid*., p.8

dysfonctionnement physique, psychologique ou social qui est la conséquence du fait que les individus ne se sentent pas à la hauteur des demandes ».

Comme nous l'avons vu, le phénomène des risques psychosociaux est difficile à définir et à appréhender. Toutefois, les législations tant au niveau communautaires que nationales imposent aux entreprises de prendre en compte ces risques.

2) L'appréhension française des risques psychosociaux

En France, on a évolué de manière progressive de la protection de la santé physique à la protection de la santé mentale. On a toutefois semble-t-il assisté à une véritable prise de conscience à l'égard de ces risques, notamment ces dernières années. Ainsi, la France semble disposer d'un cadre juridique en matière de protection des salariés, bien que celui-ci n'apparaisse pas complet. La loi de modernisation sociale du 17 janvier 2002 a étendu l'obligation de sécurité de l'employeur à la protection de la santé mentale. La santé mentale au travail est dorénavant plus fréquemment appréhendée sous l'angle de la prévention[177]. Des dispositions législatives existent, ainsi l'article L4121-1 du code du travail rappelle que l'employeur doit éviter les risques et protéger la santé physique et mentale du salarié. Cet article contient des dispositions de prévention spécifique relatives à certains risques. Une obligation de sécurité s'impose donc à l'employeur dès lors que cet article dispose : « l'employeur prend les mesures nécessaires pour assurer la sécurité ». En plus de ce cadre, la jurisprudence est venue imposer une obligation de sécurité de résultat dont certains ont pu dénoncer toutefois l'ambiguïté. La Cour de cassation a dégagé de l'article L4121-1 une obligation de résultat pour l'employeur. L'employeur ne peut pas se contenter de prétendre ne pas avoir été en position de connaître le risque, mais il doit démontrer qu'il avait pris toutes les mesures nécessaires pour l'éviter.

En outre, un accord interprofessionnel du 2 juillet 2008 s'est également intéressé au stress au travail. Il transpose l'accord cadre européen signé le 8 octobre 2004. Cet accord rappelle que l'employeur est responsable de « protéger la santé mentale des salariés au même titre que la santé physique », que toute entreprise est susceptible d'être affectée par la problématique du stress au travail, quelle que soit sa taille, son type d'activité, le type de contrat. L'objet de

[177] VALLOIS (C.), *L'employeur contre les risques psychosociaux*, Master 2 Professionnel Droit et Pratique des Relations du Travail, 2013-2014, p.8

l'accord est le suivant : « augmenter la prise de conscience et la compréhension du stress au travail, par les employeurs, les travailleurs et leurs représentants ».

Par le biais du développement des technologies de l'information et de la communication mobiles, la pression pouvant être exercée sur les salariés peut se révéler plus importante. La problématique du juste équilibre entre vie personnelle et professionnelle n'est ainsi pas seule. En effet, une partie de la doctrine et des auteurs spécialistes des TIC dénoncent la culture de « l'instantanéité »[178] qui peut avoir des conséquences sur les RPS. Ainsi, on assiste à une véritable prise de conscience de plus en plus importante de la part des juristes et aussi des professionnels en France, du bien-être physique et psychique des salariés.

3) L'appréhension italienne des risques psychosociaux

Les risques psychosociaux sont reconnus comme l'un des principaux problèmes de santé dans le milieu professionnel en Italie. Les RPS y sont entendus comme « un ensemble de facteurs affectant la réponse psychologique des salariés en milieu professionnel et à leurs conditions de travail, et renvoyant à la fois au bien-être physique et psychologique. » [179] Le droit italien ne comporte pas de dispositions spécifiques sur la question. La Constitution italienne contient des dispositions générales relatives à la santé et à la sécurité des personnes. Le Code civil exige que l'employeur prenne toutes les mesures nécessaires pour protéger la santé physique et mentale de ses travailleurs. L'idée des dispositions précitées est que la protection de la santé et de la sécurité des salariés sur le lieu de travail ne relève pas seulement du droit individuel, mais aussi de l'intérêt collectif.

Un « décret-législatif » du 9 avril 2008 concernant la santé et la sécurité au travail fait référence au stress et oblige les employeurs à élaborer un rapport d'évaluation de tous les risques liés à la santé et à la sécurité de leurs salariés. Ce rapport doit décrire toutes les mesures prise par l'employeur pour assurer la santé et la sécurité de ses travailleurs et identifier les tâches qui peuvent entraîner des risques spécifiques. Enfin, le « decreto legislativo» n°81/2008 a instauré, en Italie, un organe représentatif du personnel spécialisé en santé et sécurité au travail, constitué de trois structures distinctes. En général, ces comités doivent identifier et analyser les problèmes concernant la santé et la sécurité au travail et formuler toutes les mesures d'amélioration. Au-delà, le véritable objectif du décret-loi a été de

[178] BESSEYRE DES HORTS (C-H.), *L'entreprise mobile : comprendre l'impact des nouvelles technologies*, Pearson, *op.cit*, p .164
[179] COTTIN (J-B.), MIR (J-M.), « Risques psychosociaux : perspectives internationales », op.cit, pp.47-59

créer une coopération entre tous les membres du personnel de l'organisme, d'établir un cadre dans lequel les employeurs et les représentants des employés peuvent travailler ensemble pour prévenir les risques psychosociaux, et en particulier, le stress au travail.

§2 – L'employeur, acteur de la protection contre ces risques

L'employeur ne peut rester inactif face à ces risques. Il lui incombe ainsi une obligation de sécurité en France (A), ainsi qu'en Italie (B).

A) L'obligation de sécurité à la charge de l'employeur en France

Comme nous l'avons précédemment vu, l'employeur en France doit donc prendre toutes les mesures pour assurer la protection de la santé physique et mentale du salarié, en vertu de l'article L4121-1 du code du travail. Il s'agit d'une obligation de résultat, rappelé par la jurisprudence dans un arrêt rendu le 22 février 2002[180]. Cette obligation peut viser également les risques psychosociaux. Parmi les obligations qui lui incombent, l'employeur doit notamment mener des actions d'information et de formation de ses salariés sur la santé et la sécurité, conduire des actions de prévention des risques professionnels et mettre en place des moyens de travail adaptés.

B) L'obligation de sécurité à la charge de l'employeur en Italie

L'article 32 de la Constitution italienne dispose *« la Repubblica tutela la salute come fundamentale diritto del'individuo »*, ce qui veut dire *« la République protège la santé en tant que droit fondamental de l'individu et intérêt de la collectivité»*.

Il est aussi à noter que l'accord européen sur le stress au travail du 8 octobre 2004 évoqué précédemment ne s'applique en Italie que depuis 2008[181]. Ainsi, les entreprises ont l'obligation de protéger la santé des salariés. L'article 2 du « decreto legislativo » D.Lgs 81/2008 définit la santé comme « un stato di completo benessere fisico, mentale e sociale, non consistente solo in un'assenza di malattia o d'infermità », c'est-à-dire en français, « un état de

[180] Cass.soc, 22 févier 2002, n°99-18389
[181] BEDIN (C.), rischi psico-sociale per stress da lavoro-correlato (rappresentanti dei lavoratori per la Sicureza Università degli Studi di Padova), Padova, 22-24 Février 2011

bien-être, physique, mental ou social qui ne consiste pas seulement en l'absence de maladie ou d'handicap ». Ce texte évoque également l'obligation de sécurité à la charge de l'employeur en Italie. Ainsi, l'employeur est entre autres responsable de l'évaluation des risques.

En résumé, il apparaît qu'aujourd'hui la prise en compte des RPS est encore largement insuffisante, et de plus en plus de salariés semblent maintenant attirés par « la déconnexion » afin de préserver leur santé « mentale » et parfois aussi « physique ».

Section 2. La pertinence de la déconnexion : une utopie face à l'hyper-connexion, « mal du siècle »

Face à l'hyper-connexion qui concerne notamment les salariés, l'idée d'un droit à la déconnexion s'est progressivement imposée (**paragraphe 1**). Aujourd'hui, la déconnexion ne semble plus être simplement une idée, mais une véritable tendance qui s'impose parfois comme une « obligation » qui concerne de plus en plus d'entreprises et qui apparaît véritablement en voie de devenir effective. Ainsi, Jean-Emmanuel Ray n'hésite pas à qualifier ce droit, de « droit à la vie privée du 21e siècle ». (**paragraphe 2**).

§1 – L'émergence de l'idée d'un droit à la déconnexion

Les moyens mis à la disposition des salariés aujourd'hui permettent une multi-connexion qui peut dans certains cas conduire à une hyper-connexion (A). Face à ce phénomène, la tendance de plus en plus marquée est aujourd'hui la déconnexion. Toutefois, il est intéressant de souligner que selon Jean-Emmanuel Ray, professeur en droit social, il s'agirait néanmoins d'une problématique assez récente (B).

A) De la multi-connexion à l'hyper-connexion

Il me parait pertinent de s'interroger préalablement sur un précédent : le droit au repos (1), afin d'analyser la problématique de l'hyper-connexion (2).

1) Le droit au repos : un hypothétique précédent au droit à la déconnexion

Si le thème qui fait l'objet de l'actualité est maintenant celui de l'hyper-connexion, il y a quelques années, le thème était plutôt celui du droit au repos. Bien qu'au départ, il est important de le rappeler le repos n'était pas considéré comme un droit. Le « repos » était alors plutôt assimilé à un besoin des salariés face aux conditions de travail très difficiles et bien souvent éprouvantes. Progressivement, le repos est devenu une obligation qui s'impose à l'Etat et à l'employeur[182]. Le repos peut être défini comme « le fait de cesser son activité ». Il me paraît ici opportun de faire un parallèle entre d'une part le droit au repos et d'autre part le droit à la déconnexion. En effet, selon moi, en souhaitant permettre aux salariés de se déconnecter à certains moments, on cherche également à leur assurer d'une certaine façon un droit au repos plus important, en vue d'éviter que les salariés soient trop sollicités en étant hyper-connectés. En effet, la déconnexion devrait en principe permettre un bien-être « psychologique » pour le salarié face à une connexion qui devient parfois omniprésente et où la « déconnexion » est parfois inexistante au détriment de la vie personnelle de l'individu. En outre, l'idée d'un droit à la déconnexion fait également toutefois débat. Comment mettre en place la déconnexion au sein de l'entreprise ? Sur qui faire reposer la responsabilité de la mise en place de ce dispositif ? Autant de questions qui n'ont pas toujours de réponses.

Il est également intéressant de citer une autre décision de justice pour illustrer ces propos. Par exemple, la décision rendue par la Cour de cassation le 17 février 2004 au sein de laquelle les juges ont considéré que « le fait de ne pas pouvoir joindre un salarié en dehors des horaires de travail sur son téléphone personnel ne constitue pas une faute disciplinaire et ne justifie pas un licenciement ». Par conséquent, le salarié a droit à son « temps de pause ».

Au niveau du droit communautaire, la CJUE a également été amenée à rappeler que le droit au repos constitue un principe du droit social communautaire important. Ainsi, la protection de la santé a été consacrée constitutionnellement au même titre que le droit au repos au sein de l'article 17 du préambule de la constitution de 1946.

En effet, très rapidement, les conséquences que peuvent avoir le travail sur la santé ont été appréhendées par le droit. Ainsi, le droit au repos permet non seulement de protéger la santé physique ainsi que psychologique des salariés[183].

2) La problématique de l'hyper-connexion

[182] SOLIVERES Anne-Victoria, *Le droit au repos*, Mémoire Master 2, Université Panthéon-Assas, 2013, p.29
[183] SOLIVERES Anne-Victoria, *Le droit au repos* , Mémoire Master 2, *ibid.* 2013, p.29

La déconnexion : tendance de passage ou véritable nécessité ? L'hyper-connexion est souvent accusée de conduire régulièrement à une perte de contact avec la réalité, d'où le mal être qui peut en résulter pour le salarié et qui peut conduire à un « burn-out professionnel ». Dans le cadre de cette sous-partie, il me paraît important d'évoquer la progression de « l'intensité » de la connexion chez les individus. En effet, il semblerait que l'hyper-connexion soit en lien avec la « multi-connexion ». Ainsi, la connexion « limitée et fixe» a évolué de façon très importante. Face au développement des nouvelles technologies et de « l'Internet des objets », on assiste à l'apparition constante de nouveaux outils mobiles et connectés. Ces outils contribuent à renforcer la connectivité et l'interaction qui semble parfois devenir quasiment permanente entre les individus, tant au niveau personnel que professionnel. A titre d'illustration, aujourd'hui, le nombre d'écrans dans un foyer français est en moyenne de 5. Ainsi, si l'entreprise fournit d'autres écrans à son salarié ou qu'elle lui permet d'apporter ses propres écrans sur son lieu de travail, il est possible de s'inquiéter des effets « néfastes » de l'hyper-connexion. Certains n'hésitent plus à qualifier ce comportement de « course à l'interconnexion ». En effet, nombreux sont les individus connectés en « permanence » car ils expriment souvent « la crainte » de « perdre une information ». « Cette crainte » qui peut s'exprimer dans un cadre personnel peut également s'exprimer dans un « cadre professionnel ». On distingue aujourd'hui trois moyens privilégiés pour se connecter à internet : l'ordinateur, la tablette et le smartphone. L'utilisation de ce dernier est en générale brève mais très fréquente[184].

En général, le terme d'hyper-connexion est employé pour un temps consacré à Internet excessif par rapport à d'autres types d'activités, c'est-à-dire à partir de 3h par jour, environ. Selon un sondage qui a été publié par l'APEC en décembre 2014, 23% des cadres disent ne « jamais se déconnecter », 22% « rarement », et 63% considèrent que les TIC « perturbent leur vie personnelle et familiale ». Selon une autre étude Roambi et Zebab qui a été mené auprès de décideurs français : 54% d'entre eux travaillent au moins la moitié de leurs temps en dehors de leur lieu de travail, 62% consultent leurs données professionnelles au moins une fois par jour et 89% consultent leurs e-mails plusieurs fois quotidiennement. En outre, pendant les congés, cette étude met en évidence que les « cadres » continuent d'être toujours très connectés en consultant de façon très fréquente certaines informations relevant de la sphère professionnelle. Ainsi, 93% consultent ce type de données pendant leurs vacances. En

[184] MADEROU (T.), Mémoire d'étude, Mémoire de projet, sur l'hyperconnexion, Ecole Boulle, 2013, p.18

outre, 47% considèrent les devices mobiles (smartphones, tablettes) comme étant « indispensables ».

Historiquement, selon Yves Lasfargues, consultant et spécialiste des nouvelles technologies de la communication, la notion d'hyper connectivité ne serait pas nouvelle mais remonterait à l'utilisation des premiers téléphones portables et à l'envoi des premiers e-mails, c'est-à-dire au cours des années 1990. Une nouvelle étape aurait été franchie avec l'arrivée des smartphones. Toutefois, Yves Lasfargues souligne qu'il a fallu attendre 2010 pour que l'on s'interroge véritablement sur les problématiques issues de cette notion. Cette hyper-connexion entraîne de nombreuses conséquences néfastes parmi lesquelles il est possible de distinguer l'harcèlement numérique et l'infobésité.

« L'hyper-connexion » est également un phénomène qui peut être constaté en Italie et qui soulève des problèmes dans la balance et la recherche d'un équilibre entre vie personnelle et vie professionnelle. Pour certains, le fait que la « connexion soit devenue omniprésente a transformé notre fréquence d'utilisation en un flux continu n'admettant presque plus la déconnexion ».[185] Le terme « d'infobésité » est souvent évoqué pour qualifier la surcharge d'information à l'égard des salariés. Il est à noter toutefois que le droit à la déconnexion a véritablement des difficultés à être accepté par tous. Néanmoins, de nombreux acteurs tentent d'encadrer cette évolution afin de préserver le droit au repos du salarié.

B) La déconnexion face à l'usage intensif des TIC : une tendance en hausse

La déconnexion semble être « une tendance » qui réussit à s'implanter de plus en plus dans l'Hexagone. Selon une étude HAVAS Média de septembre 2012, le nombre de déconnectés en France s'élève à 9,3 millions, soit 18,3% de la population. Ainsi, les bienfaits de la déconnexion font parler d'eux dans le milieu professionnel. En effet, une étude réalisée par Metric Lab sur les déconnectés de France semble témoigner de la nécessité de la consécration de ce droit. Ainsi, selon cette étude : « 27,6 % des personnes interrogées répondent souvent à des mails professionnels après le travail ou lors des week-end et congés » et « 37,7 % répondent à des SMS ou à des messages pendant un déjeuner ». Toutefois, cette étude semble très encourageante dès lors que « 65,2% des individus ont envie de se déconnecter de ces nouvelles technologies et 59,7% le font effectivement par intermittence ». Régulièrement, les

[185] MADEROU (T.), Mémoire d'étude, Mémoire de projet, sur l'hyperconnexion, *op.cit.*, p.44

TIC sont présentées comme intensifiant et généralisant ces échanges parfois à outrance. Il est certain que les TIC rendent les échanges beaucoup plus brefs et formels dorénavant[186]. A cet égard, la banque française « Société générale » a fait circuler à ses salariés un document relatif au bon usage de « la messagerie et de l'e-mail » dès 2009. En effet, la rédaction et l'envoi de l'e-mail sont souvent pointés du doigt car conduisant à une « infobésité ».

Les raisons de la déconnexion sont nombreuses et diverses. Ainsi, toujours selon cette même étude, parmi les 65,5% de français qui ont envie de se déconnecter de ces nouvelles technologies, 59,7% le font effectivement par intermittence. 74,8% des français « déconnectés » le font car ils se disent « trop sollicités », 59,3% car ils souhaitent « se ménager un peu de tranquillité » pour eux-mêmes, 52,5% car ils considèrent être coupés de la « vraie vie », des relations avec la famille et les amis. La déconnexion 2.0 semble marquer une véritable prise de conscience.

Selon le reportage « *Digital Detox* » du journaliste Pierre-Olivier Labbé, *« l'avenir s'annonce hyper-connecté* » et la « *déconnexion est l'un des grands luxes de la fin du siècle* ». Le journaliste n'hésite pas à qualifier son smartphone de « prolongement » de lui-même et dit être « devenu esclave d'une technologie intrusive ». Selon lui, « la déconnexion sera de plus en plus difficile » avec tous les objets et environnements connectés qui se démocratisent. Au sein de ce reportage, des chiffres percutants ont été énoncés. Par exemple, « 1 français sur 2 est dorénavant équipé d'un smartphone et un cadre consulterait son smartphone en moyenne 150 fois par jour ». L'objectif du journaliste à travers ce reportage était de comprendre de quelle manière la révolution numérique a bouleversé nos existences. Le journaliste a ainsi voulu s'interroger sur l'hypothèse de solutions alternatives pour « mieux gérer » et « moins subir » selon ses dires. Selon lui, le mail serait devenu l'unique moyen de communiquer « professionnellement ». Par ailleurs, « un cadre consulterait ses mails environ 50 fois par jour, 70% d'entre eux vérifieraient leur mails toutes les 5 minutes, 1 salarié sur 2 se dit victime d'overdose d'information ». Ce reportage a reçu un très bon accueil et a attiré de très nombreux téléspectateurs, ce qui témoigne de l'intérêt que les français commencent à porter à l'égard de cette problématique.

Il est alors possible de s'interroger : cette hyper-connexion ne serait-elle pas le mal du siècle dans l'entreprise ? L'hyper-connexion ou connexion « à outrance » aujourd'hui inquiète notamment les syndicats comme la CFDT ou la CGT. En effet, selon ces derniers, l'envoi et

[186] ANONYME, « La technologie n'est pas l'ennemie du bien-être au travail », publié le 8 mars 2012, <www.manpowergroup.fr>

la réception d'e-mails en permanence conduit à une pression permanente des salariés. Selon la CGT, le salarié doit avoir le droit de ne pas se connecter à sa boîte e-mail en soirée. Toutefois, la CGT souligne que chaque salarié est aussi pollueur. Par conséquent, à charge pour chacun de ne pas polluer. Il s'agit donc d'un devoir de ne pas se connecter vis-à-vis des autres. Selon ceux qui se montrent en faveur d'un droit à la déconnexion, celle-ci permet de nombreux apports, entre autres, elle permettrait de bénéficier d'un meilleur équilibre et d'une meilleure qualité de vie au travail.

Ainsi, selon un sondage Ugict-Cgt publié en avril 2015[187], parmi les trois priorités des cadres qui sont : la qualité de vie au travail, le salaire, l'équilibre entre vie privée et vie professionnelle, c'est ce dernier qui arrive en tête à 67%. Ce sondage révèle également que 3 cadres sur 4 font un usage professionnel des outils numériques en dehors des heures de travail et que le temps de travail déclaré s'élève en moyenne à 44,6 heures.

Le besoin d'une consécration d'un droit à la déconnexion interroge et divise en entreprise. En effet, certains ont pu mettre en évidence un paradoxe sur ce point. Nombreux sont ceux qui rappellent que bien souvent, ce sont ceux qui sont à l'origine de l'hyper-connexion, qui se plaignent le plus de cette connexion exacerbée et qui s'en disent « victimes ». [188]

§2 – L'effectivité du droit à la déconnexion

Si le droit à la déconnexion est parfois une revendication des salariés, certains dirigeants et de nombreux syndicats dénoncent aussi un usage des outils mobiles et connectés qui a pour conséquence une connexion quasiment permanente (A). Néanmoins, la mise en œuvre de ce droit interroge et divise (B).

A) Une revendication dans le milieu professionnel

Selon un rapport commandé par l'Office allemand pour la sécurité au travail regroupant des études internationales « *plus le travail empiète sur la sphère privée, plus les salariés font état*

[187] Sondage Ugict-CFT, avril 2015, Viavoice
[188] BISEUL (X.), « Le droit à la déconnexion peine à s'appliquer », publié le 31 mars 2015, <www.pro.01net.com>

de stress, de burn-out, et d'incapacité à se déconnecter ».[189] Les syndicats professionnels ont été particulièrement actifs dans le cadre de la revendication du droit à la déconnexion. Ainsi, l'Ugict-CGT a notamment émis un certain nombre de propositions dont Monsieur Jean-Luc Molins, secrétaire national de l'Ugict-CGT m'a parlé lors de notre entretien (**cf.annexe n°2**) et mène actuellement une campagne pour « le droit à la déconnexion » avec des images fortes pour sensibiliser les individus (**cf.annexe n°3**). L'objectif qui doit être poursuivi selon le syndicat est « l'encadrement de l'usage des TIC pour protéger le repos et la vie privée des salariés ». C'est pourquoi, le syndicat préconise entre autres « *d'instituer une négociation obligatoire dans chaque entreprise sur l'utilisation des outils numériques, qui prévoit des plages de trêve de mails* » et « *l'interdiction que le salarié puisse être récepteur d'une sollicitation professionnelle durant ses temps de repos* ». Il me paraît ici opportun de citer quelques chiffres percutants évoqués au cours du séminaire « Négocier le droit à la déconnexion » qui s'est tenu le 15 octobre 2014 et qui illustrent parfaitement les risques liés à l'hyper-connexion dans le milieu professionnel. Au cours de ce séminaire, il a été rappelé qu'aucune étude officielle sur les TIC et le temps de travail n'existait. Toutefois, certains chiffres ont été énoncés. Ainsi, 75% des cadres disent utiliser les nouvelles technologies pour leur usage professionnel sur leur temps personnel[190]et 68% des cadres estiment que leur charge de travail a augmenté avec le développement des TIC. Par ailleurs, un cadre est interrompu en moyenne toutes les 4 min, en raison des TIC.

Jean-Luc Molins, secrétaire national de l'UGICT-CGT, m'a confié au cours de notre entretien **(cf. annexe n°2)** que « le droit à la déconnexion n'existe pas encore réellement ». Il s'agirait encore d'un droit « en construction » à travers notamment des accords souvent récents qui prévoient certaines dispositions. Ainsi, il est intéressant de souligner que la Poste a très récemment mis en place un accord sur l'égalité Homme/Femme qui consacre un chapitre à la problématique de l'articulation entre la vie personnelle et la vie professionnelle où est instauré le droit à la déconnexion. En outre, il existe également un accord Areva du 31 mai 2012 qui contient la disposition suivante : « chaque salarié veillera à se déconnecter du réseau et à ne pas envoyer de courriel en dehors des heures de travail ». Par ailleurs, le droit à la déconnexion est également reconnu au sein d'un accord « Société générale » du 30 mars 2015[191].

[189] ANONYME « Déconnecter après le travail, l'idée fait son chemin en Allemagne et en France », <Huffingtonpost.fr>, publié le 27 mai 2015
[190] Baromètre UGICT/ Viavoice, cadres et professions techniciennes, mai 2014
[191] RAY (J-E.), « Tous connectés, partout, tout le temps », Droit social, juin 2015, n°6 p.516-527

A défaut d'une intervention législative consacrant le « droit à la déconnexion », nombreuses sont également les entreprises qui se sont pourtant déjà orientées vers une « obligation de déconnexion » de leurs salariés. A cet égard, il apparaît que le secteur automobile est particulièrement actif. Ainsi, j'ai choisi d'illustrer ce propos par quelques exemples d'entreprises allemandes qui ont déjà consacré ce droit pour leurs salariés. Il s'agit notamment de l'entreprise « Volkswagen » qui a mis en place une « trêve quotidienne » de réception d'e-mails sur les téléphones professionnels. Ainsi, les serveurs ne dirigent plus les e-mails après une certaine heure. La société BMW a également pris acte des limites entre vie privée et vie professionnelle. Néanmoins, le porte-parole de la direction a déclaré « ne pas vouloir de règles rigide ». Enfin, le fabricant des automobiles Mercedes-Benz a quant à lui lancé un « assistant d'absence » qui est chargé d'effacer les emails arrivant dans la boîte électronique des salariés qui le souhaitent pendant leur congés. L'émetteur de l'email est prévenu de l'opération et invité à contacter un remplaçant[192].

En France, il est également possible de souligner certaines initiatives notamment celle d'Orange, qui a par exemple en 2013 fait le test « d'une journée sans courriers électroniques ».

Le secteur automobile n'est pas le seul à être particulièrement actif à cet égard, puisqu'il existe aussi une convention de branche du 16 décembre 2014 dans le domaine de l'hôtellerie et de la restauration. Cette convention rappelle que « l'employeur doit rappeler au salarié que le matériel professionnel qui est mis à sa disposition ne doit pas être utilisé en principe pendant des périodes de repos, dans le cadre de l'articulation entre le travail et la vie professionnelle ».

En outre, il est nécessaire de souligner à cet égard l'intervention très active des syndicats. En effet, le 1er avril 2014, un accord a été signé entre les organisations patronales Cinov, la fédération Syntec et la CFDT/CGC. Il s'agissait de la signature d'un avenant à l'accord de 1999 concernant la durée du travail

Cet accord, souvent présenté comme une « grande avancée » introduit une obligation de déconnexion des outils de communication à distance. Cet accord, très attendu prévoit notamment que les cadres doivent déconnecter les accès distants, les mails et les moyens de communication à distance. Par ailleurs, cet accord prévoit aussi que les entreprises doivent

[192] ANONYME « Déconnecter après le travail, l'idée fait son chemin en Allemagne et en France », <Huffingtonpost.fr>, publié le 27 mai 2015

« garantir le droit à la santé, au repos, et à l'articulation entre vie professionnelle et vie privée ».

La réception de cet accord a été plutôt positive en France. A l'étranger, en particulier, outre-manche, l'accord a pu faire l'objet de quelques critiques. Ainsi, les médias anglo-saxon n'ont pas hésité à « rire » de cet accord, en titrant que les « français rendaient le travail après 18h, illégal ». En outre, il est intéressant de souligner que nombreux sont ceux qui considèrent que la problématique de l'hyper-connexion serait réservée aux cadres. Or, il me semble qu'avec le développement du BYOD et du CYOD en entreprise, la problématique est aujourd'hui susceptible de concerner tous les types de salarié. A cet égard, l'exemple da société La poste qui a équipé ses salariés de smartphones peut être cité. En outre, la baisse des prix des outils mobiles et connectés a également contribué à renforcer le taux d'équipement des individus et par conséquent a parfois participer à renforcer l'intensité de la connexion. Le nombre de personnes susceptibles d'être concernées par cette problématique devient de plus en plus important. Par conséquent la question suivante peut se poser : est-il nécessaire dorénavant de légiférer pour prendre en compte ce phénomène et l'encadrer ?

B) Des interrogations sur la pertinence d'une intervention législative

Aujourd'hui, il est possible de faire un parallèle entre d'une part le droit à la déconnexion et d'autre part le droit au repos. En effet, celui-ci est un droit constitutionnel, énoncé au paragraphe 11 du préambule de 1946. Il s'agit également d'une obligation de sécurité de résultat qui incombe à l'employeur. Ce dernier doit s'assurer de l'effectivité de ce droit. La consécration du droit à la « déconnexion » par la voie législative interroge toutefois bien qu'elle puisse apparaître pertinente. En effet, certains allèguent que cela pourrait « une échappatoire ». Nombreux sont ceux qui préconisent plutôt des accords discutés en fonction des conditions de travail, négociés dans l'entreprise qui prévoit sa mise en œuvre. C'est déjà le cas effectivement comme nous l'avons vu dans certaines grandes entreprises. Ainsi, par exemple, 35 entreprises ont signé une charte consacrée au bon usage de l'e-mail.

La « digital detox » semble être devenue un label de conduite et de mieux vivre numérique. Selon Yves Lafargues, consultant et spécialiste des nouvelles technologies de la communication, l'intervention législative ne serait pas pertinente dès lors que les besoins des

salariés sont très divers. Il serait plus opportun selon lui de se limiter à des accords locaux au sein des entreprises.

Par ailleurs, des doutes sur la pertinence d'une intervention législative existent également en Europe. Ainsi, cela permet de souligner que la problématique de l'hyper connexion n'est pas spécifiquement française. Par exemple, pour le grand syndicat d'Europe IG Metall, « les avancées en entreprise sont insuffisantes et il faut légiférer », tandis que selon le syndicat suédois Unionen, il faut faire preuve de plus de souplesse. Ainsi, selon Martin Wastfelt, membre du syndicat, « il serait plus efficace de faire appel à la raison et d'expliquer aux entreprises qu'il est dans leur intérêt de préserver la santé de leur personnel ».[193]

En outre, il apparaît que le « droit à la déconnexion » ne fait pas l'unanimité. Ceux qui y sont réticents dénoncent des difficultés de mise en place, des problèmes techniques et organisationnels.

[193] ANONYME « Déconnecter après le travail, l'idée fait son chemin en Allemagne et en France », Huffingtonpost.fr, 27 mai 2015

Conclusion

La mobilité semble désormais un élément indispensable. C'est pourquoi, les entreprises doivent le prendre en compte. Bien que les dirigeants y soient traditionnellement opposés, la mobilité, comme nous l'avons vu dans le cadre de ce mémoire, s'est imposée par le biais des salariés. Par ailleurs, la mobilité favorise l'entreprise « connectée » ce qui est opportun dans un contexte où les TIC prennent de plus en plus de place. Les problématiques juridiques liées à ces différents types de mobilité sont très nombreuses. Ainsi, en conclusion, l'ultra-mobilité qui est constatée de l'entreprise aujourd'hui semble véritablement nécessiter un encadrement spécifique eu égard à la multiplicité des problématiques, bien qu'un certain nombre de règles puissent déjà s'appliquer en matière par exemple de protection des données personnelles ou bien de propriété intellectuelle. Par ailleurs, face à l'hyper connexion des salariés, les risques pouvant exister sont bien réels et doivent être pris en compte par l'employeur. A défaut, ce dernier prend le risque de voir sa responsabilité engagée. Néanmoins, le salarié n'est pas le seul concerné par ces risques, puisque l'employeur peut également être confronté à de nombreuses problématiques face au BYOD. Il apparaît que certaines d'entre elles sont déjà prises en compte par l'Etat (ex : téléchargement illicite). D'autres, n'ont pas encore été appréhendés par le droit.

Personnellement, un encadrement spécifique me paraît opportun, dès lors que selon moi, les entreprises qui seront confrontées au BYOD ou à d'autres formes de mobilité seront toujours plus nombreuses à l'avenir. Il est très probable qu'un cadre juridique plus précis soit posé dans les prochains mois. En effet, le 19 juin dernier, un rapport du Conseil national du numérique a été remis au Premier Ministre, contenant 70 recommandations s'agissant d'une future loi sur le numérique.

Sur un plan personnel, la rédaction de ce mémoire de fin d'études a été très importante pour moi. Elle m'a apporté énormément. En effet, cela m'a permis de m'intéresser davantage au droit italien, et d'approfondir mes connaissances juridiques sur certaines problématiques existantes également en droit français, du point de vue de ce droit que je ne connaissais pas. Le fait d'être parti à l'étranger pour la réalisation de mon stage de fin d'études pendant la rédaction de ce rapport m'a également beaucoup apporté. En effet, ce séjour m'a énormément ouvert l'esprit et je pense qu'il a contribué à rendre ce mémoire un peu plus riche dès lors que ma problématique concerne aussi bien la France que l'Italie.

BIBLIOGRAPHIE

I- RAPPORTS

▪ RAPPORTS JURIDIQUES

➢ *Rapport français*

Etude annuelle 2014 du Conseil d'Etat, « Le numérique et les droits fondamentaux », Edition La Documentation Française, Etudes et documents, septembre 2014, 446p.

LOIC (H.) et BOUCHOUX (C.), « Loi HADOPI : totem et tabou », rapport d'information n°600 (2011/2015) du 8 juillet 2015 fait au nom de la Commission de la culture, de l'éducation et de la communication, 141p.

➢ *Rapport italien*

Rapport Garante per la protezione dei dati personali , Privacy e lavoro, Le regole per il corretto trattamento dei dati personali dei lavoratori da parte di soggetti pubblici e privati, avril 2015 , 13 p.

▪ RAPPORTS D'ENTREPRISES

➢ *Rapports français*

Rapport d'étude Club EBIOS, *BYOD : Elements de réflexion pour gérer des risques*, sous la direction de M.GRALL Matthieu, responsable des travaux, 11 février 2014, 17p.

Rapport de l'Observatoire de la Responsabilité Sociétale des Entreprises (ORSE), *Du meilleur usage des outils de communication numérique dans les entreprises*, janvier 2015, 78p.

Rapport d'étude, *Les Terminaux personnels en Entreprise – FAQ*, Forum des Compétences, étude menée avec Caprioli&Associés, Société d'avocats, disponible sur <www.forum-competences.com>, 21p.

Rapport d'étude CISCO IBSG Horizons, *BYOD : une perspective mondiale*, 2012, disponible sur www.cisco.com, 21p.

Rapport d'étude EPITA/SOLUCOM, *Comment sécuriser les usages du BYOD ?*

➢ *Rapport italien*

Rapport Cicsco ISBG Horizons,L'impatto finanziaro del BYOD – I ventaggi per le aziende multinazionali, 2013, 26p.

LIVRES BLANCS

Livre blanc Sophos de M. ESCHELBECK Gerhard, *Les risques et avantages du BYOD* , Juillet 2013, disponible sur www.sophos.com, 7p.

Livre blanc Aerohive Networks, *Au-delà du BYOD : comment transformer le BYOD en productivité,* 2012, 14p.

Livre blanc, Cabinet d'avocats Mathias, *Livre blanc BYOD : un défi juridique à anticiper, septembre 2013, 17p.*

Livre blanc IDC, BAHLOUL Karim et BRINDAVOINE Florent, *Télétravail et ultra-mobilité un nouvel environnement de travail pour les salariés, de nouvelles problématiques pour les entreprises,* janvier 2014, 21p.

Livre Blanc Microsoft, GRASSET (J.), Bring Your Own Device, Vision sécurité et approche des solutions, Microsoft France, septembre 2013, 67p.

RAPPORTS ET LETTRES D'INSTITUTIONS

ANACT, INRS, Ministère du travail ; Guide pratique pour prévenir le syndrôme d'épuisement professionnel, 21 mai 2015, 34p.

La lettre innovation et prospective de la CNIL, *Intimité et vie privée du travailleur connecté : BYOD, capteurs, sécurité des données dans l'entreprise numérique*,n°7, juin 2014, 4p.

Rapport de la CNIL, Vie privée à l'horizon 2020, Cahier IP n°1, www.cnil.fr, 60p.

CNIL, Guide pratique pour les employeurs, www.cnil.fr, 52p.

EUROGIP, Risques psychosociaux au travail, une problématique européenne, Janvier 2010, 22p.

II- OUVRAGES

- **OUVRAGES GENERAUX JURIDIQUES**

➢ **Français**

AUZERO (G.) et DOCKES (E.), *Droit du travail*, Dalloz, Précis, 2014, 28 édition, 1556p.

BELIER (G.), *13 paradoxes en droit du travail*, Lamy Axe Droit, 495p.

CHENEDE (O.) et JOURDAN (D.), *Contrat de travail du recrutement à la rupture*, 6e édition, 2005, 335 p.

COEURET (A.), GAURIAU (B), MINE (M.), *Droit du travail*, 2006, Syrey, DALLOZ, 679p.

DUQUESNE (F.), *Droit du travail*, 2014, Lextenso Editions, 4 editions, Gualino, 624p.

MAZEAUD (A.), *Droit du travail*, 9e édition, LGDJ, Lextenso, 680p.

MOULY (J.), *Droit du travail*, 6e edition, Lexifac DROIT, 288p.

PANSIER (F-J.), *Droit du travail*, 6e edition, LexisNexis, 363p.

PIZZIO – DELAPORTE (C.), *Droit du travail*, 2e édition, VUIBERT Droit, 447p.

TOURNAUX (S.), *Droit du travail*, Grand Amphi Droit, 555p

- **Italien**

INDICTALIA, LAVORO, Guide e Soluzion, Ipsoa, 2014, 1220p.

- **OUVRAGES SPECIALISES**

ASSING (D.), CALE (S.), *La sécurité des accès mobiles : au delà du BYOD*, Hermes Science Publications, coll. Management et informatique, septembre 2012, 274p.

BESSEYRE DES HORTS (C-H.), L'entreprise mobile : comprendre l'impact des nouvelles technologies, Pearson, coll.ENTREPRISES/MAN, avril 2008, 201p.

PASSET (M.), VERDEL (C.), NAUGES (L.), *BYOD : réussir son intégration dans l'entreprise*, Ed.ENI, 2014, 218p.

GILMORE (G.) et BEARDMORE (P.), *Sécurité mobile et BYOD pour les nuls*, Kaspersky Lab, John Wiley&Sons, Ltd, 60p.

III- THESES OU MEMOIRES

- **Mémoires**

- *En français*

BARBIER (H.), *Les enjeux de l'encadrement juridique de la géolocalisation*, Aix-Marseille, année 2013-2014, 76p.

BOUCHE (S.), *Droits et libertés du salarié comme limites au pouvoir disciplinaire de l'employeur en droit français et en droit italien*, disponible en ligne sur le site www.juripole.com

MADEROU (T.), Mémoire d'étude, Mémoire de projet sur l'hyper-connexion, Ecole Boulle, 2013, 92p.

MARRAUD (L.), *De la conception d'une plateforme de télétravail virtualisée et unifiée : analyse socio-technique du travail « à distance » équipé*, Business administration . Telecom Paris-Tech, 2012, 327p.

MATIGNON (E.*), La cybercriminalité : un focus dans le monde des télécoms*, Sorbonne, 25 juin 2012, 95p.

OLSEN (M.*), BYOD Sans stress Institut Supérieur d'Electronique de Paris*, 2011-2012, Master management et protection des données personnelles, 96p.

SOLIVERES (A-V.), *Le droit au repos*, Mémoire Master 2, Université Panthéon-Assas, Paris II, 2013, 203p.

VALLOIS (C.), *L'employeur contre les risques psychosociaux, Master 2 Professionnel Droit et Pratique des Relations du Travail*, 2013-2014, 61p.

- *En italien*

LAURI (M.), I limiti del potere di controllo del datore di lavoro, Tesi di Laurea, 109p.

IV- ARTICLES JURIDIQUES

ANONYME, « Qualité de vie au travail : transformer la contrainte en opportunité », *Les Cahiers du DRH 2014*, n°125, 1 décembre 2014, pp.13-21

ADAM (P.), « SMS, vie privée et portable professionnel : histoire (courte) d'un Homme « sans territoire », *Revue Droit du travail Dalloz*, n°3, pp.191-194

AYACHE-REVAH (L.) et AYAD (M.), « Vie privée, vie publique : droit du travail et libertés individuelles », n°345, juin 2013, jurisprudence sociale Lamy, pp.4-7

BARRIERE (C.), « Les SMS envoyés ou reçus par le salarié sur son téléphone professionnel sont présumés professionnels », *La Semaine Juridique Edition générale*, février 2015, n°8, p.373

BARRIERE (F.), « SMS, téléphone professionnel et vie privée du salarié », *La Semaine Juridique Entreprise et Affaires* n°14, 2 avril 2015, pp.56-60

CAPRIOLI (E.), Contrôle de l'employeur des données se trouvant sur l'outil personnel d'un salarié, *CCE*, n°9, septembre 2012, comm.104, pp.43-45

CAPRIOLI (E.), Caractère professionnel d'une clé USB privée connectée à l'ordinateur professionnel, *CCE*, n°5 , mai 2013, comm. 62, pp.50-51

CASANOVA (A.), « Consultation des courriers électroniques et des SMS du salarié : même cause, même combat, même principe aux yeux de la Cour de cassation », *Lamy Droit de l'immatériel*, mai 2015, n°115, p.12-15

COSTES (L.), « Possibilité pour l'employeur de consulter les SMS du mobile de ses salariés », *revue Lamy Droit de l'immatériel*, mars 2015, n°113, p.34
COTTIN (J-B.), MIR (J-M.), « Risques psychosociaux : perspectives internationales », *Les cahiers du DRH*, février 2011, n°173, pp.47-59

CULLAFROZ-JOVER (S.) et LUBET (P.), « La souplesse du droit face à l'usage croissant du BYOD : étude sur la gouvernance des données au sein de l'entreprise connectée », *Revue des « Juristes de Sciences-Po »*, 1 mars 2015

D'HEULLEY (A.), « Utilisation des TIC par les salariés et leurs représentants », *JCP S* (Edition sociale), octobre 2014, n°42, pp.18-22

FUNKE (J-F.), « La pratique du BYOD (Bring Your Own Device), *JCP S* (édition sociale), n°4, janvier 2015, pp.3-5

LANDREAU (I.), « Le téléphone portable : instrument angélique ou diabolique lors d'un usage mixte professionnel et personnel ? », *Revue Lamy Droit de l'immatériel*, n°95, juillet 2013, pp.69-72

MERAV (G.), « Les risques liés au BYOD : quelles mesures prendre en interne ? » *Cahiers de droit de l'entreprise*, n°3, mai 2012, pp. 74-76

MERAV (G.), « La cybersécurité des entreprises », *Cahiers de droit de l'entreprise*, septembre 2014, n°5, pp.62-64

MEURIS (F), « Le salarié connecté », *CCE*, 1er octobre 2014

PANSIER (F-J.), « La clé USB est présumée contenir des fichiers professionnels », *Cahiers sociaux du Barreau de Paris*, mars 2013, n°250, p.78

POGGI (A-S), « Les offres Coud pour entreprises et la protection des données à caractère personnel : les recommandations dont les entreprises doivent tenir compte lorsqu'elles choisissent une offre cloud », *Lamy Droit de l'immatériel*, 1er juillet 2014, n°105, pp.44-56

RAY (J-E.), « Tous connectés, partout, tout le temps », Droit social, juin 2015, n°6 p.516-527

RICCIO (G-M), « La protection de la vie privée : brève analyse de la situation italienne », Lex eletronica, vol. 6, n°2, 2001

SOUVIRA (A.), « La cyber sécurité des entreprises », *Lamy droit de l'immatériel*, 2013

SOUVIRA (A.), La « cyber sécurité des entreprises », *Lamy Droit des affaires*, novembre 2013, n°87, pp.95-99

V- ARTICLES NON JURIDIQUES

ARNAUD (S.), « Analyse économique du droit au respect de la vie personnelle : application à la relation de travail en France ? », *Revue internationale de droit économique*, avril 2007, n°2,

pp.129-156

PRAS (B.), « Entreprise et vie privée », *Revue française de gestion* 5/2012 (N° 224) , p. 87-94

VALLEJO (J-L.), « Digital : chronique d'une mutation du travail », L'expansion Management Review 2/2014 (n°153), pp.120-128

VI- NOTES, OBSERVATIONS, COMMENTAIRES ET CHRONIQUES DE JURISPRUDENCE

BARRIERE (F.), « SMS, téléphone professionnel et vie privée du salarié », *La Semaine Juridique Entreprise et Affaires* n°14, 2 avril 2015, pp.56-60

BOSSU (B.), « Vie privée du salarié, la consultation par l'employeur de la clé USB du salarié », *JCP (S.),* mai 2013

CAPRIOLO (E.), « Condamnation pour vol et abus de confiance d'une ex-salariée ayant transféré des fichiers sur une clé USB », *CCE*, mars 2012, n°3, p.39-42

FROUIN (C.), « L'employeur peut ouvrir la clé USB du salarié connectée à l'ordinateur professionnel », *La gazette du Palais*, mars 2013, n°81-82, p.29-30

LALOT (L.), « Une clé usb connectée à l'ordinateur est présumée utilisée à des fins professionnelles », *revue Lamy droit de l'immatériel*, mars 2013, n°91, p.46-47

LHERNOULD (J-P), « NTIC- les secrets de la clé USB personnelle du salarié accessibles à l'employeur », *Jurisprudence sociale Lamy*, mars 2013, n°340, p.13-14

NORD-WAGNER (M.), « Présomption d'utilisation à des fins professionnelles d'une clé USB connectée à l'outil informatique mis à disposition du salarié par son employeur » , *revue droit du travail* Dalloz, mai 2013, n°5, p.339-340

PANSIER (F-J.), « La clé USB est présumée contenir des fichiers professionnels », *cahiers sociaux du barreau de Paris*, mars 2013, n°250, p.78

VII- TEXTES LEGISLATIFS

➢ EUROPEEN

Proposition de règlement européen sur la protection des données à caractère personnel (COM25(2012)11 final) 25/01/2012

Proposition de directive (COM(2013) 48 final) 07/02/2013

Accord européen sur le stress au travail du 8 octobre 2004

- **FRANCAIS**

Loi du 6 Janvier 1978 Informatiques et libertés

- **Italien**

Loi du 20 mai 1970 n.300 (Statuto dei Lavoratori)

Décret législatif n°81/2008

VIII- JURISPRUDENCE

- **Européenne**

CEDH 16 décembre 1997, n°95-41.326, NIEMETZ C/Allemagne

CEDH 23 septembre 2010, SCHUTH c/Allemagne

- **Française**

TGI

TGI de Versailles du 18 décembre 2007, n°0511965021, L c/Valéo

TGI Clermont-Ferrand, ch.corr., 26 septembre 2011, Société X et Y / Mme Rose

Cour d'appel

CA Bourges, 15 octobre 2010 n°09/01531

CA Paris 28 juin 2011 n°09/09327

CA Paris, 14 mars 2013

CA de Versailles, 5e ch., 31 mars 2011, Société X et Y / Mme Rose

CA Riom, chambre civile, 4e, 12 février 2013, n°11-01.747

Cour de cassation

Cass.Soc.26 février 1991, n°88-44.908

Cass.civ, 16 décembre 1992, n°91-11480

Cass.soc., 16 décembre 1997, n°95-41.326, Delamaere c/ Office notarial Ryssen et Blondel

Cass. 14 mars 2000 n°98-42.090

Cass.soc. 2 octobre 2001 n°99-42.942, Société Nikon

Cass.soc, 22 févier 2002, n°99-18.389

Cass.crim, Nortel, 15 mai 2004

Cass.crim., 9 septembre 2003, 02-87.098

Cass.soc, 17 mai 2005, n° 03-40.017

Cass.crim, 4 mars 2008, n°07-84.002

Cass. soc., 9 juillet 2008, n° 06-45800

Cass. soc.23 mai 2012,n°10-23.521

Cass.crim, 16 novembre 2011, n°10-87.86*4*

Cass.soc., 26 juin 2012, n°11-15.310

Cass.soc. 12 février 2013, n°11-28.649

Cass. 17 févier 2014

Cass. Soc. 29 octobre 2014, Monsieur X. c/Elb Multimédia

Cass. 10 février 2015

Cass.soc., 16 juin 2015, M.X c/Fico Graphie

- **Italienne**

- **Corte di cassazione**

Cassazione civile – 22 dicembre 1956 n.4487 ; Soc.produzione associata Tirrena Asso Film c.Caruso

Cassazione civile- 20 aprile 1963 n.990

Cassazione. 27 maggio 1975 n. 2129

- **Provvedimenti**

Provvedimento juin 2008 [1531604

Provvedimento 7 octobre 2010, [1763071]

Linee guida sul trattamento di dati personali dei lavoratori privati – 23 novembre 2006 [1364939]

Verifica preliminare richiesta da Wind Telecomunicazioni s.p.a, 9 octobre 2014

Verifica preliminare richiesta da Ericsson Telecomunicazioni s.p.a 11 septembre 2014

IX- MULTIMEDIAS

LABBE (P-O.), Reportage « Digital Detox : Comment j'ai vécu 90 jours sans Internet », diffusé le 25 février 2015 sur Canal Plus

X- SOURCES INTERNET

- Françaises

ANONYME, Mobilité, digital et entreprise, la loi des tablettes, publié le 13 novembre 2014, <www.lenouveleconomiste.fr>

ANONYME « Déconnecter après le travail, l'idée fait son chemin en Allemagne et en France », Huffingtonpost.fr, 27 mai 2015

ANONYME, « Le CYOD, première étape vers le BYOD ? », publié le 5 novembre 2014, www.itforbusiness.fr

ANONYME, « Les 10 choses à savoir sur le CYOD », publié le 7 mars 2014, www.eurecia.com

ANONYME, « La technologie n'est pas l'ennemie du bien-être au travail », publié le 8 mars 2012, www.manpowergroup.fr

ACATRINEI- ALDEA (T.), « Le BYOD et le droit : le couple mal assorti », publié en mars 2014, www.connect.ed-diamond.com

BISEUL (X.), « Le droit à la déconnexion peine à s'appliquer », publié le 31 mars 2015, www.pro.01net.com

CALIXTE (L.), « Téléchargement illégal en entreprise : quels risques pour les salariés et pour l'employeur ?, publié en février 2014, <www.challenges.fr>

CASETTA (R.), « Les défis du BYOD en entreprise sont à relever dès maintenant », publié le 10 décembre 2014, www.lesechos.fr

DEDENIS (L.), « Byod et Cyod, Cloud ou encore télétravail : la synchronisation met les données en danger », publié le 21/01/14, www.lesechos.fr

DESJARDINS (C.), « BYOD : Panorama des risques juridiques pour l'entreprise », publié le 1 mars 2013, www.business.lesechosfr

ELYAN (J.), « BYOD : les apps zombies hantent les terminaux mobiles », publié le 29 avril 2015, www.lemondeinformatique.com

EYCHENNE (A.), « Portrait-robot d'un salarié hyper-connecté », publié le 1er mars 2012, <www.lexpress.fr>

FERRAH (R.), « BYOD & Protection des données », publié le 10 octobre 2013, www.village-justice.com

FILIPONE (D.), « CYOD : pourquoi ça va décoller en 2014 », publié le 5 mars 2014, www.journaldunet.com

GERAY (L.), « Choose Your Own Device : le vrai débat pour travailler autrement ? », publié le 5 mars, www.lesechos.fr

LELOU (P.), « La génération Y adepte du BYOD pose des défis de sécurité », publié le 22 juin 2012, www.finyear.com

LEVY-ABEGNOLI (T.), « Terminaux IT personnels (BYOD) : impacts et impératifs pour l'entreprise », publié le 3 mai 2012, www.zdnet.fr

LEVY-ABEGNOLI (T.), « BYOD : les outils de Mobile Device Management, la solution technique ? », publié le 11 juin 2012, www.zdnet.fr

MAGNIEZ (A.), « BYOD : que dit la loi ? », publié le 24 janvier 2013, IT-expert magazine, www .alain-bensoussan.com

PEPIN (G.), « Selon une étude d'IBM, tous les utilisateurs de smartphones sont en danger », publié le 1er avril 2015, disponible sur www.nextinpact.com

POPIHN (P-Y.), « BYOD : Bring Your Own Disaster ? Comment le rêve de toute organisation peut tourner au pire cauchemar », publié le 15 octobre 2014, <www.smart-webzine.com>

RENARD (L.), « L'employeur face au droit d'accès du salarié à ses données informatiques », publié le 20 mai 2015, <www.usine-digitale.fr>

SANYAS (N.), « Mobilité en entreprise : les cas Renaut, Air France et SNCF », publié le 30/01/2015, <www.zdnet.fr>

SANYAS (N.), BYOD : les conseils de la CNIL, publié le 23 mars 2015, www.zdnet.fr

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

SANYAS (N .), « Byod et mobilité : les salariés français mécontents de la politique de leur entreprise », publié le 14 juin 2013, www.zdnet.com

SANYAS (N.), « L'employé, la première faille de sécurité », publié le 25 mai 2015, <www.zdnet.com>

TRUJILLO (E.), « Le BYOD : une réalité , mais jusqu'à quand ? », publié le 12 janvier 2015, www.ideas.microsoft.fr

ZERBIB (R.), « Cybersécurité: le Cloud, talon d'Achille? », publié le 13/01, www.lesechos.fr

- *Italiennes*

ANONYME, « La privacy nei rapporto di lavoro », www.dirittierisposte.it

ANONYME, « BYOD in Italia e all'estero: i nuovi dati Intel », publié le 30 janvier 2015, <www.techeconomy.it>

ANONYME, « Il BYOD fa paura alle aziende italiane », publié le 18 mars 2014, www.corrierecommunicazioni.it

DE SANTIS (F.), « Garante Privacy : Geolocalizzare i dependenti per migliorare la qualità del servizio », www.portolano.it

LUCANTONI (S.), « Controllo sul lavoratore e sulla sua attività »,Treccani.it, 2014

LONGO (A.), « Il BYOD si diffonde senze regole in aziende e PA », Digital4.biz

ODDO (I), « ADAPTability/14 BYOD : la nuova frontiera del lavoro « mobile », publié le 29 mai 2014, www.ilsole24ore.com

MAROSCIA (A.), « Privacy : uso dei dati di geolocalizzazione dei lavoratori », publié le 5 novembre 2014, www.lavoroediritti.com

RAPICAVOLI (R.), « Geolocalizzazione e Privacy : una convivenza possibile », 24 janvier 2015, www.fedaiisf.it

RUSCONI (G.), « Il Byod è sinonimo di produttività. Ma anche una sfida ancora da vincere », publié le 1er novembre 2014,www.ilsole24ore.com

XI- POWERPOINTS

BEDIN (C.), « Rischi psico-sociale per stress da lavoro-correlato » (rappresentanti dei lavoratori per la Sicureza Università degli Studi di Padova), Padova, 22-24 Février 2011

CLUSIF, « Consumération de l'IT la Sécurité de l'information », mai 2012, 11p.

JOLY (C-R.), « CYOD/BYOD : Quels outils pour une gestion maîtrisée de la mobilité en entreprise ? », 14/06/2013, 18p, <www.ulys.net>

ANNEXES

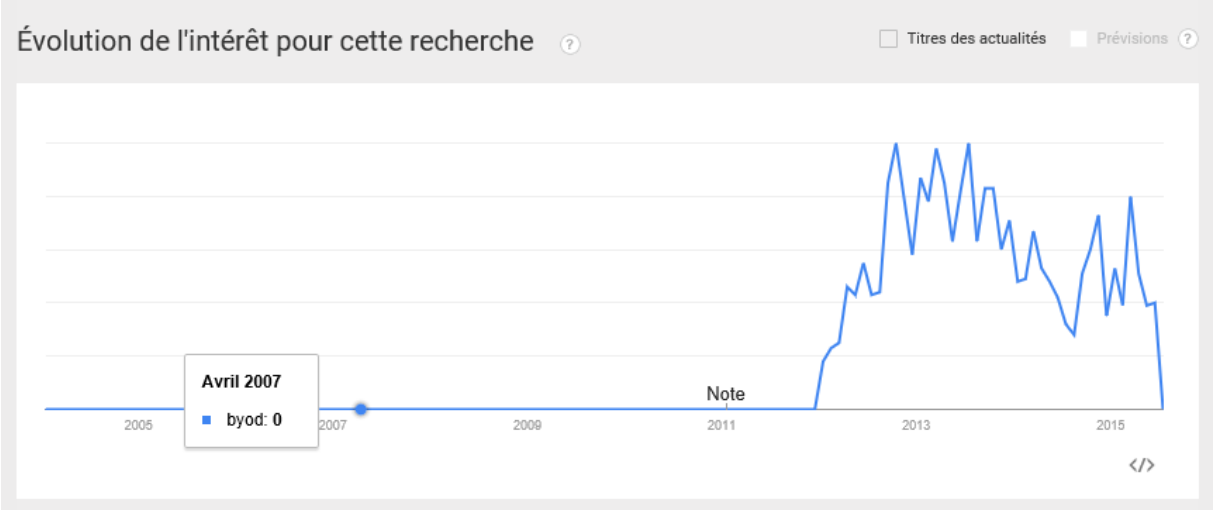
Liste des annexes

Annexe n°1 : Comparaison de l'intérêt porté au BYOD entre la France et l'Italie (GOOGLE TRENDS) réalisée le 6 juillet 2015

Annexe n°2 : Interview de M. Jean-Luc Molins, secrétaire national de l'Union générale des ingénieurs, cadres et techniciens (Ugict-CGT), réalisée le 13/08/2015

Annexe n°3 : Visuels de la campagne « Pour le droit à la déconnexion », Ugict-CGT

Annexe n°1 : Comparaison de l'intérêt porté au BYOD entre la France et l'Italie (GOOGLE TRENDS)



France, au 6 juillet 2015

Italie, au 6 juillet 2015

Annexe n°2 : Interview de M. Jean-Luc Molins, secrétaire national de l'Union générale des ingénieurs, cadres et techniciens (Ugict-CGT), réalisée le 13/08/2015

1) Quelles sont les différentes actions menées par l'Ugict-CGT pour le droit à la déconnexion ?

Depuis septembre 2014, la cgt-UGICT a lancé une campagne très importante « pour le droit à la déconnexion et la réduction effective du temps de travail ». Nous dénonçons principalement l'hyper-connexion et l'infobésité dans le milieu professionnel. Nous sommes particulièrement actifs pour nos engagements. En septembre 2014, nous avons également interpelé le comité national de lutte contre la fraude afin de demander une étude pour chiffrer le nombre d'heures de travail réalisées par des salariés en dehors de leur lieu de travail.

2) Quel regard portez-vous sur l'accord « Syntec » ?

Cet accord marque une avancée certes, mais il reste encore beaucoup à faire. Par ailleurs, je tiens à rappeler que nous sommes parvenus à obtenir la condamnation de la France à de nombreuses reprises en raison du non-respect de la charte européenne des droits sociaux sur le respect de temps de repos et de la préservation de la santé des salariés. Toutefois, nous avons d'autres objectifs en vue.

3) Quels peuvent être les obstacles rencontrés et les difficultés constatées dans la mise en œuvre de ce droit ?

Le droit à la déconnexion n'existe pas encore réellement. Il est en phase de « construction » à travers notamment des accords qui sont plutôt récents et qui prévoient déjà certaines dispositions.

4) Quels sont les différents apports pour les salariés liés à la déconnexion ?

Le principal apport selon nous est de pouvoir bénéficier d'un meilleur équilibre entre la vie privée et la vie professionnelle ainsi que d'une meilleure qualité de vie au travail. Une étude réalisée par l'ugict-CGT en avril 2015 confirme mes propos. En effet, selon cette étude, les 3 priorités des cadres sont : le salaire, le bien-être et l'équilibre entre vie personnelle et vie professionnelle.

5) Quel bilan pour le droit à la déconnexion aujourd'hui ?

Nous sommes très satisfaits de l'accueil réservé à notre campagne

depuis près d'un an. Depuis le lancement du 4 septembre 2014 de notre campagne, nous sommes en phase de déploiement terrain avec des résultats très encourageants, un taux de réponse important et une meilleure prise en compte de nos propositions. Nous sommes optimistes pour la suite.

Annexe n°3: Visuels de la campagne « Pour le droit à la déconnexion » menée par l'Ugict-CGT

Source : http://ugict.cgt.fr/deconnexion/category/visuels/

Table des matières

REMERCIEMENTS 1
TABLE DES ABREVIATIONS 2
SOMMAIRE 3
INTRODUCTION 4
PARTIE 1. 15
LA MISE EN PLACE DE TERMINAUX MOBILES ET CONNECTÉS DANS LE MILIEU PROFESSIONNEL : UN CHOIX À HAUTS RISQUES POUR L'EMPLOYEUR FACE AUX ENJEUX JURIDIQUES 15
Chapitre I. La remise en cause de la classification et de la sécurité des données personnelles et professionnelles 16
Section I. La problématique de la porosité des données personnelles et professionnelles 17
§1 - La porosité croissante des données personnelles et professionnelles par l'utilisation d'un terminal privé à des fins professionnelles 17
A) Les données personnelles 17
1) L'identification des données 18
2) Les obligations de l'employeur et les droits des salariés 19

a) Les obligations de l'employeur 19
b) Les droits des salariés 22
B) Les données professionnelles 24
§2 – La porosité limitée de la frontière entre données personnelles et professionnelles par la mise en œuvre de solutions techniques 26
A) L'émergence de nouvelles politiques de mobilité et les solutions techniques : des alternatives pertinentes pour la protection et la distinction des données 27
B) L'opportunité de la mise en place de mesures techniques face au Cloud 28
Section 2. La problématique de la sécurité et de la confidentialité des données personnelles et professionnelles 30
§ 1 – Les risques internes à l'entreprise 31
A) L'origine non-intentionnelle du risque : la négligence ou la maladresse 31
1) L'identification des risques 31
2) Un comportement, objet de sanctions 33
B) L'origine intentionnelle du risque : la malveillance interne, entre cyber criminalité et cyber vengeance 34
1) L'identification des risques 34
2) Les sanctions à l'égard du salarié 35
§2- Les risques externes à l'entreprise 36
A) L'identification des risques 37
B) Les obligations en vue de la prévention des risques 37
Chapitre 2. L'atteinte aux droits de propriété intellectuelle du fait de l'usage illicite d'un terminal 38
Section 1. Les usages en termes de propriété littéraire et artistique 39
§1 - Le téléchargement illicite 39
A) L'augmentation des risques en matière de respect des droits de propriété intellectuelle des tiers 40
1) Le téléchargement illicite en entreprise en France 40
2) Focus sur la situation du téléchargement illicite en Italie 41
B) Les risques en matière de responsabilité 43
§2 - La problématique annexe relative à la propriété de la création réalisée sur un terminal connecté 45
A) Le rappel des principes généraux 45
B) La problématique soulevée par le BYOD 46
Section 2. Les usages illicites en matière de logiciel 47
§1- La problématique de la gestion des licences de logiciel 47
§2- Des solutions potentielles pour la gestion des licences de logiciels 49

PARTIE 2. 50

LA MISE EN PLACE DE TERMINAUX MOBILES ET CONNECTÉS DANS LE MILIEU PROFESSIONNEL : LA NÉCÉSSITÉ D'UN ENCADREMENT JURIDIQUE FACE À UNE POLITIQUE A RISQUES POUR LE SALARIÉ 50

Chapitre 1. Vers une dangereuse réduction de la frontière entre les sphères personnelle et professionnelle 51

Section 1. Le risque d'atteintes à la vie privée accru par la mise en place de terminaux mobiles et connectés 52

§1 - Le droit à la vie privée du salarié consacré 52

A) L'affirmation du droit à la vie privée 53

1) En France 53

2) En Italie 57

B) La mobilité, facteur potentiel de risque pour l'effectivité des libertés du salarié 59

§2- Le droit à la vie personnelle du salarié limité par le pouvoir de contrôle de l'employeur 60

A) Le pouvoir de contrôle de l'employeur 60

1) Le pouvoir de contrôle de l'employeur en droit français à travers les textes 60

2) Le pouvoir de contrôle de l'employeur en droit italien 62

B) Le pouvoir de contrôle de l'employeur au cœur de jurisprudences récentes en France 63

1) Les prémisses d'un pouvoir de contrôle sur les terminaux connectés personnels à travers le contrôle de la clé USB 63

2) L'affirmation du pouvoir de contrôle de l'employeur sur les SMS professionnels 66

Section 2. Le risque d'atteintes à la vie privée renforcée par la cybersurveillance et la géolocalisation intensive 68

§1 - Les principes généraux relatifs à l'utilisation des nouvelles technologies par l'employeur à des fins de surveillance dans l'intérêt de la protection du salarié en droit français 68

A) L'encadrement de la géolocalisation par les textes en droit français 68

B) La CNIL, autorité garante de l'application des principes 69

§2- Les principes généraux relatifs à la géolocalisation des salariés en droit italien 70

A) L'encadrement de la « géolocalisation » par les textes en Italie 70

B) Le garant pour la Privacy, gardien de l'application des principes en Italie 72

Chapitre 2. Vers une consécration opportune d'un droit à la déconnexion face aux risques liés à l'exigence d'hyper productivité et à l'usage intensif du numérique 74

Section 1. L'appréhension des risques psychosociaux 75

§1 – Le salarié, sujet de risques et de troubles psychosociaux 76

A) L'identification des risques et des troubles psychosociaux 76

B) La reconnaissance progressive des risques et des troubles psychosociaux 77

1) L'appréhension internationale des risques psychosociaux 78

2) L'appréhension française des risques psychosociaux 79
3) L'appréhension italienne des risques psychosociaux 80
§2 – L'employeur, acteur de la protection contre ces risques 81
A) L'obligation de sécurité à la charge de l'employeur en France 81
B) L'obligation de sécurité à la charge de l'employeur en Italie 81
Section 2. La pertinence de la déconnexion : une utopie face à l'hyper-connexion, « mal du siècle » 82
§1 – L'émergence de l'idée d'un droit à la déconnexion 82
A) De la multi-connexion à l'hyper-connexion 82
1) Le droit au repos : un hypothétique précédent au droit à la déconnexion 82
2) La problématique de l'hyper-connexion 83
B) La déconnexion face à l'usage intensif des TIC : une tendance en hausse 85
§2 – L'effectivité du droit à la déconnexion 87
A) Une revendication dans le milieu professionnel 87
B) Des interrogations sur la pertinence d'une intervention législative 90
Conclusion 92
BIBLIOGRAPHIE 93
I- RAPPORTS 93
II- OUVRAGES 94
III- THESES OU MEMOIRES 95
IV- ARTICLES JURIDIQUES 96
V- ARTICLES NON JURIDIQUES 97
VI- NOTES, OBSERVATIONS, COMMENTAIRES ET CHRONIQUES DE JURISPRUDENCE 98
VII- TEXTES LEGISLATIFS 98
VIII- JURISPRUDENCE 99
IX- MULTIMEDIAS 101
X- SOURCES INTERNET 101
XI- POWERPOINTS 103
ANNEXES 104
Table des matières 108