Droit social 2021 p.139

Les objets connectés au travail : quelles régulations pour quels enjeux ?

Isabelle Desbarats, Professeur, CDA (Centre de droit des affaires), université Toulouse Capitole, Toulouse, France

L'essentiel

Alors que l'usage d'emplois connectés se développe dans l'entreprise, à l'initiative des salariés mais aussi des employeurs, la question se pose de savoir, non seulement comment réguler l'usage de ces dispositifs, mais également de qui dépend une telle régulation (pouvoirs publics et/ou acteurs privés). Les enjeux sont importants : en effet, si les objets connectés offrent de nombreux avantages, leur usage est également facteur de risques.

Qu'est-ce qu'un objet connecté ? « Un objet connecté est un appareil électronique sans fil communicant. Il récolte et stocke des informations, en émet, interagit avec d'autres appareils (*smartphone*, ordinateur, autre objet connecté, serveur, etc.). Il peut recevoir et transmettre des instructions. Pour ce faire, il est équipé de capteurs [...] connectés à Internet par des réseaux longues portées (Lora ou Sigfox), moyennes portées (Wi-Fi) ou courtes portées (Bluetooth, ...). Toutes les informations qu'il va collecter sont transmises à une plateforme de traitement des données (*data centers*). Elles vont pouvoir être analysées et exploitées en temps réel et sans discontinuité »(1).

Les objets connectés sont donc des « équipements qui incluent à la fois des capteurs capables d'enregistrer divers phénomènes [...] liés à l'utilisateur (déplacement, mouvement, postures, son, [...] conversations) et des mécanismes de transmission d'échange de données vers des bases de données ou vers d'autres objets connectés qui permettent de réaliser des traitements et activités algorithmiques de ces données [...] »(2). Ce faisant, « liée naturellement à Internet, la notion d'objet connecté est également indissociable [des] algorithmes [...] utilisés pour le traitement des données produites, [de] l'intelligence artificielle, [des] données produites contribuant à l'apprentissage des systèmes, [du] *big data*, [...] »(3).

Des milliards d'objets connectés et une diversité d'applications. Aujourd'hui, c'est un développement sans précédent de ces objets connectés qui s'opère, tant sur le plan quantitatif qu'au regard de leurs usages. Explosion de leur circulation d'abord, encore que les chiffres avancés varient : « 20 milliards d'objets connectés en 2017 et 75 milliards avant 2025. [...]. Le volume annoncé des données générées par l'IoT est tout aussi impressionnant : [il doublerait] tous les deux ans et [devrait dépasser] les 40 000 milliards de giga-octets [en] 2020 dans le monde »(4). On souligne que le phénomène est difficile à évaluer précisément en raison de la distinction « rarement claire entre les objets industriels et les *"wearables"* pour le grand public (montres, bracelets connectés, objets domestiques...) »(5) avec, néanmoins, une certitude : le fait que le passage vers le réseau 5G devrait renforcer le déploiement de ces objets à l'ère de l'industrie 4.0, présentée comme la quatrième révolution industrielle, après celles de la mécanisation, de la production de masse et de l'automatisation. Quant à la diversité d'usage des objets connectés, elle est tout aussi exponentielle que leur quantité, que ces usages concernent la vie privée des individus ou le fonctionnement des organisations. C'est ainsi que, sous le premier angle, des objets connectés existent dans de nombreux domaines, tels

que la domotique(6), le sport, le bien-être et la santé, les activités de loisirs : « Les premiers objets connectés de loisirs étaient des bracelets ou de petits capteurs de type podomètre [...] », puis « sont venus les montres connectées et les objets liés à l'habitat [ainsi que] de nouveaux jeux et accessoires interactifs (gants, bracelets) qui proposent des activités mêlant le réel et le virtuel »(7). Pour l'heure, sont cependant prédominants « les objets connectés « de santé » (dits de *quantified self* : montres, balances, [...], bracelets, *smartphones*), [qui] permettent de collecter les données de santé de leurs utilisateurs (rythme cardiaque, tension...) ou en lien avec leur santé (mesures des efforts physiques, comptage des pas effectués...) »(8).

Quant aux opportunités offertes aux entreprises, elles sont multiples puisque les objets connectés peuvent contribuer à une réduction des coûts de production et de logistique via une optimisation de la gestion des stocks ; à un perfectionnement des processus organisationnels et opérationnels des entreprises ; ou bien encore à une amélioration de la relation client, grâce à des offres personnalisées s'appuyant sur le traitement de données comportementales(9).

Plus précisément encore, sous l'angle du travail, on observe un recours croissant, bien que variable selon les secteurs d'activité, à de multiples objets connectés, tels que les badges ou bracelets communicants ; les dispositifs d'alarme pour travailleur isolé (DATI) ; les vestes, gilets, casques ou chaussures de sécurité (avec capteurs de pression pour évaluer le poids des éléments portés) ; les lunettes de protection intégrant une caméra ; les coussins vibrant en cas de mauvaise posture... : tous objets en capacité de communiquer avec leur environnement, qui sont « équipés de capteurs ou d'une puce [leur permettant] de transcender [leurs usages initiaux] pour proposer de nouveaux services »(10), qui utilisent l'infrastructure d'Internet et qui transmettent des informations à des serveurs. Point notable : si, d'un côté, ce sont les entreprises qui peuvent décider de recourir à ce matériel électronique, singulièrement dans le champ de la santé/sécurité au travail mais pas exclusivement(11), ce sont, d'un autre, les salariés eux-mêmes qui peuvent introduire leurs équipements en milieu de travail (bracelets, montres, cigarettes électroniques, etc.).

Or c'est d'une certaine ambivalence dont témoignent ces dispositifs électroniques dès lors que, s'ils « recèlent [des] potentialités opportunes, ils engendrent aussi des risques professionnels nouveaux plus difficiles à appréhender dont la gestion est complexe et encore incertaine... »(12) (I). Voilà pourquoi se pose la question de savoir, non seulement comment réguler l'usage de ces dispositifs, mais également de qui dépend une telle régulation : pouvoirs publics et/ou acteurs privés (II).

I. - Les objets connectés en milieu de travail : une pratique ambivalente

A priori, le recours, par le salarié, à des objets connectés personnels peut être qualifié de « vieille question neuve », si on le met en miroir avec l'utilisation, toujours par le salarié, de ses propres outils informatiques à des fins professionnelles : cette pratique dite BYOD (pour *bring your own device*, c'est-à-dire « apportez vos appareils personnels »), consistant pour « les propriétaires de *smartphones*, de tablettes ou [...] d'ordinateurs portables, [à apporter et à utiliser] leurs appareils personnels sur leurs lieux de travail »(13).

Cela étant, l'emploi d'objets connectés au travail génère de nouvelles problématiques parce que cet usage n'est pas seulement le fait du salarié mais également celui de l'employeur, ce qui rend la pratique ambivalente. En effet, si, d'un côté, le recours à des objets connectés, qu'ils soient personnels ou pas aux salariés, peut être source de risques pour l'entreprise et/ou les droits et libertés salariales (A), il peut, d'un autre, présenter des avantages, que ces objets soient, ici encore, la propriété du salarié ou celle de son employeur (B) : il en résulte un usage complexe de ces objets dont la régulation se révèle délicate.

A - Les objets connectés : facteurs de risques pour l'entreprise et/ou les droits et libertés des salariés

C'est d'un triple point de vue que l'usage d'objets connectés en milieu de travail peut être source de risques, tant pour

les droits et libertés salariaux que pour la sécurité informatique de l'organisation(14). Plus précisément, si, d'une part, c'est l'utilisation, par le salarié, de ses propres objets connectés qui peut léser les droits d'autrui ainsi que la sécurité de son entreprise, c'est, d'autre part, le recours patronal à de tels objets qui peut menacer les droits et libertés des salariés.

Menaces pour les droits d'autrui. En premier lieu, c'est aux droits et libertés d'autrui que l'utilisation d'objets connectés personnels peut nuire, ce qui conduit à s'interroger sur la teneur d'une éventuelle réplique patronale. Ainsi, et alors que « certains objets connectés peuvent être ressentis comme une [...] une agression par d'autres salariés à l'occasion de la vie en collectivité (lunettes connectées enregistrant des propos ou images d'autres salariés sans leur autorisation préalable) »(15), un employeur peut-il faire cesser cette situation, au besoin en sanctionnant, voire en rompant le contrat du salarié récalcitrant ? Certes, devrait s'appliquer le principe selon lequel nul ne peut être sanctionné pour un fait relevant de la vie privée, ici le port d'un objet personnel (lunettes...). À une condition cependant : le fait qu'aucun trouble caractérisé n'en résulte au sein de l'entreprise, auquel cas un licenciement personnel non fautif serait envisageable(16).

Menaces pour la cybersécurité. En deuxième lieu, c'est à l'intérêt même de l'entreprise que le recours à de tels objets peut nuire de deux points de vue distincts(17). Le premier est lié au fait que « le port ou l'utilisation d'équipements [sont] susceptibles d'attenter à la confidentialité [du] patrimoine informationnel [de l'entreprise] (montres avec micros, lunettes avec dispositifs d'enregistrement) »(18), ce qui soulève la question d'une éventuelle interdiction patronale de l'usage de tels dispositifs : le fait est que « l'IOT [constitue] un point noir en matière de cybersécurité (dès lors) qu'il existe [...] du matériel de qualité extrêmement diverse, dont une frange est peu sécurisée et représente une porte d'entrée facile vers les réseaux »(19). Certes, il est vrai qu'ici encore, pourrait être opposé l'article L. 1121-1 du code du travail selon lequel « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ». Mais le secret des affaires, la protection d'informations confidentielles ne pourraient-ils pas être invoqués par un employeur craignant que des objets appartenant au salarié y portent atteinte(20) ? À ce stade toutefois, on relève qu'un employeur ne saurait recourir à des solutions à ce point drastiques qu'elles sont en sont prohibées : ainsi, « l'article L. 33-3-1 du code des postes et communications électroniques (CPCE) [semble lui interdire de] mettre en place un dispositif de filtrage ou de brouillage des objets connectés des salariés, y compris dans certaines pièces spécifiques »(21).

Par ailleurs, c'est à un autre égard que l'intérêt de l'entreprise peut se trouver affecté par l'utilisation salariale d'objets connectés : tel peut être le cas en présence d'une demande d'interconnexion de ces objets avec le système d'information de l'entreprise. À la question de savoir si le salarié dispose du droit de s'interconnecter à ce système, une réponse négative semble cependant s'imposer. La raison en est qu'« en vertu de la maîtrise de l'employeur sur son système d'information et de la sécurité qu'il doit y assurer [...], il est libre d'accepter ou de refuser les pratiques de BYOCL conduisant à l'interaction avec [ce] système. Que ce soit pour une montre ou des lunettes connectées, un *smartphone* ou une tablette, le principe est clair : le salarié ne dispose pas d'un droit acquis à s'interconnecter au système d'information de son employeur »(22). « Si dans cette hypothèse, [celui-ci] acceptait l'interconnexion, il pourrait imposer des conditions d'accès strictes au système [...], à charge pour lui d'éviter toute discrimination dans les autorisations accordées »(23). Soulignons en outre qu'à supposer possible une telle interconnexion, il faudrait en tirer toutes les conséquences, s'agissant de la nature personnelle ou professionnelle de l'objet connecté : en effet, « à partir du moment où un équipement de communication est connecté au système d'information de l'employeur, il est présumé être utilisé à titre professionnel », ce dont il ressort que l'employeur peut en « contrôler le fonctionnement ou le contenu »(24).

Menaces pour les droits et libertés. Cela étant si, d'un côté, c'est l'utilisation, par le salarié, de ses objets connectés qui peut nuire soit aux droits de ses collègues, soit à la sécurité de la structure, on ne saurait occulter, d'un autre, les risques liés à une « surveillance connectée » du travail, eu égard aux atteintes potentielles aux droits et libertés ainsi

contrôlés et notamment au respect de la vie privée(25). Le fait est que, si les entreprises peuvent recourir aux objets connectés dans le champ de la santé/sécurité au travail, le risque est qu'ils soient également utilisés à des fins de surveillance incontrôlée. C'est ainsi qu'au coeur de potentielles « dérives », on trouve le risque que les informations collectées soient utilisées à des « fins d'évaluation professionnelle », y compris « pour surveiller la vie émotionnelle des employés [et pour y adapter les] décisions managériales »(26). Sans doute, l'enjeu est un renforcement de la productivité et de la performance des salariés, via le recours à des logiciels munis d'algorithmes, des balises GPS, des puces électroniques(27), des objets connectés et autres badges sociométriques permettant, non seulement l'enregistrement des déplacements et la durée des temps de pause, mais également le ton ou la fréquence des conversations, voire le langage corporel : des objectifs qui, s'ils peuvent se justifier par le souci de réduire « les incidents client », renouvellent cependant la question des modalités de la surveillance numérique au travail, à laquelle l'accord national interprofessionnel (ANI) du 26 novembre 2020 pour une mise en oeuvre réussie du télétravail vient d'apporter sa contribution. Celui-ci rappelle en effet que, non seulement tout moyen de contrôle de l'activité du salarié et du temps de travail doit être justifié par la nature de la tâche à accomplir et proportionné au but recherché, mais que la mise en place de dispositifs numériques spécifiques nécessite, outre l'éventuel contrôle de la Commission nationale de l'informatique et des libertés (CNIL), le respect de deux conditions cumulatives : la consultation préalable du comité social et économique (CSE) et l'information préalable des salariés.

Incontestablement, l'utilisation d'objets connectés en milieu de travail peut donc constituer un facteur de risque, tant pour l'entreprise que pour les droits et libertés des salariés, qu'ils soient leur propriété ou celle de leur employeur. Preuve de leur ambivalence, ces objets peuvent, cependant, constituer simultanément des outils utiles, singulièrement dans le champ de la prévention des risques professionnels, voire de l'amélioration du bien-être au travail.

B - L'objet connecté : un allié potentiel dans la prévention des risques professionnels

Une diversité d'avantages. S'il est une question centrale, c'est celle relative aux multiples intérêts liés à l'usage d'objets connectés, lesquels recouvrent un large spectre : rationalisation et rentabilisation du temps de travail ; enjeux de géolocalisation et d'optimisation des espaces(28) ; mais, également, objectifs de réduction de la pénibilité au travail, de prévention des risques professionnels, voire d'amélioration du bien-être et de la qualité de vie au travail, via une surveillance des données vitales des travailleurs, une détection des environnements de travail dangereux ou l'instauration d'espaces de travail et de services « connectés » (identification automatique, déverrouillage de l'ordinateur, déclenchement du photocopieur...). Ainsi, certains objets permettent de mesurer et d'adapter automatiquement les paramètres de travail (humidité, température, lumière, bruit, vibrations), via l'édiction de rapports destinés à les améliorer(29). D'autres objets (robot français Numii) ambitionnent de mesurer la pénibilité au travail, en détectant, prévenant, réduisant les troubles « musculo-squelettiques », en numérisant l'espace de travail et la posture des salariés(30). D'autres encore (vêtements ou bracelets connectés) permettent de vérifier les constantes vitales (pouls, pression artérielle...) du travailleur confronté à des contraintes physiques importantes.

Ce faisant, on comprend pourquoi les objets connectés peuvent être perçus comme des alliés dans la réduction de la pénibilité professionnelle et la prévention des risques au travail puisque, en résumé, ils peuvent être utilisés « pour surveiller les constantes physiques et physiologiques des travailleurs, contrôler l'environnement du travail et s'assurer que les conditions de sécurité sont respectées. [Ils] peuvent [également] [...] transmettre un signal d'alarme si [l']utilisateur est en danger [...] »(31).

D'une obligation salariale d'utiliser des objets connectés de santé ? Pour autant et si l'on conçoit l'intérêt qu'un employeur peut avoir de requérir d'un salarié qu'il utilise ce type de dispositifs, est-il en droit de l'exiger ? Et, dans ce cas, « pourrait-il obtenir un accès aux données produites par [les salariés], quand celles-ci concernent non plus leurs performances professionnelles mais leur bien-être au travail, pour ne pas dire leur santé »(32) ?

S'agissant du premier point, la réponse réside, comme précédemment, dans l'article L. 1121-1 du code du travail, ce qui conduit à se demander si l'usage d'un objet connecté à la demande patronale peut relever soit d'impératifs d'hygiène et de sécurité, soit de l'intérêt de l'entreprise, qui sont les deux justifications généralement admises par les juges. Or tel devrait être le cas selon certains. « Par exemple, si un bracelet connecté permet de prévenir en temps réel un malaise ou un accident du travail, ce pourrait être un impératif de sécurité pour le salarié d'en porter un. Quant à l'intérêt de l'entreprise, il pourrait éventuellement être invoqué en ce que l'usage d'objets connectés améliorerait à la fois les performances et l'image de l'entreprise »(33). À ce stade, se pose cependant cette question : « la responsabilité [de l'employeur] pourrait-elle être engagée s'il s'avérait [...] que ces objets ont des conséquences négatives sur la santé des salariés »(34) ? Alors que l'employeur souhaitait imposer le port de ces objets au nom de son obligation de sécurité, pourrait-il ultérieurement se voir reprocher sa violation ? Alors que l'on « ne connaît pas [...] l'impact des ondes émises par les objets connectés sur le corps de leur utilisateur », « les problématiques relatives à l'amiante pourraient resurgir », dans le cas où « le port d'objets connectés [se révélerait] nocif pour la santé des salariés » : en effet, « qui [serait] responsable ? Comment indemniser les salariés affectés qui se [seraient] vu proposer le port d'objets connectés par leur employeur, le médecin du travail [voire] leur assurance »(35) ?

Quant à la question de savoir si, en cas de port d'un objet connecté, l'employeur peut avoir accès aux données produites par les salariés, notamment celles relatives à leur santé, elle renvoie à la problématique du traitement des données ainsi recueillies : une problématique qui est celle des conditions et modalités d'un usage raisonné des objets connectés en milieu de travail.

II. - D'un usage raisonné des objets connectés en milieu de travail. Comment ? Par qui ?

Outre ceux précédemment évoqués, plusieurs risques semblent liés à l'usage d'objets connectés en environnement de travail : « Fuite de données personnelles et exploitation abusive [...], crainte [...] d'atteinte à la vie privée, [inquiétude] sur la surveillance [...] de la présence [...] à seule fin d'accroitre la productivité. [En outre], l'utilisation possible d'objets connectés implantés [...] sous la peau [...] [accroît] les problèmes éthiques [...], avec le sentiment de dépossession partielle de soi et d'espionnage permanent »(36). Deux risques suscitent plus précisément l'attention. Le premier est relatif à « la gestion des données [...], sachant que, dès qu'un objet connecté est associé à l'identité de la personne qui le porte, les données deviennent personnelles »(37). Le second est celui d'un usage - abusif (?) - d'objets connectés pour contrôler comportements et performances des salariés, au risque d'une atteinte à leur vie privée et de comportements discriminatoires à raison de l'état de santé.

Certes, des garde-fous d'ores et déjà instaurés par le législateur peuvent contribuer à un cantonnement de ces risques. Cependant, aucune réglementation spécifique n'encadrant le recours aux objets connectés en environnement de travail, la question se pose de savoir de quelle façon une régulation du numérique par les chartes (B) est susceptible de compléter les prémices d'un encadrement juridique (A).

A - L'apport public : les prémices d'une régulation juridique du numérique

Alors que l'usage d‘objets connectés au travail constitue une pratique ambivalente, c'est de deux façons complémentaires que l'action publique tente de limiter les risques encourus, avec des effets cependant perfectibles. Le premier levier est celui de la protection des données issues des objets connectés. Le second est celui contribuant à une préservation de la vie privée du salarié, même si le « droit à la déconnexion » qui peut y participer a été plus largement instauré pour réduire les effets négatifs du recours aux technologies de l'information et de la communication (TIC) et non des seuls objets connectés.

Les données issues des objets connectés : quelle protection ? Alors, on l'a vu, qu'un employeur peut souhaiter

confier un objet connecté à ses salariés afin de réduire pénibilité et risques professionnels, les données issues de ces objets peuvent-elles, pour cette raison, être qualifiées de données « de santé » ?

L'enjeu est important puisqu'un régime protecteur(38) est appliqué à celles-ci, en raison de leur caractère « sensible » au sens de l'article 9 du règlement général sur la protection des données (RGPD). Or tout porte à croire que l'assimilation des données personnelles issues des objets connectés à des données de santé ne va pas de soi, au motif que celles-ci ne peuvent être ainsi qualifiées qu'« au cas par cas, compte tenu de la nature des données recueillies ». Plus précisément, trois types de données relèvent de cette catégorie, selon la CNIL : « celles qui sont des données de santé par nature : antécédents médicaux, maladies, [...] ; celles qui, du fait de leur croisement avec d'autres données, deviennent des données de santé [car permettant] de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne : croisement d'une mesure de poids avec d'autres données (nombre de pas, mesure des apports caloriques...), [...] ; celles qui deviennent des données de santé en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite au plan médical »(39).

Dans ces conditions, l'enjeu est de savoir si les données recueillies en dehors d'un contexte médical (nombre de pas, poids, activité quotidienne...), par des outils de mesure de soi (montres, bracelets connectés, applications mobiles...), peuvent être, ou pas, qualifiées de données de santé : une question à laquelle la CNIL répond de façon nuancée. Pour elle, en effet, ne peuvent pas être ainsi qualifiées « celles à partir desquelles aucune conséquence ne peut être tirée au regard de l'état de santé de la personne concernée (par ex. une application collectant un nombre de pas [...] sans croisement de ces données avec d'autres) »(40). « [Tout] dépend [donc], d'une part, de la nature des données [...], d'autre part, du croisement ou non de ces données [avec] d'autres données révélant ainsi des informations sur l'état de santé de la personne »(41).

Conséquences ? Ce n'est qu'à la condition d'être qualifiées de « données de santé » que celles issues des objets connectés seront soumises au régime juridique instauré pour protéger ce type de données sensibles ; en revanche, ne seront pas concernées les données dites « de bien-être », celles-ci se différenciant de celles-là en fonction, non pas seulement de « la nature de la donnée collectée mais [de] la finalité qui en est faite »(42).

À la question de savoir si la réglementation issue du RGPD protège efficacement les salariés dont les données sont collectées par le biais d'un objet connecté, une réponse nuancée s'impose donc. Certes, le traitement de ces données - personnelles, parce que se rapportant à une personne physique identifiée ou identifiable, directement ou non, grâce à un identifiant ou à un ou plusieurs éléments propres à son identité(43) - est soumis aux dispositions destinées à protéger la vie privée et les libertés individuelles(44) : d'un côté, dispositifs protecteurs des droits des personnes (consentement renforcé et transparence ; droit à la portabilité des données ; droit à l'oubli ; droit à notification ; droit à réparation du dommage matériel ou moral) ; de l'autre, obligations imposées aux entreprises (obligation générale de sécurité, de confidentialité et d'information ; analyse d'impact en cas de risque élevé pour les droits et libertés des personnes ; délégué à la protection des données). En revanche, le régime juridique particulier des données « sensibles »(45) - et les obligations y afférentes imposées à l'employeur en tant que « responsable du traitement »(46) - ne s'appliqueront qu'aux données qualifiées « de santé », en raison de la « valeur » qu'elles représentent désormais(47) : une qualification qui ne s'impose donc pas, puisque concurrencée par celle de données de « bien-être ».

Cela étant, la protection des données ne constitue pas le seul levier actionnable pour gérer les risques générés par l'usage d'objets connectés en milieu de travail : le respect du droit à la déconnexion en constitue un second dont la portée semble cependant circonscrite comme celle du premier.

Objets connectés *vs* droit à la déconnexion. À la question de savoir si le droit à la déconnexion peut constituer un outil de régulation de l'utilisation d'objets connectés en milieu de travail et, plus précisément, de protection de la vie privée des salariés, une réponse prudente s'impose. Certes, rien ne devrait s'opposer à ce que ce droit, « initialement

pensé pour les envois de *mails* (et/ou appels) tardifs ou pendant les jours de congé des salariés », puisse également « avoir pour conséquence d'interdire à l'employeur de demander à ses salariés de garder leurs objets connectés en dehors de leur temps de travail »(48). Mais, comme on l'a souligné, non seulement, il n'en existe pas une définition explicite(49), mais « ce "droit à la déconnexion" ne semble pas pleinement consacré. Le législateur n'a mis à la charge des employeurs qu'une obligation de négociation sur les modalités de sa mise en oeuvre, [...] qui, de plus, ne concerne que les entreprises employant au moins cinquante salariés »(50). Peut-être, cependant, l'ANI du 26 novembre 2020 pour une mise en oeuvre réussie du télétravail va-t-il favoriser une explicitation de ce droit puisqu'il rappelle que « le droit à la déconnexion a pour objectif le respect des temps de repos et de congé ainsi que la vie personnelle et familiale du salarié. C'est le droit pour tout salarié de ne pas être connecté à un outil numérique professionnel en dehors de son temps de travail ». Rien de certain cependant en raison de l'absence de portée contraignante de cet accord.

À ce stade, une question se pose alors : la régulation juridique de l'utilisation d'objets connectés en milieu de travail se révélant imparfaite, qu'attendre d'une régulation par les acteurs privés ?

B - La part patronale. Vers une régulation du numérique par les chartes ?

Synthétisées par la Direction générale de la sécurité intérieure (DGSI)(51) « suite aux nombreuses actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes », « les vulnérabilités induites par l'utilisation d'objets connectés en milieu professionnel », qui sont générées par leur connexion à Internet, sont multiples : risques de captation des données de l'entreprise par une entreprise intermédiaire proposant « de stocker, d'analyser et de gérer en temps réel les données issues des capteurs industriels connectés » ; « équipements électroniques des entreprises utilisés comme porte d'entrée des hackers » parce que présentant des « failles de sécurité » ; prise de contrôle à distance des capteurs des objets connectés détenus par des salariés « préalablement ciblé[s] d'une entreprise sensible, [afin de] donner accès à certaines de ses informations stratégiques ».

Si l'on trouve alors - parmi les différentes préconisations formulées par la DGSI pour minimiser les risques créés par les objets connectés -, des actions de « sensibilisation des salariés aux vulnérabilités liées [à ces objets] », on trouve également l'invitation à « encadrer [leur usage] dans une charte de bonnes pratiques ». Il s'agit, au premier chef, de la charte dite informatique pouvant éventuellement compléter une charte relative au droit à la déconnexion : deux outils de régulation dont le développement est d'actualité, en raison du recours croissant aux objets connectés.

Tel est d'abord le cas de la charte définissant les modalités d'exercice du droit à la déconnexion et la mise en place, par l'entreprise, de dispositifs de régulation de l'utilisation des outils numériques, qui doit être adoptée par l'employeur après avis du CSE, à défaut d'accord conclu dans le cadre de de la négociation annuelle sur l'égalité professionnelle entre les femmes et les hommes et la qualité de vie au travail prévue à l'article L. 2242-17, alinéa 7, du code du travail. En effet, si, pour l'heure, le droit à la déconnexion peut être qualifié de « droit mou »(52) pour les raisons précédemment évoquées, peut-être la crise sanitaire déclenchée par la Covid-19, qui a pour effet de faire du télétravail la norme et le travail sur site l'exception(53), va-t-elle mettre sous les feux des projecteurs ce droit à la déconnexion et la nécessité de mieux l'organiser. Selon certains, les moyens de le faire sont « facile[s] tant du point de vue technique (outils asynchrones, bloqueurs de notifications, etc.), qu'humain, en désignant un référent pour son application de façon durable »(54). Quant aux raisons d'y procéder, elles sont, selon les mêmes auteurs, impératives puisque, « en l'absence de tels aménagements, la seule possibilité [...] pour un salarié de déconnecter réellement et durablement, en dehors des congés payés ou des RTT, est l'arrêt maladie ou le droit de retrait, lorsqu'il est déjà trop tard »(55). Nul doute qu'une clarification du droit de se déconnecter bénéficierait alors aux salariés utilisant des objets connectés et que l'outil pertinent pour le faire est l'élaboration d'une charte sur le droit à la déconnexion, dont l'importance est rappelée par l'ANI précité du 26 novembre 2020. Le fait est, cependant, que cet ANI ne va guère au-

delà de ce simple rappel et qu'il ne semble finalement constituer qu'un « guide de bonnes pratiques », nullement contraignant.

Quant aux chartes dites « informatiques », elles sont celles définissant les conditions générales « d'utilisation du système informatique d'une entreprise (matériel, réseaux, communications) par toute personne ayant accès ou recours à ce système informatique, qu'il s'agisse des salariés, des dirigeants, mais aussi des prestataires, fournisseurs, visiteurs ou stagiaires »(56), un double objectif étant plus précisément poursuivi : d'un côté, la protection du salarié (via son information sur les modalités de surveillance électronique) ; d'un autre, celle de l'organisation, grâce à une anticipation de « pratiques à risque en matière d'accès, par les salariés, à l'Internet, de l'usage des réseaux sociaux, des appareils mobiles et, singulièrement, des objets connectés »(57).

Utile, une telle charte informatique est-elle cependant opposable aux utilisateurs - notamment salariés - et juridiquement contraignante ? La réponse à ces deux questions liées dépend de l'intégration de la charte dans le contrat de travail ou de son annexion au règlement intérieur, cette seconde option étant recommandée lorsque la charte prévoit des sanctions disciplinaires. Encore faut-il que le règlement ainsi modifié fasse l'objet des mêmes formalités que lors de son élaboration, de telle sorte que la charte informatique ainsi intégrée puisse acquérir sa nature juridique. Si tel est le cas, jugé que constitue une faute - éventuellement grave - la violation de règles de sécurité d'une charte informatique(58).

À la question de savoir si une régulation par les chartes peut utilement compléter les mécanismes juridiques permettant de rationaliser, d'ores et déjà, l'utilisation d'objets connectés en milieu de travail, une réponse positive semble ainsi s'imposer, l'adoption d'une charte informatique présentant un autre avantage : celui de permettre aux responsables de traitement - employeurs au premier chef - de démontrer qu'ils ont mis en oeuvre les mesures nécessaires destinées à assurer la sécurité des traitements et donc identifié, évalué, et encadré les risques en matière de protection des données personnelles, conformément au principe d'*accountability* prévu par le RGPD. Nul doute que l'élaboration d'une charte dite « éthique » peut également y contribuer, à l'heure où l'éthique est perçue comme un outil de régulation majeur de l'intelligence artificielle(59).

Mots clés :
ENTREPRISE * Intelligence artificielle * Usages et régulation * Objet connecté * Encadrement juridique * Enjeux

(1) L. Georges, Les objets connectés, quelles opportunités et intérêts pour les entreprises, ideematic.com, 20 déc. 2018. Plus précisément, « on distingue [...] deux grands groupes d'objets connectés : [ceux] destinés à la collecte et l'analyse de données, dont la mission principale est de collecter et transmettre des informations ; [ceux] qui répondent à une logique de contrôle-commande et permettent de déclencher une action à distance. Les capteurs installés sur ces objets connectés sont plus ou moins intelligents, selon qu'ils intègrent ou non eux-mêmes des algorithmes d'analyse de données, et qu'ils soient pour certains auto-adaptatifs » (Définitions autour des objets connectés, www.smartgrids-cre.fr/index.php?p=objets-connectes-definition).

(2) Les objets connectés, INRS, avr. 2018.

(3) *Ibid.* V., M.-F. Mazars et W. El Boujemaoui, Algorithmes, une utilisation à l'épreuve du droit de la protection des données personnelles, *in* P. Adam, M. Le Friant et Y. Tarasewicz (dir.), Intelligence artificielle, gestion algorithmique du personnel et droit du travail, Les travaux de l'AFDT, Dalloz, 2020. 163 s.

(4) IoT : des déploiements dans tous les secteurs (ou presque), www.silicon.fr, 25 mai 2018.

(5) *Ibid.*

(6) Surveillance et commande du chauffage, des caméras, des volets, ampoules ou thermostats connectés, via une application sur téléphone.

(7) Objets connectés : n'oubliez pas de les sécuriser !, CNIL, 4 déc. 2017.

(8) R. Martinière, Les droits des salariés confrontés aux objets connectés de santé, E. Brosset, S. Gambardella et G. Nicolas (dir.), La santé connectée et « son » droit, approches de droit européen et de droit français, PUAM, 2017. V. CNIL, Le corps, nouvel objet connecté. Du *quantified-self* à la m-santé : les nouveaux territoires de la mise en donnée du monde, Cahier Innovation & Prospective, mai 2014. Exemple significatif de l'irruption de nouvelles technologies « persuasives » : le Pavlok, au nom évocateur, qui est un bracelet chargé d'envoyer un petit choc électrique à l'utilisateur en cas de comportement « déviant » - c'est bien sûr ce dernier qui choisit dans quelles situations activer le bracelet (se lever à une heure précise, ne pas rester trop longtemps assis, etc.) et quelle puissance électrique leur associer. Comme l'indique le concepteur de ce bracelet : « Avec Pavlok, nous pouvons enfin devenir la personne que nous avons toujours su que nous pourrions être » (rapport d'information déposé en application de l'article 145 du règlement par la commission des affaires économiques sur les objets connectés et présenté par M^{mes} C. Erhel et L. de la Raudi[#1104]re, 10 janv. 2017).

(9) L. Georges, préc.

(10) Définitions autour des objets connectés, préc.

(11) Des objets connectés peuvent être utilisés pour personnaliser la relation client (dans le secteur ferroviaire, dans le secteur bancaire...).

(12) Objets connectés portables et santé et sécurité du travail, Officiel prévention, juill. 2018.

(13) L. Le Moine, Intimité et vie privée du travailleur connecté : BYOD, capteurs, sécurité des données dans l'entreprise numérique, La lettre innovation et prospective de la CNIL, n° 7, juin 2014.

(14) Objets connectés : les risques à connaître, DGCCRF, nov. 2019.

(15) F. Coupez et F. La Pinta, Les *data* issues des objets connectés du salarié, objets de convoitise ?, https://blogatipic-avocat.com, 23 avr. 2015.

(16) Soc., 16 sept. 2009, n° 08-41.837.

(17) A. Le Denn, Les réseaux informatiques des entreprises sont fragilisés par les objets connectés de leurs employés, www.usine-digitale.fr, 27 févr. 2020.

(18) F. Coupez et F. La Pinta, préc.

(19) A. Le Denn, préc.

(20) « Les logiciels embarqués dans ces objets [connectés] peuvent contenir des vulnérabilités, ou présenter des défauts de configuration permettant d'en prendre le contrôle. Si ces objets sont connectés directement sur Internet, ils peuvent représenter des cibles faciles pour des attaquants qui pourront les utiliser [...] comme vecteur d'attaque ». (M. Untersinger, La sécurité des objets connectés en question après une violente attaque informatique, Le Monde, 25 oct. 2016).

(21) F. Coupez et F. La Pinta, préc.

(22) F. Coupez et F. La Pinta, préc.

(23) *Ibid.*

(24) F. Coupez et F. La Pinta, préc.

(25) E. Perez, Intimité et vie privée du travailleur connecté : BYOD, capteurs, sécurité des données dans l'entreprise numérique, CNIL, Innovation et prospective, n° 7, juin 2014.

(26) A. André, L'objet connecté en entreprise : un ami qui vous veut du bien ?, www.chefdentreprise.com, 31 juill. 2019.

(27) Permettant aux porteurs « d'ouvrir les portes, de se connecter à leurs ordinateurs, d'utiliser la photocopieuse ou de payer à la cantine sans utiliser leurs mains, juste en tendant le bras ». Ces entreprises qui implantent des puces électroniques dans leurs salariés, www.capital.fr, juill. 2017.

(28) Une société belge équipe certains employés de puces électroniques, Le Figaro Économie, 7 févr. 2017.

(29) La prévention des risques grâce aux objets connectés, www.sstrn.fr, 28 févr. 2019.

(30) Numii, l'objet connecté qui révolutionne la santé au travail, https://up-magazine.info, 7 déc. 2017.

(31) Objets connectés portables et santé et sécurité du travail, Officiel prévention, juill. 2018. V., P-Y Verkindt, Ambivalences et promesses de l'intelligence artificielle dans le champ de la santé et de la sécurité des travailleurs, *in* Intelligence artificielle, gestion algorithmique du personnel et droit du travail, Les travaux de l'AFDT, *op. cit.*, 2020. 199 s.

(32) F. Coupez et F. La Pinta, préc.

(33) « Objets connectés du quotidien utilisés en entreprise » : risques opérationnels et environnement juridique, Forum des compétences, p. 36.

(34) *Ibid.*

(35) R. Martinière, préc. V., M. del Sol, Enjeux juridiques des objets connectés en matière d'assurance santé. Réflexions à partir et au-delà du cadre français, 3e colloque de l'Association Information & management (AIM), Rapprochons les communautés TI francophone, mai 2018, Montréal, Canada.

(36) Objets connectés portables et santé et sécurité du travail, Officiel prévention, juill. 2018.

(37) Objets connectés au travail : révolution ou surveillance ?, http://resources.grouperandstad.fr, juill. 2018.

(38) CNIL, Qu'est-ce qu'une donnée de santé ? RGPD, loi informatique et libertés, dispositions relatives aux conditions d'échange et de partage des données de santé (CPS, art. L. 1110-4), dispositions relatives aux référentiels de sécurité et d'interopérabilité (CSP, art. L. 1110-4-1), dispositions sur l'hébergement des données de santé dès qu'il existe un enregistrement et une conservation des données par un prestataire entrant dans le champ de l'hébergement des données de santé (CSP, art. L. 1111-8), interdiction de procéder à une cession ou à une exploitation commerciale des données de santé (CSP, art. L. 1111-8, art. L. 4113-7), etc. V. Applications mobiles en santé et protection des données personnelles : Les questions à se poser, CNIL, 17 août 2018.

(39) CNIL, Qu'est-ce qu'une donnée de santé ?, préc.

(40) *Ibid.*

(41) *Ibid.*

(42) Le traitement des données de santé, www.eurasante.com, févr. 2018, p. 5.

(43) RGPD, art. 4.

(44) Sur l'ensemble, v. Obligations en matière de protection des données personnelles (www.service-public.fr/professionnels-entreprises/vosdroits/F24270).

(45) Donnée sensible, CNIL (www.cnil.fr/fr/definition/donnee-sensible).

(46) Au sens de l'article 4 du RGPD.

(47) L. Belot, Les données de santé, un trésor mondialement convoité, Le Monde, 2 mars 2020.

(48) R. Martinière, préc.

(49) T. Dailler L'émergence du droit à la déconnexion en droit du travail, LPA, 1er mars 2017. 6.

(50) R. Martinière, préc. V. aussi C. Mathieu, M.-M. Péretié et A. Picault, Le droit à la déconnexion : une chimère ?, RDT 2016. 592.

(51) Les dangers de l'utilisation des objets connectés en milieu professionnel, www.otre.org, 6 févr. 2019.

(52) C. Willmann, La déconnexion des salariés : un droit « mou » aux forts enjeux, Dalloz IP/IT 2019. 684.

(53) Protocole sanitaire du 29 oct. 2020.

(54) T. Champey, Au regard des dispositifs mis en place pour le télétravail, refuser le droit à la déconnexion serait une faute pour l'entreprise, tribune, Le Monde, 25 nov. 2020.

(55) T. Champey, préc.

(56) Y. Cohen-Hadria, Charte informatique : peut-on l'annexer au règlement intérieur ?, www.ych-avocats.fr, 20 juill.

2015.

(57) *Ibid*. Plus largement, v. P Lubet et Scullafroz-Jover, La souplesse du droit face à l'usage croissant du BYOD : étude sur la gouvernance des données au sein de l'entreprise connectée, Cabinet Altana, 18 mars 2015.

(58) Soc., 5 juill. 2011, n° 10-14.685.

(59) CNIL, Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, Synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique, déc. 2017.

Copyright 2024 - Dalloz – Tous droits réservés