EDITIONS LEGISLATIVES
actuEL RH
Le quotidien des professionnels des ressources humaines

La dématérialisation du travail. Appréhender les risques et les opportunités

02/01/2018

Angéline Dufour, avocate associée, et Anna Milleret-Godet, avocate au sein du cabinet Cohen & Gresser LLP analysent les enjeux du numérique dans la relation de travail et les questions de sécurité informatique qui en découlent.

Le numérique fait intégralement partie de notre vie tant privée que professionnelle. Les salariés peuvent désormais travailler partout et sont joignables à tout moment grâce à leurs smartphones, tablettes, ordinateurs portables et autres objets connectés.

Une nouvelle manière de travailler est née, plébiscitée par les générations X et Y, également appelées "digital natives" qui virtualisent leur rapport au monde du travail. Se sont ainsi développés de nouveaux modes de communication au sein de l'entreprise. L'email est ringardisé au profit d'outils tels que Skype, Slack ou encore WhatsApp et le Wifi est désormais disponible dans la plupart des lieux publics (lounges d'aéroport, gares, taxis, restaurants, etc.), permettant notamment aux salariés de rester connectés à tout instant. En outre, les salariés utilisent de plus en plus leur propre équipement numérique, les BYOD ("Bring Your Own Devices"), dans le cadre de leur activité professionnelle.

Les récentes réformes emboîtent le pas à ces changements. La loi n°2016-1321 du 7 octobre 2016 dite loi numérique aborde des sujets tels que l'open data et la portabilité des données. La loi n°2016-1088 du 8 août 2016 dite loi Travail introduit officiellement le droit à la déconnexion dans le code du travail. Plus récemment, l'ordonnance n° 2017-1387 du 22 septembre 2017 relative à la prévisibilité et la sécurisation des

relations de travail, favorise le recours au télétravail et donc l'utilisation des outils numériques "nomades" par les salariés.

L'omniprésence du numérique dans le cadre du travail fait cependant peser sur l'entreprise des risques non négligeables.

Les enjeux de cette évolution

Le rapport au travail change et l'utilisation des outils de communication avec lui. Ainsi, l'utilisation à des fins professionnelles par le salarié de son équipement personnel est souvent souhaitée par ce dernier par simple commodité. Pour l'employeur, cela représente des coûts en moins et un certain gage de productivité.

Pour autant les BYOD sont dans la ligne de mire de la cybercriminalité puisqu'ils sont très souvent à l'origine de la première faille de sécurité dans le réseau d'une entreprise, se traduisant notamment par des attaques de Malwares *(1),* Ransomwares *(2)* ou encore des fuites ou pertes de données sensibles (relatives aux salariés, aux clients, au secret des affaires ou de fabrication d'une entreprise, etc.). En effet, l'employeur n'a aucune maîtrise sur les BYOD qui ne sont souvent pas sécurisés comme peuvent l'être les outils professionnels mis à disposition par l'employeur.

En outre, ils favorisent l'hyperconnectivité des salariés, ce qui peut malmener l'équilibre entre vie privée et vie professionnelle et accroître les risques psychosociaux (burn-out, "harcèlement numérique", etc.) d'autant plus qu'il est très difficile de contrôler parfaitement la durée du travail des salariés lorsqu'ils se connectent à distance.

Il s'agit également d'un véritable casse-tête pour l'employeur qui souhaite contrôler l'activité de ses salariés. En effet, depuis l'arrêt Nikon*,* la Cour de cassation a posé le principe selon lequel les contenus créés par le salarié à l'aide d'outils de travail mis à disposition de l'employeur sont présumés professionnels et l'employeur peut y accéder librement, sauf lorsque le salarié les a identifiés comme étant "privés" ou "personnels". Or, les BYOD sont par nature personnels et contiennent des données privées. Ils échappent ainsi au contrôle de l'employeur qui ne saurait y accéder librement. C'est notamment ce que la Cour de cassation a considéré à l'égard d'un dictaphone personnel utilisé par une salariée pour enregistrer des conversations professionnelles*.* Toutefois, dès lors que l'outil personnel est relié aux sources informatiques de l'entreprise, l'employeur peut de nouveau y accéder librement*.* L'employeur peut même se prévaloir d'emails figurant sur la messagerie personnelle du salarié dès lors qu'ils sont intégrés sur le disque dur de l'ordinateur professionnel mis à disposition au salarié*.*

Les bonnes pratiques pour limiter les risques

Les menaces susvisées visent toute utilisation d'outils de communication qu'ils soient mis à disposition par l'employeur ou dans le cadre des BYOD, sauf que ces derniers sont plus exposés et augmentent ainsi la vraisemblance de ces risques. Cependant, il

semble toutefois vain d'interdire totalement aux salariés d'utiliser leurs outils personnels dans le cadre du travail. L'employeur doit plutôt encadrer leur utilisation afin d'en réduire les risques.

Tout d'abord, la mise en place d'une charte informatique est essentielle pour informer les salariés des risques et les inviter à adopter un comportement conforme à la politique informatique de l'entreprise en leur demandant par exemple de mettre à jour régulièrement les logiciels et antivirus sur leur BYOD ou de ne pas télécharger certaines applications. La mise en place de règles simples, claires et peu contraignantes incitera les salariés à les respecter.

Des actions de formation, notamment auprès des managers peuvent en complément s'avérer pertinentes, afin de responsabiliser les salariés dans le cadre de l'utilisation des outils informatiques.

D'autres moyens, plus techniques, peuvent aussi être mis en œuvre tels que le MAM ("Mobile Application Management") qui permettent de faire coexister des données personnelles et professionnelles sur un outil personnel, sans compromettre la sécurité des données de l'entreprise ni entraver la vie privée du salarié, en cloisonnant les données professionnelles à une application sécurisée à laquelle le salarié n'a accès que via cette application.

Par ailleurs, le télétravail ayant vocation à se démocratiser dans les années à venir, il est également important d'encadrer ce nouveau mode de travail. A cet égard, les changements introduits dans l'ordonnance Macron relative à la prévisibilité et la sécurisation des relations de travail par les députés lors de l'examen du projet de loi de ratification, permettraient le recours au télétravail de manière durable, en dehors de tout accord collectif ou document unilatéral le prévoyant. Il est toutefois selon nous impensable de ne pas encadrer le télétravail, le cas échéant à travers un avenant au contrat de travail.

Et demain ?

Se prémunir contre la cybercriminalité grandissante et assurer la protection des données professionnelles et personnelles de ses clients, salariés, etc. sont les véritables préoccupations de demain pour les entreprises, de tout secteur d'activité et de toute taille.

Un rapport Fortinet en date du 31 mars 2017 *(3)* souligne les défis auxquels devront faire face les entreprises, compte tenu de l'augmentation des attaques cybercriminelles qui évoluent aussi vite que la technologie, les objets connectés étant des cibles privilégiées de ces attaques et une voie royale pour pénétrer un système informatique. Les entreprises doivent donc se doter des dernières technologies de sécurité et inciter leurs salariés à adopter un comportement responsable dans le cadre de l'utilisation des outils de communication au travail.

En outre, le règlement européen n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (dit "RGPD" ou "GDPR" en anglais) qui entrera en vigueur le 25 mai 2018, va sensiblement modifier le rôle des entreprises concernant le traitement des données personnelles qu'elles sont amenées à traiter. Le responsable du traitement des données, en l'occurrence l'employeur, devra assurer un niveau de sécurité accru des données personnelles qu'il traite. Parmi les mesures obligatoires dès le mois de mai prochain, une procédure de notification des failles de sécurité devra être mise en place en cas de perte ou de fuite de données personnelles *(4)*. Concrètement si l'ordinateur ou le portable d'un salarié contenant des données personnelles relatives aux salariés ou aux clients de l'entreprise par exemple, venait à lui être volé, celui-ci devra en avertir immédiatement sa hiérarchie et le responsable du traitement sera tenu de notifier l'incident à la Cnil dans les meilleurs délais et si possible 72 heures au plus tard après en avoir pris connaissance.

En outre, certaines entreprises, devront se doter d'un DPO ("Data Protection Officer" ancien "CIL" Correspondant Informatique et Liberté) chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'entreprise. La désignation d'un DPO est selon nous vivement conseillé, même si celle-ci n'est pas obligatoire.

La dématérialisation du travail ne doit être crainte. Au contraire, il s'agit ici d'une véritable opportunité pour repenser le rapport au travail des nouvelles générations qui ne veulent plus travailler comme avant. Cette évolution doit toutefois être mesurée et accompagnée par l'employeur qui devra en appréhender les risques, afin d'y apporter des solutions concrètes et satisfaisantes tant pour les salariés que pour l'entreprise.

[1] Programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté ;

[2] Logiciel informatique malveillant, prenant en otage les données. Le ransomware chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer ;

[3] Rapport Fortinet du 31 mars 2017 sur les principales menaces se penche sur l'émergence d'armées d'objets connectés malveillants, une évolution qui ouvre de nouvelles perspectives en matière de cybersécurité.

[4] Article 33 du RGDP.

Angéline Dufour et Anna Milleret-Godet
