LIBERTE ET SECURITE

La liberté d'un salarié doit-elle s'arrêter là où la sécurité des données numériques commence ?

MBA - Management de la Sécurité des Données Numériques

Intervenant

Monsieur Gérard PELIKS
gerard.peliks@noos.fr

Bernadette LEROY

Rapport du 25/11/2015

INSTITUT LÉONARD DE VINCI

Bernadette LEROY

Liberté et sécurité

La liberté d'un salarié doit-elle s'arrêter là où la sécurité des données numériques commence ?

Un peuple prêt à sacrifier un peu de liberté pour un peu de sécurité ne mérite ni l'une ni l'autre, et finit par perdre les deux." Cette fameuse phrase de Thomas Jefferson, philosophe et président des Etats-Unis du XIXème siècle, prend tout son sens lorsque l'on parle coexistence vitale, mais au combien difficile, de la liberté et de la sécurité.

Dès lors, nous pouvons comprendre la complexité pour tout chef d'entreprises d'assurer et de garantir les libertés des collaborateurs tout en assurant la sécurité des biens, matériels et immatériels, et des personnes. Comment concilier deux valeurs aussi antagoniques mais dont la complémentarité n'est plus à prouver. Le sujet « liberté et sécurité » est un sujet d'actualité qui fait débat mais qui n'a pas réellement abouti à un consensus. En effet, les notions de liberté et de sécurité sont ambivalentes, car pour qu'une personne puisse jouir de sa liberté, elle a besoin de sécurité, qui implique aussi un recul de la liberté.
Il ne peut y avoir de liberté sans sécurité !

Tocqueville définit la liberté comme étant à la fois une absence d'oppression et une liberté individuelle. Elle reflète à la fois l'absence de contrainte, la possibilité d'agir, de penser, de s'exprimer selon son souhait et sans être entravé par le pouvoir d'un autre. La Déclaration des Droits de l'Homme et du Citoyen de 1789 précise que « *La liberté consiste à pouvoir faire ce qui ne nuit pas à autrui* ». La maxime des lumières qui dit « *La liberté des uns s'arrête là où commence celle des autres* » vient compléter cette approche.

En quoi la sécurité est-elle une composante essentielle de la liberté ?

Quel que soit sa taille ou son secteur d'activité, la sécurité est un sujet fondamental pour une entreprise. Il est un fait notoire qu'en cas de faute d'un collaborateur la responsabilité civile et pénale de l'employeur est recherchée car ses fonctions de direction dont il est investi fondent sa responsabilité. Sur le plan pénal, les poursuites visent à faire sanctionner les atteintes protégées par le Code du travail et par le Code pénal en ce qui concerne la vie et l'intégrité physique d'autrui. La responsabilité pèse ici au premier plan sur le chef d'entreprise dans la

mesure où il est tenu de veiller personnellement à l'application des règles destinées à protéger la santé et la sécurité des travailleurs placés sous son autorité. Ce n'est pas pour autant, et on le verra plus loin, que l'employé n'est pas exempt de poursuite pénale dans certain cas. Dans le domaine spécifique du numérique, lorsqu'un collaborateur commet une infraction, la responsabilité de l'employeur est alors recherchée et c'est à l'employeur de réparer les dommages causés par son collaborateur. L'employeur peut se dégager de cette responsabilité s'il arrive à prouver que son collaborateur est l'auteur d'un « abus de fonctions », ce qui est difficile.

Dans ce contexte, la sécurité est la situation dans laquelle quelqu'un ou quelque chose n'est exposé à aucun danger, à aucun risque d'agression, d'accident, de vol, de détérioration, etc. Le collaborateur doit pouvoir s'épanouir au sein de l'entreprise et ceci en toute tranquillité et confiance. Assurer la sécurité des collaborateurs implique la mise en place de règlements qui permettront d'encadrer l'utilisation des outils et moyens de communication. Les agissements des collaborateurs sur internet peuvent engendrer des risques majeurs pour les employeurs. La sécurité est l'affaire de tous, reviens à dire qu'elle n'est l'affaire de personne : la sécurité est l'affaire de chacun et chaque jour. Ainsi, le chef d'entreprise est tenu de mettre en place des outils de prévention des risques en matière de protection des systèmes d'information. Il faut que chaque collaborateur se sente concerné par la problématique des menaces qui pèsent sur l'entreprise sans pour autant bunkeriser l'entreprise. Il faut prendre conscience des risques et faire en sorte d'avoir les bons réflexes et surtout les bonnes pratiques afin de minimaliser le niveau des risques. Ainsi, l'entreprise doit être capable de faire face aux menaces en un minimum de temps. Si la sensibilisation des collaborateurs est alors indispensable, la mise en place de contrôles et de restrictions dans une optique de sécurisation est aussi nécessaire. Et c'est là que certains vivront cette surveillance comme une atteinte aux libertés individuelles, alors que d'autres n'y verront qu'un moyen de protéger les intérêts collectifs.

Projecteur sur le numérique dans les entreprises et les risques qui lui sont liés.

Aujourd'hui, les réseaux de communications électroniques et les systèmes d'information convergent et sont de plus en plus interconnectés. Ils font partie de notre quotidien et sont indispensables au bon fonctionnement de très nombreuses entreprises et institutions. Le développement et l'utilisation du numérique dans le monde de l'entreprise représentent un maillon faible dans la chaine sécuritaire, spécialement pour les TPE et les PME qui n'ont pas toujours les moyens d'employer un responsable de la sécurité des systèmes d'information (RSSI) ou sont souvent peu sensibiliser à ce sujet. Si la révolution ~~d'~~internet a permis à des millions de personnes d'accéder à une source presque inépuisable d'informations et de données, il n'en reste pas moins l'un des outils à l'origine d'une nouvelle forme de délinquance. Le développement des nombreux usages et fonctionnalités du web a engendré des menaces inquiétantes car celles-ci sont protéiformes, elles ne connaissent pas de frontières et demeurent très souvent anonymes, tout en pouvant s'actualiser à tout moment. Par conséquent, l'univers virtuel a offert aux criminels de nouveaux territoires de conquête. Il leur a permis d'élargir leur horizon

tout en développant de nouveaux types de délits. Ce panel peut aller du vol de matériels ou de logiciels, au piratage les plus ingénieux, en passant par le rançonnage, le hameçonnage ou encore la fraude. Aucune entreprise n'est à l'abri de la cybercriminalité. Et, un détournement de l'internet à usage professionnel à des fins personnelles peut devenir critique pour une entreprise qui en aurait sous-estimé l'impact. L'utilisation des réseaux sociaux par exemple, augmente le risque de social engineering. Le social engineering (ou ingénierie sociale) est une technique qui a pour but d'obtenir d'une personne un bien ou une information stratégique sans qu'elle ne s'en rende compte. Il s'agit donc d'exploiter les failles humaines et sociales de la structure cible. La fraude aux baux, la fraude au Président ou encore l'usurpation des moyens de communication sont des exemples de fraudes par ingénierie sociale.

Pensons aussi au cyberterrorisme. Que se passerait-il si des groupes terroristes accédaient aux réseaux d'information de sociétés des secteurs du transport, de l'énergie ou de la finance ? Il pourrait y avoir de graves incidents, nous pourrions être privé d'électricité, de communication ou ne plus avoir accès à nos comptes bancaires. En tout état de cause, le profit demeure la première motivation des cybercriminels et internet offre des opportunités très fortes de passer à l'acte. Il est important de rappeler que les attaques peuvent provenir de l'intérieur comme de l'extérieur. Qu'il s'agisse de malveillance, de maladresse, d'inconscience ou de naïveté certaines études montrent que l'erreur humaine est à la base de 98% des problèmes de sécurité informatique. Si l'homme est le maillon fort de toute entreprise, il en est aussi le maillon faible. Qu'il s'agisse de maladresse, d'inconscience, de négligence ou de malveillance, c'est bien l'homme qui se trouve devant l'écran. Internet est donc un outil idéal pour des employés sans scrupules qui l'utilisent à des fins personnelles. En agissant ainsi, ils exposent l'entreprise à des attaques potentielles. En mettant en péril l'entreprise, ils menacent de surcroit l'ensemble des collaborateurs qui y travail. Mais une attaque, qu'elle soit interne ou externe, peut aller bien plus loin. Prenons le cas récent d'Orange qui a été victime en 2014 de deux piratages de grande ~~d~~'ampleur. En plus des pertes financières engendrées par ces attaques, les données personnelles de plusieurs millions de clients ont été volées, devenant ainsi des cibles d'escroquerie et de phishing. La définition de la liberté de La Déclaration des Droits de l'Homme et du Citoyen prend alors tout son sens (« La liberté consiste à pouvoir faire ce qui ne nuit pas à autrui ») et nous comprenons d'autant plus la réelle problématique de l'équilibre entre sécurité et liberté.

Comment le chef d'entreprise peut-il agir ?

En règle générale, l'utilisation d'internet sur le lieu de travail doit être à usage professionnel, cependant bon nombre d'entreprises tolère une utilisation raisonnable d'internet à des fins personnelles. La Cour de Cassation stipule que l'usage d'Internet par un salarié sur son temps de travail via l'outil informatique mise à sa disposition doit relever du caractère professionnel. L'employeur peut contrôler les connexions de ses collaborateurs et installer un logiciel de surveillance à condition de les informer au préalable et de leur en donner les raisons. Une

déclaration auprès de la CNIL doit être effectuée et, le cas échéant, le comité d'entreprise doit en être informé.

Selon la CNIL, l'utilisation d'internet au travail à titre personnel doit être raisonnable et les sites consultés ne doivent pas avoir un contenu contraire ~~ni~~ à l'ordre public et ~~ni~~ aux bonnes mœurs. Un salarié qui détourne la connexion internet de l'entreprise de son usage professionnel pour visiter des sites à caractère pornographique, par exemple, se rend coupable d'abus de confiance et peut donc faire l'objet de poursuites pénales. En conséquence, il est préférable de mettre en place une charte qui va lui servir à fixer les règles et les conditions d'utilisation d'internet. Il est possible de prévoir dans le règlement intérieur une clause autorisant une utilisation personnelle, ponctuelle et raisonnable des sites Internet dont le contenu n'est pas contraire à l'intérêt ou l'image de l'entreprise. Dans ce cas, le règlement intérieur ou la charte mise en place doit préciser de manière exhaustive tous les comportements interdits au sein de l'entreprise : la consultation de certains sites dit « sensibles », le téléchargement de films, de musiques ou de logiciels, etc. Dès lors, le salarié doit respecter ces règles. Dans le cas inverse, l'utilisation abusive à titre personnel peut entrainer une sanction disciplinaire pouvant aller jusqu'au licenciement. En effet, selon la jurisprudence, cet abus est de nature à constituer une faute grave rendant impossible le maintien du salarié dans l'entreprise.

Un arrêt de la Cour d'appel d'Aix en Provence du 30 janvier 2015, attire l'attention sur les questions de cyber surveillance au travail.

Une salariée utilisait internet pour des besoins privés et les historiques de connexion ont permis d'établir qu'elle ne se connectait pas sur son temps de pause, comme celle-ci l'affirmait, mais dans la journée, immobilisant ainsi son poste de travail pour des jeux en ligne. Le règlement intérieur de l'entreprise prévoyait expressément que « *l'usage abusif de l'intranet et/ou de l'accès à internet à des fins personnelles notamment l'accès à des sites de rencontre, shopping privé, jeux en ligne à plusieurs joueurs*", constituait des agissements proscrits, dispositions également affichées dans les locaux de l'entreprise. Licenciée de ce fait pour faute grave, la salariée a assigné son employeur en licenciement abusif pour défaut de cause réelle et sérieuse. La cour d'appel d'Aix n'a pas suivi la décision du Conseil des prud'hommes de Nice et a infirmé la condamnation de l'employeur et déclaré le licenciement justifié, notamment au motif que « l'employeur a payé à ~~la~~ sa salariée de très nombreuses heures de présence sans contrepartie d'un travail effectif ».

Communication et sensibilisation des collaborateurs.

Une bonne communication interne sur le fonctionnement et les raisons de la mise en place de mesures de contrôle et de surveillance permet de dissuader toute utilisation tendancieuse des outils informatiques de l'entreprise, tout en permettant de constater, stopper et sanctionner les éventuels abus. Il s'agit surtout de faire prendre conscience aux collaborateurs qu'ils peuvent être à l'origine d'attaques envers l'entreprise. Ainsi, il est très important de rédiger le règlement en

collaboration avec les employés afin de trouver un juste équilibre entre les libertés individuelles et le tout sécurité qui ne leur donnera plus la possibilité de travailler en exploitant des outils performants comme internet. L'idée est de leur faire comprendre qu'ils sont acteurs et garants de leur propre sécurité et de la sécurité de l'entreprise, et *in fine* du maintien de leur emploi. La sensibilisation des collaborateurs est donc une nécessite. Si ces derniers n'en perçoivent pas l'utilité, un chef d'entreprise peut mettre en place les meilleurs outils de sécurité possible sans la moindre chance de succès. Le but n'est pas de tomber dans la paranoïa mais de construire une démarche d'anticipation et de prévention, via des moyens simples et efficaces. Ainsi, les notions de sécurité et liberté ne sont pas antinomiques. La liberté est alimentée de sécurité, même si cela est encore mis à mal aujourd'hui par une certaine forme de « trop plein ». Il est important qu'employés et employeurs deviennent tous acteurs de leur propre sécurité, tout en conservant leur liberté. Ils doivent agir conjointement afin de maintenir la coexistence vitale de la sécurité et de la liberté.

Le « Bring Your Own Device (BYOD) », un phénomène émergent.

Le développement de ce phénomène, qui désigne l'usage d'équipements informatiques personnels dans un contexte professionnel, provoque un effacement progressif des frontières entre vie professionnelle et personnelle. L'utilisation d'outils personnels, dans un cadre professionnel, ne peuvent être utilisés qu'à titre subsidiaire car le droit du travail impose à l'employeur de fournir à ses employés les moyens nécessaires à l'exécution de leurs tâches professionnelles. Mais ce qui essentiel ici, avec cette nouvelle pratique, c'est qu'il devient encore plus difficile pour l'employeur de garantir la sécurité des informations. Lorsque la vie personnelle se mêle à la vie professionnelle, comment allier sécurité et liberté ? Là encore, politique de sécurité et sensibilisation seront des mesures à mettre en œuvre pour trouver le bon équilibre.

Ainsi, la coexistence entre liberté et sécurité en entreprise n'est pas un exercice facile. L'apparition de nouvelles menaces et les mutations technologiques invitent à réinventer chaque jour le fragile équilibre entre liberté et sécurité. Sécurité de son emploi du côté de l'employé et sécurité de l'entreprise du côté de l'employeur, l'implication de chacun permet d'instaurer une certaine confiance garantissant les libertés de chacun. Mais, la confiance n'exclue pas le contrôle. Ainsi, la mise en place de mesures et/ou dispositifs construits sur un échange et sur une sensibilisation devrait pouvoir contribuer à une prise de conscience de la nécessité de sécurité des informations tout en protégeant les libertés. La liberté des collaborateurs ne doit pas s'arrêter là où la sécurité des données commence. Il est nécessaire de sécuriser la liberté pour empêcher tout excès d'usage de la liberté et protéger ainsi la liberté de chacun.