« La liberté d'un salarié (droit de s'exprimer, droit de surfer, droit d'utiliser tel ou tel logiciel, tel outil, dans son entreprise, …) doit-elle s'arrêter là où la sécurité des données numériques commence ? »

franck.helie@free.fr

Franck HELIE
décembre 2015

INSTITUT LÉONARD DE VINCI
M.B.A. « MANAGEMENT DE LA SÉCURITÉ DES DONNÉES NUMÉRIQUES »
promotion 2015-2016

En matière de droit d'expression du salarié, le droit du travail est absolument clair en la matière :

« *Les salariés bénéficient d'un droit à l'expression directe et collective sur le contenu, les conditions d'exercice et l'organisation de leur travail.* », Art. L2281-1 du code du Travail.

En cela, cet article du Code du travail ne fait que retranscrire l'article 11 de la Déclaration des Droits de L'homme et du Citoyen *« la libre communication des pensées des opinions est un des droits les plus précieux de l'homme…* ».

Cela veut-il dire pour autant que le salarié, en tant que citoyen comme un autre, est complètement libre de faire ce que bon lui semble sur son lieu de travail ? Quelles peuvent être les conséquences de ses actes pour l'entreprise ? A-t-il seulement conscience que ses actes peuvent avoir un effet sur la sécurité des données numériques de l'entreprise ? L'entreprise peut-elle ou doit-elle mettre en place des systèmes de protection ? Sous quelle forme ? Judiciairement, quelles sont les responsabilités du salarié ? Du dirigeant d'entreprise ?...

Bref, voici défini un tout petit inventaire de questions posées par la « simple » notion de « *liberté du salarié* », si on examine ce sujet sous l'angle de la sécurité informatique.

Une frontière entre vie privée, vie du salarié très perméable

Le salarié est lié à son entreprise par l'intermédiaire d'un contrat de travail. Ce document fixe un cadre bien précis à ses activités. Il y est décrit les tâches qu'il devra accomplir et pour lesquelles il recevra en contrepartie une rémunération.

D'un autre coté, aujourd'hui, l'entreprise équipe de plus en plus souvent ses salariés de moyens technologiques modernes pour faciliter la communication interne et accessoirement améliorer la productivité globale. Ces moyens sont généralement des ordinateurs de bureau, un accès internet, une boîte aux lettres électronique ainsi que toute une infrastructure technique qui collecte et sécurise les données produites.

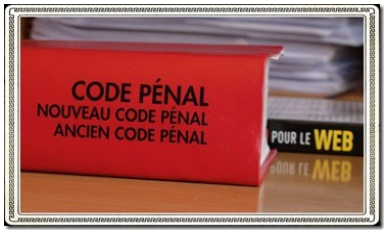
Or, ces données constituent de plus en plus souvent des éléments essentiels à l'activité de l'entreprise dans son ensemble, quand celles-ci ne forment pas tout simplement son fonds de commerce.

Un autre phénomène apparaît de plus en plus souvent. En effet, cet environnement devient de plus en plus familier pour le salarié qui retrouve sur son lieu de travail des « choses » qu'il possède également à son domicile et qu'il utilise très régulièrement. L'amalgame est rapidement fait. Ce que je peux faire à la maison, pourquoi ne pourrais-je pas le faire au travail ? C'est la même « chose » …. Le haut débit, voire très haut débit aidant (ADSL 2+, fibre optique etc …), il peut même arriver que le salarié en vienne à critiquer les performances des infrastructures de l'entreprise, ne comprenant pas pourquoi la navigation internet est plus lente qu'avec sa connexion personnelle.

L'ensemble de ces éléments réunis, la liberté d'expression à laquelle on ajoute les moyens techniques, créé des conditions qui conduisent à rendre de plus en plus floue la frontière entre vie « au travail » et « vie privée ».

Cet état de fait soulève également plusieurs questions pour les équipes IT et notamment pour la gestion de la sécurité des données numériques de l'entreprise. Si on se place du point de vue de l'entreprise, on est en droit de se demander si le salarié a le droit d'utiliser ou non les moyens techniques à sa disposition à des fins privées. En effet, est-il légitime que le salarié utilise la liaison internet de l'entreprise pour stocker sur son « espace partagé » ou « Cloud public » ses vidéos et photos de vacances par exemple ? Qu'il mette à jour sa page facebook ou son blog personnel ? Sans envisager pour l'instant les aspects juridiques de ce genre de comportements sur le temps de travail, de telles actions, multipliées par quelques dizaines d'individus peuvent très rapidement occuper inutilement les ressources techniques de l'entreprise et indirectement détériorer potentiellement les performances globales, jusqu'à peut-être saturer le lien réseau qui achemine internet dans la société.
En contrepartie, ces salariés « indélicats » s'exposent potentiellement à des sanctions, tout dépend comment l'entreprise gère sa sécurité informatique. Il est possible que ces salariés indélicats risquent leurs emplois, comme l'a appris à ses dépens cet employé d'un huissier de justice qui téléchargeait illégalement des fichiers de musiques depuis son ordinateur professionnel. (*CA Versailles, 31 mars 2011, n° 09/00742, 5e ch.*). Celui-ci a été licencié pour faute grave et ce licenciement a été confirmé en appel, créant ainsi de la jurisprudence en la matière. De la même façon, tenir des propos injurieux envers son employeur sur un espace « numérique » public (type facebook…) peut non seulement conduire au licenciement pour faute, mais aussi à une condamnation au pénal pour délit d'injure publique (*CA Besançon, 15 novembre 2011, n° 10-02642, ch. Soc.*)

Un cadre légal généralement en faveur du salarié



Deux attitudes sont possibles dans de telles situations pour l'entreprise. Le méthode "laxiste" qui considère que de tels agissements sont peu importants, et que de toute façon l'entreprise se doit de respecter la liberté d'expression des salariés définie par le code du travail, confirmée par la loi n° 78-17 du 6 janvier 1978 relative à « *l'informatique, aux fichiers et aux libertés* ». L'autre méthode possible est au contraire le mode « autoritaire » qui vise à contrôler et interdire ces flux de données. Mais dans ce cas, l'entreprise s'expose à des problèmes légaux, car elle peut être accusée de se livrer à un contrôle des salariés. Auquel cas, elle doit en informer les instances représentatives du personnel (IRP) et peut conduire à des situations juridiquement délicates comme le rappel un article paru le 28 janvier 2013 sur le site de la Commission Informatique et Libertés (CNIL) : « *Le recrutement, contrôle des horaires, gestion des carrières, cybersurveillance, impliquent la collecte par l'employeur de données personnelles aux salariés qui, pour être légitime, doit respecter le cadre légal et les principes rappelés par la CNIL* ». (http://www.cnil.fr/linstitution/actualite/article/article/protection-des-donnees-personnelles-au-travail-les-bonnes-pratiques/)

La bonne attitude à tenir dans de tels cas est certainement de rechercher un mixte entre les deux approches. Comment être certain qu'il s'agit bien des photos « personnelles » qui circulent et non les photos du dernier prototype de voiture qui sortira l'année prochaine ? D'un autre côté, nous ne pouvons pas interdire à notre service communication de mettre en ligne sur le site internet de la société les

photos du dernier arbre de Noël organisé par le CE …..Il est donc clair que la réponse ne peut être ni blanche, ni noire.

La nécessité d'une politique de sécurité interne claire et précise

Par contre, lorsque nous parlons de sécurité des données numériques, nous voyons bien que l'entreprise a l'obligation de mettre en place une politique de sécurité clairement définie, adaptée aux métiers et connue de tous ses salariés. Encore faut-il qu'elle soit appliquée par tous et contrôlée continuellement.
Voici un autre exemple qui fait encourir un risque important à la sécurité du système d'information de l'entreprise et donc aux données numériques qu'il renferme. On parle de plus en plus souvent « d'entreprise sans frontières » dans laquelle beaucoup de salariés sont mobiles. C'est à dire qu'ils utilisent le système d'information sans être physiquement présents dans les locaux de la société. Le télétravail en est la représentation la plus courante. Là encore, la frontière vie privée, vie professionnelle est encore plus floue.

Sur le lieu de travail, les ordinateurs mis à disposition des salariés sont le plus souvent gérés par les équipes informatiques de l'entreprise. Il est donc tout à fait légitime que ces postes de travail soient verrouillés et équipés de logiciels de sécurité permettant de suivre l'ensemble des accès et des données, sous les réserves exposées par la CNIL. Ces moyens techniques mis en place par les équipes IT visent essentiellement à garantir un certain niveau de sécurité mais peuvent être très facilement détournés de leur but premier. La CNIL veille donc à ce qu'il n'y ait pas de dérapages ou d'abus potentiels et surtout elle est très vigilante pour que soit maintenu « un équilibre entre le contrôle de l'activité des salariés et la protection de la vie privée ».
Pour y parvenir et par l'intermédiaire du correspondant informatique et libertés (CIL) de l'entreprise, la CNIL oblige cette dernière à effectuer une déclaration préalable concernant les processus de traitements des données à caractère personnel qu'elle met en œuvre. Cette déclaration inclus notamment l'obligation d'information des salariés de l'existence de tels processus. A cet égard, la vigilance de la CNIL porte principalement sur tous les dispositifs de vidéosurveillance, de géolocalisation, de contrôles de l'usage de la messagerie, d'internet et des horaires de travail. Car effectivement, techniquement, certains logiciels installés pour sécuriser les postes de travail de l'entreprise collectent de très nombreuses informations, y compris des données concernant l'utilisation qui est faite du poste, et donc indirectement ces éléments techniques peuvent constituer un moyen de « surveillance » des salariés si une exploitation de ces informations est réalisée. La transparence est donc de mise, même si la CNIL relève très régulièrement des manquements à ce niveau…

À l'extérieur de l'entreprise, le niveau de sécurité chute considérablement car il est beaucoup plus difficile de contrôler l'utilisation qui est faite du poste de travail, et surtout de contrôler qui l'utilise réellement. En effet, si l'entreprise se contente d'un système basé sur un login et un mot de passe pour établir la connexion sur son réseau, elle s'expose à un risque très net d'usurpation d'identité. Il est relativement simple pour quelqu'un qui aurait, par exemple, dérobé l'ordinateur d'un salarié de

retrouver ses identifiants de connexions et de les utiliser pour se connecter au réseau. A son insu, l'entreprise se retrouve alors avec un utilisateur connecté sur son système d'information mais qui ne fait pas partie des effectifs et qui potentiellement a accès à des données sensibles, voire stratégiques. En d'autre termes, une source potentiellement non négligeable de fuite de données.
Cet aspect de la sécurité du système d'information est malheureusement trop souvent sous estimée par les dirigeants de PME principalement, car les technologies à mettre en place pour se prémunir de ce risque sont relativement onéreuses (Firewall, PKI, single sign on, biométrie, systèmes un peu plus intrusifs de « Data Leak Prevention », ou « DLP », etc …) C'est tout le problème de l'authentification sur un système d'information qui est posé. Il ne suffit pas de dire qui je suis, encore faut-il prouver qui je suis. Des méthodes existent bien entendu pour y parvenir, mais elles sont très souvent complexes à mettre en place, exigent une extrême rigueur du service informatique et sont donc bien souvent hors de portées des "petites" et "moyennes" structures que sont les PME/PMI et qui ne disposent pas des ressources techniques nécessaires.

L'émergence de nouvelles menaces technologiques qui peuvent compromettre les politiques de sécurité mises en place

Mais sans aller jusqu'à envisager cette usurpation « d'identité numérique » du salarié par un tiers mal intentionné, considérons simplement le salarié en télétravail. Celui-ci peut avoir la possibilité d'utiliser son propre matériel informatique pour effectuer ses tâches quotidiennes. Tout dépend des conditions définies au sein de l'entreprise pour gérer le télétravail. Lorsqu'on sait qu'en 2012, L'INSEE indiquait que 75,2% des foyers français étaient équipés d'ordinateur et que ce chiffre est en constante progression depuis 2004 où le taux d'équipement était de 44,7% (http://www.journaldunet.com/solutions/dsi/micro-ordinateurs-france.shtml). Il peut être tentant pour une entreprise d'inciter ses salariés à utiliser leur propre matériel et ainsi réaliser une économie substantielle.
Mais est-ce que ce mode de fonctionnement, appelé aussi « B.Y.O.D. », « Bring Your Own Device » est-il si intéressant pour une entreprise ? Quels en sont les risques inhérents ?
Cette lettre de la C.N.I.L.
(http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/Lettre_IP_n__7__Intimite_et_vie_privee_du_travailleur_connecte.pdf) parue le 18 juillet 2014 rappelle les bonnes pratiques a adopter en matière de BYOD.

Si le service IT de l'entreprise ne prend pas de dispositions particulières telles que celles énumérées dans cette lettre pour gérer ces équipements (limitation et contrôle des usages, proposer des environnements « sécurisés » tels que le VPN, chiffrement des données stockées, effacement des données en cas de perte ou vol des devices...), l'entreprise se retrouve immédiatement exposée au risque de présence sur son système d'information d'un matériel potentiellement infecté par des logiciels malveillants de types virus, malwares ou autre ver.
En effet, généralement, par simple ignorance ou simple méconnaissance des risques encourus,

l'ordinateur des particuliers est bien souvent très peu protégé contre ce genre de menaces. D'autant plus que l'ordinateur familial est utilisé par tous les membres du foyer, y compris les adolescents qui y ont bien souvent installé toute une série de jeux récupérés d'on ne sait où. Ces jeux sont le plus souvent « crackés », c'est à dire que tous les systèmes de protection contre les copies illicites ont été retirés. Même si cet état de fait est tout à fait illégal, c'est l'attrait économique qui pousse les jeunes à braver ces interdictions. Mais le geste est non dénué d'intérêts pour les contrefacteurs. En effet, ces personnes qui ont si « généreusement » modifié le code exécutable du jeu pour le rendre « copiable » sont généralement des hackers qui ne le font pas si innocemment que cela. Ils en profitent bien souvent pour intégrer un code binaire malicieux à l'intérieur du jeux. Le but recherché par ce bout de programme est variable. Bien souvent, il s'agit de transformer l'ordinateur qui exécute ce bout de logiciel, en ordinateur « zombie » qui pourra être utilisé à distance par la suite pour participer, avec des milliers d'autres, à une attaque coordonnée par déni de service contre un site internet ou un hébergeur cible. Mais les buts recherchés par ces hackers peuvent être beaucoup plus malicieux. Ainsi, la simple installation innocente du jeu infecté transforme l'ordinateur en véritable bombe à retardement ou en ordinateur « espion » qui communiquera par exemple aux hackers tous les codes d'accès, mots de passe ou autre numéros de carte bleue qui seront saisis sur l'ordinateur infecté (logiciels type « key loggers »).

Les ordinateurs des particuliers sont bien entendu les cibles privilégiées des actions de malveillance car les plus facile d'accès. Le plus terrible avec ce type de logiciels, c'est que les systèmes de parade classiques tel que les anti-virus sont en général inefficaces pour les détecter. Le particulier, s'il n'y prend pas garde, utilisera l'ordinateur en toute confiance sans savoir qu'il est infecté et qu'il encours des risques importants de vols d'informations.

On imagine très bien qu'un tel ordinateur utilisé a des fins professionnelles, en se connectant au système d'information de l'entreprise, devient une véritable menace pour l'ensemble des autres postes informatique de l'entreprise. Ces logiciels malveillants ayant la fâcheuse habitude et capacité de se répandre en infectant les autres ordinateurs qu'ils rencontrent sur le réseau.

Nous voyons bien que l'entreprise et plus particulièrement son système d'information ainsi que les données numériques qu'il renferme, est exposée en permanence à des menaces aussi bien internes qu'externes. Il en va de sa propre survie parfois, mais au moins de sa responsabilité de mettre en place impérativement des moyens aussi bien techniques qu'organisationnels pour se prémunir au maximum de ces menaces. (cf lettre de la CNIL du 18 juillet 2014)

Dans l'idéal, cela commence par une formation continue des salariés, ou tout au moins une information claire des règles mises en place pour le respect de la déontologie. Cela peut prendre la forme d'une charte informatique qui définie les règles de sécurité informatique en place et les bonnes pratiques à tenir au quotidien avec les postes de travail et connexions internet mis à leur disposition. Il est juridiquement conseillé d'annexer cette charte au règlement intérieur de l'entreprise. En effet, tous les contrats de travail font référence à ce règlement. Ainsi, la signature du contrat de travail engagera

implicitement le salarié au niveau de ses actes en terme de sécurité informatique. Il convient néanmoins de rappeler régulièrement ces règles, voire les mettre à jour si besoin.
Tout outil technique utilisé pour surveiller l'activité et sécuriser les postes de travail doit cependant être clairement mentionné dans cette charte et le comité d'entreprise doit être informé de la présence de tels logiciels. Accessoirement, l'entreprise a aussi obligation légale de déclarer auprès de la CNIL le fait qu'elle utilise de tels outils.

Une jurisprudence à « géométrie variable » en matière d'utilisation des outils informatique sur le lieu de travail

Nous avons abordé les principaux aspects pratiques à mettre en œuvre pour garantir au minimum la sécurité du système d'information de l'entreprise. Maintenant, sur un plan juridique, à quels risques l'entreprise est-elle exposée si parmi ses salariés, il est découvert des comportements répréhensibles ?
En tout état de cause, la jurisprudence est très claire en matière d'utilisation des moyens informatiques de l'entreprise à des fins personnelles. Elle tolère en effet, par exemple, l'utilisation à titre privée de la connexion internet professionnelle « *tant que l'utilisation de celle-ci reste raisonnable* »

Cela dit, les juges ont considéré que constitue une faute grave justifiant le licenciement du salarié, le fait d'avoir usé de la connexion internet de l'entreprise, à des fins non professionnelles, pour une durée totale de 41 heures sur un mois (*Cass. Soc. 18 mars 2009, n°07-44247*)
La Haute juridiction a également retenu la faute grave dans le cas d'une salariée qui s'était connectée pendant son temps de travail à de très nombreuses reprises à des sites extra professionnels (*Cass. Soc. 26 février 2013, n°11-27372*).
Par ailleurs, l'usage abusif de la connexion internet peut entraîner des poursuites pénales à l'encontre d'un salarié. Ainsi, le salarié qui détourne la connexion internet de l'entreprise de son usage professionnel, pour visiter des sites à caractère pornographique, se rend coupable du délit d'abus de confiance (*Cass. Crim. 19 mai 2004, n°03-83953*).
Ou encore, un salarié se rendant sur son lieu de travail sur des sites « d'activité sexuelle et de rencontres » se rend coupable de manquements graves à ses obligations découlant du contrat de travail. Ces consultations étant constitutives d'une faute grave (*Cass. Soc. 21 septembre 2011, n°10-14869*)
La responsabilité du salarié est donc clairement engagée s'il est prouvé qu'il se rend coupable d'utilisations abusives des ressources informatiques de l'entreprise à des fins non professionnelles.

Et pourtant, en matière de consultation de sites pornographiques sur le lieu de travail, la Cour de Cassation a rendu le même jour, deux arrêts radicalement opposés (*Cass Soc., 10 mai 2012, nos 11-11060, et 10-28585*). Le premier confirmant la faute grave, le second, au contraire, estimant que cette consultation de tels sites n'est pas une faute… Ces deux décisions se sont basées sur les règles internes de gestion de la sécurité informatique en place dans les entreprises concernées. Elles ne font que confirmer l'importance pour une entreprise, de la nécessité de faire respecter scrupuleusement la charte informatique, au risque de la rendre inefficace si cela n'est pas fait.
D'autre part, en terme de droit pénal, il est à noter que les tribunaux ont de plus en plus tendance à

considérer que l'employeur est responsable de l'utilisation qui est faite par ses salariés des moyens informatiques qu'il met à leurs disposition. Pour cela, les juges s'appuient particulièrement sur les termes de l'article 121-7 du code pénal : «*Est complice d'un crime ou d'un délit la personne qui sciemment, par aide ou assistance, en a facilité la préparation ou la consommation. (…)*». L'employeur qui met à disposition des outils informatiques servant à commettre un délit de détention d'images pédophiles par exemple ne risque t-il pas de se retrouver complice de ce délit pénal ?
La réponse est a priori négative, dans la mesure où la complicité implique que doit être démontré un élément intentionnel. Or, le plus souvent, l'employeur ignore tout du délit jusqu'à sa découverte, il n'est donc pas complice. En revanche, s'il ne fait rien après avoir découvert les fichiers illicites et laisse perdurer la situation, il risque alors effectivement de devenir complice…
La jurisprudence introduite par l'arrêt *Cass. crim, 10 juillet 1963, n°6293417*, confirme depuis de nombreuses années la responsabilité pénale du dirigeant d'entreprise.
« *Le dirigeant est présumé avoir commis une faute de négligence dans son devoir de contrôle, du seul fait que l'infraction du préposé est matériellement établie.* »
La justification de cette présomption tient ainsi au fait « *qu'il appartient au chef d'entreprise de veiller personnellement à la stricte et constante exécution des prescriptions réglementaires* ». Cette responsabilité pénale du dirigeant d'entreprise s'étend bien entendu aujourd'hui au domaine de la sécurité des données numériques de l'entreprise ; cela particulièrement face aux éventuels délits ou crimes que pourrait commettre un salarié sur son lieu de travail en utilisant les moyens technologiques mis à sa disposition.

Conclusion

En conclusion et pour répondre au sujet général de ce billet. Est-il une autre réponse possible que la réponse affirmative ? Je ne pense sincèrement pas. Nous avons vu un certain nombre d'exemples qui obligent la mise en place de barrières techniques et garde-fous pour assurer une sécurité minimum des données numériques et du système d'information dans son ensemble. Même si ces moyens (firewall, NOC, anti-virus, appliances d'authentification, PKI, systèmes de « DLP », etc …) ne sont pas infaillibles, loin de là (cf « backdoor » découvertes très récemment dans tous les firewalls Juniper) et sont forcément obsolètes face aux vulnérabilités qui apparaissent quotidiennement, ils ont le mérite d'exister et de remplir correctement leurs fonctions essentielles. Les ignorer ou penser qu'une entreprise peut s'en passer serait irresponsable, voire suicidaire.
Par conséquent, le simple fait de mettre en place des procédés qui visent à limiter et/ou surveiller l'activité d'une personne et à fortiori d'un salarié constituent déjà une entrave à sa liberté il me semble. Sartre ne disait-il pas : « Ma liberté s'arrête où commence celle des autres », cette maxime s'applique donc aussi, et de façon évidente, à la sécurité des données numériques.
D'une manière plus générale, cette notion de liberté au sens large si chère aux philosophes des Lumières n'est-elle tout simplement pas une illusion finalement ? En démocratie, les lois ne sont-elles pas là pour régir la vie de la Cité et de chaque citoyen, en limitant implicitement la liberté de chacun ?