COURTOIS LEBEL

Communiqué de presse
27 mars 2013

L'encadrement juridique de l'utilisation de leurs équipements personnels par les salariés

Le BYOD (« Bring your own device »), ou l'utilisation par les employés de leurs équipements personnels (smartphone, pc portable, tablette tactile…) dans un contexte professionnel, est aujourd'hui une pratique courante en entreprise, qui demeure pourtant peu encadrée juridiquement. Donatienne Blin, avocat au sein du département Informatique & réseaux du cabinet Courtois Lebel, passe en revue les points de vigilance.

L'accès immédiat et en toutes circonstances au système d'information de l'entreprise grâce aux BYOD améliore la réactivité et la productivité des employés.

Pourtant cette pratique souvent tolérée par les entreprises présente, en l'absence d'encadrement spécifique, des risques substantiels pesant sur la sécurité du système d'information, précisément sur la confidentialité et l'intégrité des données de l'entreprise : négligence de l'utilisateur (prêt ou perte du terminal), applications malveillantes téléchargées, virus ou failles de sécurité de l'OS (operating system) rendent possibles les accès frauduleux au système d'information par des tiers non autorisés.

Chaque type de BYOD présente des risques particuliers qui devront être traités différemment.

L'utilisation des équipements personnels et l'anticipation des risques est donc une problématique majeure au sein de l'entreprise et précisément des directions juridiques et des directions des systèmes d'information.

Toute perte ou altération des données personnelles peut provoquer des dommages économiques à l'entreprise, mais peut également engager sa responsabilité : l'article 34 de la loi n°78-17 Informatique, fichiers et libertés du 6 janvier 1978 impose au responsable de traitement de données personnelles de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement pour « préserver la sécurité des données et notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Ainsi, dans le prolongement de la politique de sécurité mise en œuvre par les DSI (directions des systèmes d'information), les entreprises doivent encadrer l'utilisation des BYOD et garder en toutes circonstances le contrôle de l'accès au réseau et des données y étant accessibles.

Cet encadrement devra se matérialiser par la mise en place d'une charte informatique, ou la mise à jour de celle-ci dès lors qu'elle serait existante, en vue d'y inclure les mesures propres à leur utilisation, applicables à l'ensemble des salariés.

Les problématiques suivantes devront y être abordées :

L’accès au système d’information de l’entreprise

Compte tenu des risques (introduction de virus, fuite, perte, altération de données personnelles ou sensibles et confidentielles...) pesant notamment sur les données de l’entreprise, des règles d’accès au système d’information de l’entreprise via un équipement personnel devront être adaptées.

On pourra prévoir que le salarié utilisant un équipement personnel soit obligé, préalablement à la connexion de son terminal au réseau de l’entreprise, d’avertir le DSI et de faire contrôler son équipement afin de s’assurer de sa conformité en termes de sécurité.

De même, le salarié devra toujours disposer d’un équipement en état de fonctionnement, et systématiquement, télécharger les mises à jour proposées par les éditeurs (du système d’exploitation, des logiciels et des applications utilisés).

Il pourra également être imposé au salarié de protéger son équipement par mot de passe afin d’en interdire l’accès aux tiers.

L’obligation de faire l’acquisition d’outils permettant de limiter les risques de sécurité pourra également être imposée au salarié : logiciel antivirus, de cryptage des données, ou encore dispositif permettant de supprimer les données à distance dès lors que les données seraient directement stockées sur l’équipement personnel du salarié.

Afin d’éviter la perte définitive des données (les applications cloud le permettent), il peut également être imposé au salarié d’installer des outils de sauvegardes journalières ou de synchronisation des données avec un autre appareil.

En cas de vol, perte, ou constat quelconque d’intrusion frauduleuse sur l’équipement personnel, le salarié devra immédiatement prévenir le DSI afin qu’il prenne toutes mesures nécessaires pour protéger le système d’information de l’entreprise et les données y étant stockées.

La propriété et le contrôle des données accessibles via l’équipement personnel

Il devra être précisé que toutes données professionnelles stockées ou accessibles via un équipement personnel demeureront la propriété exclusive de l’employeur.

Les cas d’accès et de contrôle aux données stockées sur l’équipement personnel du salarié par l’employeur devront être précisément définis dans la charte.

Pour rappel, la règle est la suivante : le salarié utilisant un équipement professionnel doit expressément identifier les éléments personnels comme tels ; à défaut d’identification explicite contraire, le contenu est considéré comme ayant un caractère professionnel et son employeur peut dès lors y accéder.

L’employeur ne peut accéder aux fichiers personnels expressément identifiés comme tels par son salarié hors la présence de ce dernier, et ce sauf risque ou évènement particulier.

Il devra être imposé au salarié, en cas de départ de l’entreprise, de transférer à son supérieur hiérarchique l’ensemble des données professionnelles éventuellement stockées sur son équipement personnel. En cas d’application cloud, l’accès doit être coupé au jour du départ.

La problématique du coût ou la participation de l'entreprise aux frais payés par les salariés

Dans le cas des BYOD, le coût des équipements personnels utilisés à des fins professionnelles et les éventuels frais annexes (assurance, maintenance, anti-virus, forfait téléphone/internet, logiciels indispensables à l'activité, tel que le Pack Office de Microsoft) sont de fait déportés chez les salariés.

Certains coûts pourraient être partiellement pris en charge par les entreprises, dès lors qu'il est raisonnable de considérer que le salarié n'aurait pas fait l'acquisition de ces différents outils, imposés par l'entreprise, dans le cadre d'une utilisation strictement personnelle.

Ces règles liées à la prise en charge totale ou partielle des coûts devront être définies et portées à la connaissance des employés.

Cette problématique rejoint celle de la discrimination entre les salariés : certains salariés pourront se procurer eux-mêmes leur propre équipement tandis que d'autres ne le pourront pas pour des raisons exclusivement financières.

La durée légale du travail

En utilisant son équipement personnel, notamment pour recevoir ses mails professionnels, le salarié reste connecté en permanence avec le réseau de son entreprise.

Cela a pour conséquence d'augmenter la durée du travail. Or les entreprises doivent respecter la durée légale du temps de travail sous peine de sanction.

La charte devra donc tenir compte du fait que l'utilisation de l'équipement personnel ne doit en aucun cas porter atteinte à la durée légale du travail applicable à chaque salarié concerné.

Au même titre, aucune sanction ne devrait découler d'une absence de réactivité d'un salarié en dehors de ses horaires de travail.

Les accès aux applications ou plus généralement au réseau de l'entreprise en dehors des horaires de travail peuvent être directement bloqués à distance par la direction des systèmes d'information. Ce système impose de créer des groupes d'utilisateurs autorisés, en fonction des horaires de travail qui leur sont applicables, du poste ou encore du rang hiérarchique occupé.

La responsabilité en cas de vol ou de dommages matériels causés à l'équipement personnel

La question des éventuels dommages causés à l'équipement personnel de l'employé sur le lieu de travail sans aucune faute de sa part devra être tranchée dans la charte.

Par exemple un virus pourrait être transmis sur l'équipement personnel du salarié qui se serait connecté au réseau de l'entreprise.

Dès lors que l'équipement du salarié serait endommagé par la faute ou la négligence de l'entreprise, celle-ci devrait, dans ces conditions, être responsable des réparations.

Les conditions de responsabilité et de réparation totale ou partielle en cas de dommages matériels doivent donc être précisément définies, dans le respect des règles du code du travail applicables.

La redéfinition des règles d'utilisation prohibées

Il conviendra d'élargir les règles d'utilisation prohibées des ressources de l'entreprise aux ressources personnelles, dès lors que le réseau internet de l'entreprise devient accessible via un équipement personnel.

Ainsi, il faudra rappeler au salarié que les règles d'utilisation prohibées des ressources de l'entreprise s'étendent à son équipement personnel (faits d'atteinte à la vie privée ou à l'image d'un tiers, diffamation, injure, discrimination, dénigrement de l'entreprise, l'atteinte à l'image de marque, à sa réputation ou à ses droits)

De même, devront être prohibés les téléchargements de contenus portant atteinte au droit de la propriété intellectuelle qui seraient effectués par le salarié via le réseau de l'entreprise avec son équipement personnel.

Enfin, il devra être interdit au salarié de se connecter via des réseaux wifi non sécurisés mais également de télécharger des applications ou logiciels non sécurisés sur son équipement personnel. La DSI pourrait préalablement établir une liste d'applications ou d'éditeurs interdits car présentant des risques en termes de sécurité, et mettre à jour cette liste.

L'opposabilité des règles

L'opposabilité de ces règles devra être assurée afin de pouvoir engager la responsabilité disciplinaire ou judiciaire du salarié qui ne les aurait pas respectées et qui aurait été responsable du dommage causé à l'entreprise par sa faute.

Ces règles peuvent donc figurer dans la charte informatique de l'entreprise, laquelle sera elle-même annexée au règlement intérieur. Les instances représentatives du personnel devront être consultées.

Courtois Lebel en bref

Cabinet d'avocats d'affaires français fondé en 1969, **Courtois Lebel** offre à une clientèle de dimension internationale une large gamme de prestations juridiques dans les principaux domaines du droit des affaires avec une réelle dimension internationale.

Nos domaines d'activités

- Assurance
- Banque et Bourse
- Conformité / Regulatory
- Concurrence
- Contentieux
- Corporate / M&A
- Distribution
- Données personnelles
- Financement immobilier
- Fiscalité
- Immobilier
- Informatique & réseaux
- Internet
- Management package
- Marketing direct / Consommation
- Outsourcing
- Propriété Intellectuelle
- Restructuring
- Social

Courtois Lebel est membre de deux réseaux de cabinets d'avocats : AEL, réseau européen, et ALFA, réseau international d'envergure.

Contacts presse :

Corinne Coman
Responsable Marketing & Communication
Courtois Lebel
15 rue Beaujon - 75008 Paris
Tél : 01 58 44 92 92
ccoman@courtois-lebel.com

Nicole Coiffard et Florence Laurent-Bellue
Agence de presse Cordiane
Tél : 01 39 62 33 42
ncoiffard@cordiane.com flaurentbellue@cordiane.com