BYOD : que dit la loi ?

0

24 jan 2013 BYOD, sécurité by Aurelie Magniez

L'ADN du social numérique

Le BYOD (« Bring your own device ») littéralement « apporter votre propre matériel » désigne la pratique consistant à apporter ses propres outils informatiques personnels, smartphones, tablettes, et autres portables et à les utiliser dans le cadre de ses activités professionnelles.

Le BYOD qui se décline aussi en « buy your own device » et qui consiste à allouer une enveloppe à l'utilisateur qui doit alors utiliser et entretenir son propre terminal au travail, dénote une transformation importante des modalités d'exécution du travail.

Apporter son propre matériel pour l'exécution de sa mission pourrait être une négation du principe même du droit du travail français.

Pourtant la réalité des marchés s'impose. Les utilisateurs souhaitent pouvoir accéder à un contenu, une information ou une offre marchande quels que soient le moment, le lieu où le mode d'accès. Il s'agit de la tendance ATAWADAC (Any Time, Anywhere, Any Device et Any Content).

L'instantanéité de l'accès à l'information est aujourd'hui un critère essentiel de l'utilisateur mais aussi de l'entreprise.

Le BYOD est ainsi associé à la question de la mobilité qui prend une importance cruciale avec la vente de smartphones embarquant des applications et un accès permanent à Internet.

Cette tendance pour un salarié ou un fonctionnaire n'est pas en soi une nouveauté. Ce qui l'est bien plus, c'est l'intégration de ces interfaces numériques personnelles au système d'information de l'entreprise ou de l'administration publique.

Utiliser son propre « IPAD » pour prendre l'ensemble de ses notes dans le cadre d'une réunion, l'intégrer instantanément dans telle ou telle application, (enregistrement numérique, transcription vers sa messagerie, photographie ou vidéo), fait partie des usages des opérationnels.

Ces réalités des sociétés numériques doivent être absorbées par des systèmes d'information dont le modèle classique demeure centré sur des équipements et logiciels façonnés, imposés par le DSI.

Recherche sur le site

Search...

Les plus commentés


Open data : opportunités et limites d'un patrimoine gratuit
3 Comments


Recrutement pour la DSI : pourquoi un tel casse-tête ?
1 Comment


La stratégie digitale de demain
1 Comment


Quelle stratégie d'image de marque sur internet et les réseaux sociaux ?
1 Comment


J.C. Moissinac - Télécom ParisTech : L'interview intégrale
1 Comment

L'utilisateur a les facultés pour se fabriquer lui-même ces applications. Combien de salariés ou d'agents ont déjà téléchargé des applications sur leurs terminaux personnels, sur lesquelles transitent les informations de leur entreprise (Dropbox)?

Le « très haut débit mobile » qui accompagne les professionnels dans leurs déplacements facilite l'accès au Cloud. Dès lors le traitement de la base de données de l'entreprise est facilité.

Cette réalité du terrain a tendance à court-circuiter le SI « classique » de l'entreprise.

Or à l'heure de la fléxisécurité, du télétravail, de la conduite du changement vers des systèmes d'information support de croissance et d'ouverture de l'entreprise, en d'autres termes, de la nécessité « de réformer en profondeur le modèle français pour l'adapter au temps présent », le BYOD apparaît comme une nouveau mode de consommation des données de l'entreprise.

Le BYOD est une situation singulière en effet, car elle propulse les principes directeurs, vie privée résiduelle et présomption d'usage professionnel, vers des contenus professionnels embarqués, et un usage professionnel par dérogation.

Quelle est la problématique juridique du BYOD ?

En environnement « traditionnel » où le matériel professionnel est mis à disposition des collaborateurs :

- les matériels et applications appartiennent à l'employeur ;
- leur utilisation est présumée être « professionnelle » ;
- l'employeur ne peut interdire un usage personnel résiduel ;
- l'employeur est en droit de contrôler les conditions d'utilisation en environnement professionnel hors la présence du collaborateur ;
- l'employeur est en droit de consulter les zones et dossiers « personnels » dans des conditions strictes.

En environnement « BYOD » :

- les matériels appartiennent au salarié ;
- les applications appartiennent au salarié en général et à l'employeur pour les applications professionnelles ;
- l'utilisation varie selon le type d'application utilisée ou d'usage :
  - application personnelle = environnement privé ;
  - application professionnelle embarquée = environnement professionnel
  - application personnelle utilisée à des fins professionnelle = environnement professionnel
  - par principe l'utilisation est personnelle, et l'usage professionnel est réalisé « sur demande ».

En d'autres termes la question posée est de savoir si le BYOD est une pratique imposée ou une pratique d'opportunité ? Quelle est la marge de manœuvre d'une entreprise ou d'une entité publique pour accepter, refuser ou conditionner l'usage du BYOD ?

Le BYOD est dès lors une décision stratégique d'entreprise. Tous les matériels sont-ils concernés ? Quelles sont les catégories de personnels impactées ? Quels sont les usages autorisés ?

Les risques juridiques dans ce panorama virtuel sont néanmoins répertoriés et ne sont pas ou ne devraient pas être un frein aux déploiements « any devices » de « l'ère poste PC ».

Synthèse des risques

La synthèse de ces risques permet de regrouper deux catégories : les risques techniques et les risques organisationnels.

Les premiers ne sont pas des risques nouveaux liés aux BYOD en lui-même. Ils sont axés d'une part vers le terminal. Ils concernent le « jailbreak », le « rooting », la compatibilité des OS, la démarcation « données privées » à celles de l'entreprise. L'autre axe vise d'autre part la protection du SI et les applications de l'entreprise.

Le réseau social d'entreprise : nouvelles questions
1 Comment

La sécurité : frein ou accélérateur à l'avènement du Cloud Computing ?
1 Comment

Oracle et les communautés Open Source
1 Comment

IT-expert n°90 - mars/avril 2011
1 Comment

Les réductions de coûts IT en tête des préoccupations des entreprises
1 Comment

Archives

Choisir un mois

La cohabitation de l'environnement personnel avec celui professionnel exige une redéfinition des usages et une inversion de la relation employeur/salarié parfois unidirectionnelle.

Les usages des terminaux mobiles d'abord concentrés sur la consultation des données et de la messagerie, nécessitent l'implémentation de mesures de protection classiques similaires au PC.

Le changement ici résulte du fait que le salarié ou l'agent devra, en quelque sorte, accepter cette incursion dans son terminal « intime ».

Plusieurs facteurs incitent à fluidifier ces relations nouvelles. Comme nous l'avons déjà dit, le BYOD est un mouvement dont le salarié lui-même est l'initiateur, car cela lui profite.

Ensuite, le DSI pourra définir des niveaux de garanties propres à rendre son intervention acceptable, s'agissant d'une intervention sur un matériel personnel.

En tout état de cause, la démarche devra faire l'objet d'une information claire, explicite et non équivoque, afin de remplir les exigences du droit d'accès.

Il peut en être ainsi de l'établissement qui conserve des données sur le terminal de son personnel. La faculté de suppression de ces données à distance devra faire l'objet d'un encadrement précis, en cas de pertes d'informations, de vol, d'absence du salarié.

De la même manière, les fuites d'informations (ces risques existaient pour la messagerie), ou plus largement la cybercriminalité (attaques, intrusions, infections) impliquent des mesures quant à l'habilitation des droits, l'authentification de l'utilisateur, le filtrage web.

De manière générale, la sécurisation des données du SI se fait selon deux méthodes que sont :
- le silo applicatif dans lequel une sphère professionnelle sécurisée est introduite dans le terminal personnel ;
- la gestion de flotte dans laquelle l'entreprise ou l'entité publique garde la main sur les terminaux (solutions de type Mobile Device Management ou Mobile Device Security).

Les risques organisationnels et RH quant à eux, touchent plus directement la protection des salariés et sont appréhendés par le droit social numérique.

Principes et règles applicables

L'absence de disposition d'ordre législative, règlementaire ou jurisprudentielle dans le BYOD n'est pas synonyme pour autant de « no man's land » juridique.

Un grand nombre de principes et de règles applicables dans la cadre des TIC représentent un socle légal servant de guide qu'il convient d'interpréter et d'adapter à la situation du BYOD.

Tout d'abord les institutions représentatives du personnel peuvent créer des cellules dédiées à la mise en place du BYOD. Le CHSCT qui concourt à l'amélioration des conditions de travail s'occupera plus spécifiquement des transformations organisationnelles importantes de l'entreprise.

La traçabilité, la géolocalisation l'accessibilité par l'employeur au matériel personnel et plus généralement la surveillance de l'utilisateur (du salarié ou de l'agent), devront être encadrées notamment par la mise à jour ou la réalisation d'outils de gouvernance, charte des systèmes d'information, guide de contrôle, guide et livret d'utilisation du système d'information, charte administrateur, guides des opérations de contrôle. Cette solution éprouvée demeure efficace pour dresser les droits et les obligations de chacun.

La charte éthique ou le code des bonnes pratiques pourront former un maillage efficace avec la charte d'utilisation des systèmes d'information à la fois pour véhiculer les intentions de l'entreprise dans l'utilisation de ces modalités de travail et appréhender le curseur que la société ne souhaite pas dépasser.

L'architecture social devient une posture efficace et forme un ensemble de dispositions souvent efficaces contre les litiges nés de supposés stress au travail, hyper connectivité, travail supplémentaire.

Le contrat de travail ou l'avenant doit aussi permettre de colmater et de sécuriser des aspects essentiels des relations engendrées par le BYOD, s'agissant :

- de la responsabilité de l'employeur (usage illicite du salarié, acte de concurrence déloyale) ;
- du lien de subordination (dont le BYOD pourrait être le prétexte à une extension déformation du contrat de travail);
- de la discrimination (pourquoi autoriser un groupe et pas un autre) ;
- confidentialité et sécurité (perte, vol, limitation de préjudice en cas d'erreur de l'administrateur sur données personnelles.).

En conclusion le BYOD impose des défis importants au DSI et aux RH qui doivent pour les premiers adapter leur infrastructure, pour les seconds sécuriser les nouvelles modalités d'exécution du travail. La conduite du changement se révèle une composante essentielle à la réussite de ce projet, ou déjà le CYOD (Choose Your Own Device) apparaît comme une solution de compromis. L'entreprise prend en charge l'équipement mobile des salariés en leur donnant un choix de terminaux et d'OS sur un catalogue prédéfini, donc avec des configurations conformes au SI.

Pour en savoir plus :

- **Très haut débit mobile** : http://www.alain-bensoussan.com/avocats/projet-de-lignes-directrices-ue-pour-developper-les-reseaux-a-haut-debit/2012/06/18
- **Fléxisécurité** : Accord national interprofessionnel du 11 janvier 2013 sur le nouveau modèle économique et social au service de la compétitivité des entreprises et de la sécurisation de l'emploi et des parcours professionnels des salariés.
- **Télétravail** : http://www.alain-bensoussan.com/avocats/le-teletravail-surgit-enfin-dans-le-code-du-travail/2012/04/05
- **Vie privée résiduelle** : Cass. Soc., 2 oct. 2001, n°99-42.542 ou *Arrêt Nikon*.
- **Présomption d'usage professionnel** : Cass. Soc. du 19 mai 2004, n°03-83.953
- **Les exigences du droit d'accès** : La loi du 6 janvier 1978 modifiée, en ses articles 39, 41 et 42, pose le principe de droit d'accès selon lequel toute personne justifiant de son identité a le droit d'interroger le responsable d'un fichier ou d'un traitement pour savoir s'il détient des informations sur elle, et le cas échéant d'en obtenir communication.
- **L'authentification de l'utilisateur** : Le principe peut être une authentification à deux facteurs identifiant plus code sms par connexion. Le contrôle de l'accès par VPN peut être simplifié.
- **Le filtrage web** : Le filtrage contrôle le flux de données sur le réseau de l'entreprise qui peut être combiné à un proxy
- **La traçabilité** : http://www.alain-bensoussan.com/avocats/juristendance-informatique-et-libertes-novembre-decembre-2012/2012/11/20
- **Guides des opérations de contrôle** : http://www.alain-bensoussan.com/avocats/guide-et-operations-de-controle-et-maitrise-de-lenquete-numerique-interne/2012/09/29

Emmanuel Walle
Avocat, Directeur du département Social numérique

Alain Bensoussan-Avocats est un cabinet d'avocat entièrement dédié au droit des technologies avancées depuis 1978. Pour la 3e année consécutive depuis 2010, il a été distingué par ses pairs, « Best Lawyer » de l'année dans le domaine du Droit des nouvelles technologies.
Site : http://www.alain-bensoussan.com/