Avis d'expert : BYOD, quand le monde du grand public s'invite dans le monde professionnel

Le BYOD (*Bring Your Own Device*), tendance à fusionner l'utilisation de son propre terminal (tablette, PC portable, *smartphones*) avec un usage d'entreprise, soulève des questions au-delà de l'aspect technique. Il amène nécessairement à réfléchir de façon globale à l'organisation de l'entreprise. Un avis d'expert proposé par **David Remaud**, responsable offre chez SPIE Communications.

La dénomination marketing laisse place à un réel phénomène

Le terme BYOD est né de la prolifération des équipements *high-tech* (*netbooks*, tablettes, *smartphones*) et de leur adoption pour un usage professionnel. Les utilisateurs séduits par la simplicité d'usage de leurs nouveaux terminaux ne peuvent plus s'en passer. L'explosion de leur utilisation brouille ainsi la barrière entre équipement personnel et professionnel. Le phénomène s'accentue en France depuis la fin de l'année 2010 avec l'entrée massive sur le marché du travail de la génération Y. Technophiles exigeants, les jeunes nés entre le début des années 1980 et le milieu des années 1990, tendent de plus en plus à utiliser leurs outils informatiques personnels dans la sphère professionnelle.

Si dans certaines entreprises outre-Atlantique, l'ordinateur de bureau est en phase d'être totalement remplacé par l'équipement personnel, le BYOD accuse un certain retard en France. Les Français conçoivent encore le BYOD comme un moyen d'enrichir les outils déjà mis à leur disposition par l'entreprise leur permettant d'améliorer leur disponibilité, leur performance et même leur image (lecture des *emails* dans les transports grâce au *smartphone*, présentation à l'aide d'une tablette, etc.). Mais ce retard pourrait bien se combler rapidement, porté par la dynamique de la consumérisation.

Quels nouveaux enjeux pour l'entreprise ?

Le problème majeur soulevé par le BYOD **est celui de la sécurité**. Banaliser l'autorisation des équipements personnels remet en cause le contrôle de l'accès au système d'information. Il est alors primordial pour la DSI de prendre en compte ces nouveaux usages dans leur politique globale de sécurité et en portant leur attention sur :

– le contrôle de l'accès au réseau d'entreprise (authentification, droits, intégrité…) ;

– la sécurité du terminal lui-même (protection anti-x, chiffrement…) ;

– la gestion du parc de terminaux mobiles (applications, données…).

De plus, avec l'arrivée du BYOD en entreprise, l'évolution des infrastructures réseau sans fil (en couverture et capacité) est à prendre en compte, car certains terminaux comme les tablettes ne possèdent que ce moyen de connexion au réseau.

L'investissement peut donc **se révéler significatif** pour des entreprises qui n'auraient pas encore déployé de réseau sans fil dans tous les bâtiments ainsi que les solutions de sécurité adaptées.

En revanche, des entreprises peuvent trouver un intérêt dans l'optimisation budgétaire générée par le BYOD. L'utilisation banalisée des terminaux peut permettre de réduire les coûts liés à leur exploitation si l'entreprise choisit de rendre l'utilisateur autonome dans la gestion de son équipement.

En contrepartie, une notion de forfaitisation de l'équipement se développe également en entreprise. L'employé achète le matériel répondant le plus à ses attentes, quelle que soit « l'enveloppe » donnée par l'entreprise. Il en résulte une plus grande satisfaction de l'utilisateur, rendu « libre » dans le choix de ses outils et une simplicité de gestion des investissements.

Réussir à intégrer le BYOD en entreprise pour ne pas le subir

Un des enjeux du BYOD est de permettre l'accès à toutes les applications du système d'information de l'entreprise. Nombreuses applications sont dorénavant accessibles au moyen d'un simple navigateur, ce qui les rendent ainsi compatibles avec la majorité des équipements et OS existants. Pour celles nécessitant l'utilisation de clients logiciels dits « lourds », la virtualisation du poste de travail peut s'avérer une alternative efficace et permettre en l'occurrence de répondre aux problématiques de portabilité et même de sécurité.

Au-delà de l'aspect sécuritaire, le BYOD n'est pas sans conséquence **sur l'organisation du travail** et notamment du télétravail. Le BYOD ne révolutionne pas le télétravail, déjà largement utilisé grâce à Internet et aux PC portables, mais il modifie le comportement des salariés. La séparation entre sphère privée et sphère professionnelle est encore plus diffuse lorsque l'on utilise le même terminal. L'employé est à même de se connecter sur ses outils de travail professionnels à tout moment. Dès lors, faut-il compter le temps de travail passé sur des terminaux secondaires ?

De plus, pour éviter l'hyperconnectivité souvent source de stress, managers et collaborateurs devront veiller à respecter un cadre de travail pour l'utilisation des outils informatiques.

Il peut parfois aussi s'avérer important de ne pas essayer d'imposer des standards sur les équipements personnels, qui restent par définition choisis et configurés selon la volonté de l'utilisateur. Il faut alors veiller à ne pas créer de discrimination entre les collaborateurs qui peuvent/veulent acheter un *smartphone*, une tablette ou un PC portable et les autres.

L'aspect juridique doit également constituer un axe majeur dans la mise en place d'une politique BYOD. En termes de politique interne, il est judicieux de réviser la charte de bon usage des moyens informatiques, en complément du règlement intérieur. Les notions d'assurance et de responsabilité de l'équipement et des données qu'il contient sont aussi à envisager. Quelle procédure, quelle solution si le matériel contenant des informations professionnelles est endommagé ou volé avec des informations confidentielles ?

Les questions sur le BYOD sont donc nombreuses, mais les réponses actuellement incertaines. Comme tout nouveau phénomène issu de la société et de ses pratiques, ce changement sera progressif et nécessitera d'être encadré au sein des entreprises. Par ailleurs, pour rendre leur

système d’information toujours plus flexible, les entreprises vont devoir intégrer cette nouvelle tendance dans les plans de transformation de leurs infrastructures et leurs applications.

Crédit photo : © SPIE Communications