Utiliser des appareils privés pour le travail? Oui mais…

L'entreprise qui envisage d'autoriser les employés à utiliser leurs appareils privés à des fins professionnelles doit au préalable se poser une série de questions de nature financière, sécuritaire et juridique, avertissent les spécialistes du domaine.

PIERRE CORMON

De plus en plus d'entreprises de toutes les tailles autorisent leur personnel à utiliser leurs propres appareils (smartphones, tablettes, etc.) à des fins professionnelles. Selon les cas, elles fournissent une carte SIM à leurs employés ou les laissent utiliser les leurs. C'est ce qu'on appelle le BYOD (*bring your own device:* apportez votre propre appareil). Les collaborateurs sont souvent à l'origine du BYOD, car ils se sentent plus à l'aise avec des appareils qu'ils ont choisis. «Le BYOD est une question à laquelle on ne peut pas échapper», estime Stephan Zwettler, directeur de SZ Informatique, une entreprise de conseils et de services. «Si vous ne décidez rien, des employés vont spontanément commencer à utiliser leurs propres appareils à des fins professionnelles. Vous pouvez l'interdire de manière générale, mais si le directeur demande une exception, ce sera difficile de la lui refuser.»

Attention! Si cette politique comporte des avantages, elle pose des questions juridiques, financières et de sécurité.

Les coûts

Une politique de BYOD peut sembler avantageuse: l'employeur n'a plus à acquérir les appareils et, le cas échéant, les abonnements téléphoniques. Il n'a plus à s'occuper du parc d'appareils et des mises à jour. Et du moment que le collaborateur utilise ses équipements en partie à titre privé, il paie en principe une partie de leur coût. C'est cependant une vue un peu courte, avertit Toni Lazazzera, fondateur de la société de conseil informatique Tmanco. «Trop souvent, quand le département informatique choisit un nouveau système, il ne se rend pas compte des coûts qu'il peut engendrer ailleurs», explique-t-il. «Chacun cherche à optimiser les dépenses de son département de manière cloisonnée, sans disposer d'une vision globale.»

Si l'entreprise adopte une politique BYOD, le département juridique, par exemple, devra veiller à ce que les questions légales soulevées par la pratique soient résolues (lire ci-dessous). Le département des ressources humaines devra adapter les contrats de travail. Les problèmes d'incompatibilité entre les systèmes risquent de faire augmenter les coûts du support informatique. Si les employés utilisent leur propre carte SIM, ils obtiendront de moins bonnes conditions que si c'est l'entreprise qui contracte les abonnements. Les employés passeront du temps à remplir des notes de frais pour leurs communications professionnelles. Le département comptabilité passera du temps à les traiter.

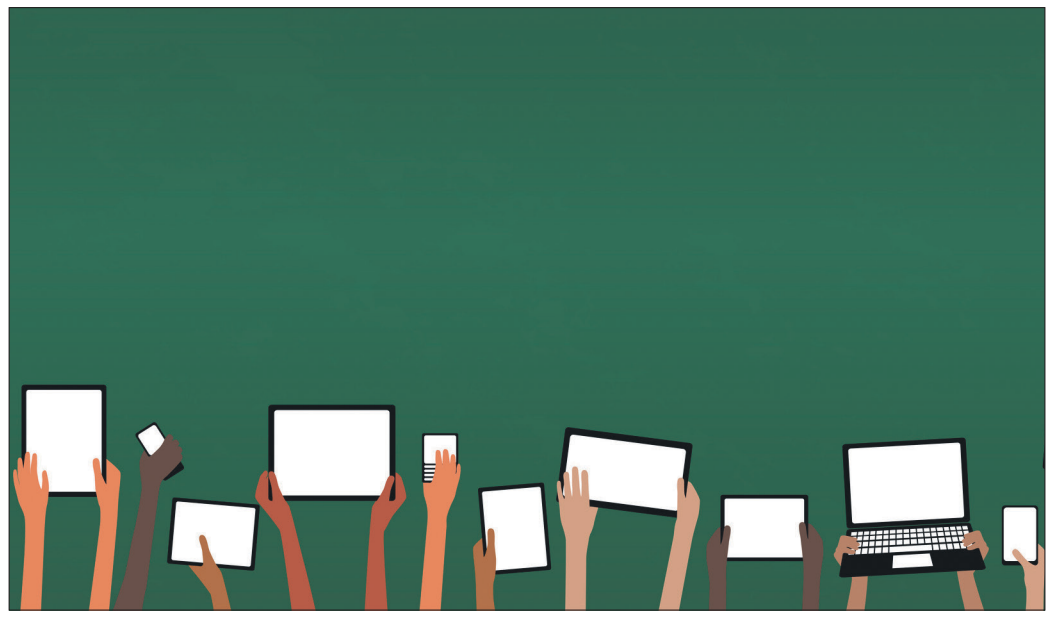
Le cabinet de conseils étasunien Aberdeen qualifie donc le BYOD d'illusion d'économies. «Si l'adoption du BYOD est dictée par une culture d'entreprise qui doit primer sur les coûts, on peut comprendre», synthétise Toni Lazzazera. «Mais si vous le faites pour faire des économies, il convient de bien peser tous les éléments, sans quoi cela peut se retourner contre vous.»

Les problèmes de sécurité

A partir du moment où les employés utilisent des appareils portables, que ce soit en BYOD ou pas, le risque que des données soient perdues ou volées augmente sensiblement. Il faut donc définir une politique de sécurité rigoureuse.

«Il faut commencer par se demander qui a besoin d'avoir accès à ses données professionnelles à distance», précise Stephan Zwettler. «On peut limiter cette possibilité à certaines données (mails, contacts, agendas, etc.) ou personnes (des chefs de projets, des directeurs, par exemple). Si les appareils contiennent des données sensibles, il est également indispensable d'installer une solution technique pour gérer les appareils mobiles. C'est ce qu'on appelle le *mobile device management* (MDM).»

Un MDM est un programme qui fournit un tableau de bord permettant de régler et de commander les appareils mobiles à distance. On peut par exemple installer ou désinstaller une application ou prévoir que, dans telle ou telle situation (perte, vol), le contenu sera effacé automatiquement.



LES EMPLOYEURS *qui autorisent leurs employés à utiliser leur propres appareils à des fins professionnelles pratiquent le BYOD, ou* bring your own device.

Quid des données privées des collaborateurs? «Toutes les solutions MDM modernes permettent de segmenter l'appareil avec une zone privée et une zone professionnelle», répond Yoann Le Corvic, Senior security engineer chez e-Xpert Solutions SA. «En fonction de la politique d'entreprise, l'impact sur la vie privée peut être limité.»

«Mais installer un MDM ne suffit pas», prévient Mickael Mortier, architecte sécurité et systèmes au sein de la société de sécurité informatique Kyos. «Il faut l'accompagner d'autres mesures.» Il faut que les utilisateurs soient sensibilisés aux questions de sécurité et à la politique que l'entreprise a adoptée en la matière. Il faut également préserver la sécurité du système. L'entreprise pratiquant le BYOD ne peut pas contrôler l'utilisation privée de l'appareil d'un employé comme elle le fait avec les appareils professionnels et le risque qu'une application infectée soit téléchargée augmente. «Chaque fois qu'un appareil demande un accès au système d'information ou au réseau d'entreprise, celui-ci doit vérifier qu'il ne présente pas de risques de sécurité», explique Mickael Mortier. «Si ce n'est pas le cas, il peut l'isoler le temps que le problème soit résolu.»

Enfin, comme l'employé peut accéder au système d'information de l'entreprise, «il convient de maintenir un niveau de contrôle d'accès au système d'information identique à celui en place pour les technologies traditionnelles», remarque Yoann Le Corvic. «Il faut privilégier si possible des authentifications fortes ne reposant pas uniquement sur un mot de passe.»

Les questions juridiques

Le BYOD soulève toute une série de questions juridiques, par exemple:

⇨ L'employeur ne peut pas imposer une politique de BYOD contre la volonté des employés au moyen d'une instruction unilatérale, remarque la dernière *newsletter* de l'étude d'avocats Schellenberg Wittmer. De manière générale, l'utilisation d'appareils privés à titre professionnel requiert le consentement tant de l'employeur que de l'employé, précise l'avocat Sébastien Fanti dans un article très complet sur le BYOD[1].

⇨ Si l'employeur met en place une politique de BYOD, il doit indemniser les collaborateurs pour leurs acquisitions de matériel, remarque Sébastien Fanti, à moins que les deux parties en aient convenu autrement, ce qui devra faire l'objet d'une modification du contrat de travail. Il doit également rembourser en totalité les frais encourus par le collaborateur pour les charges variables engendrées par les appels et le trafic de données effectués à titre professionnel. «Des tarifs fixes sont souvent appropriés», remarque la *newsletter* de Schellenberg Wittmer. «L'employé devrait généralement avoir le droit de demander le remboursement proportionnel des frais d'abonnement. Par opposition, une contribution aux frais d'amortissement ne se justifie pas, car la vie utile d'un appareil dépend principalement du développement de la technologie et non pas de l'étendue de l'utilisation professionnelle.»

⇨ L'employé ayant accès à ses documents professionnels depuis ses propres appareils risque de ne plus savoir arrêter de travailler. Or, l'employeur doit protéger la personnalité du travailleur et donc l'empêcher de se surmener. «Aux fins d'éviter de tels risques dans le cadre du BYOD, il pourrait être envisagé de bloquer l'accès à l'espace dédié aux utilisations professionnelles en dehors des heures travaillées et pendant le temps non travaillé (week-end, jour férié, vacances, etc.)», écrit Sébastien Fanti.

⇨ Le salarié doit être informé de manière complète et donner son accord formel avant que l'employeur installe un MDM, estime Sébastien Fanti. Des règles strictes doivent être adoptées pour éviter que ce système n'enfreigne la sphère privée du collaborateur. Techniquement, la meilleure solution est de prévoir des espaces strictement séparés sur l'appareil pour les usages professionnel et privé. ■

[1] *Sébastien Fanti*, Bref aperçu des aspects légaux du BYOD (Bring Your Own Device), *in Internet au travail, Genève, Schulthess éd. romandes, 2014, pp.165-203.*

Combien coûte un MDM?

Les systèmes de *mobile device management* (MDM) peuvent être loués ou achetés. Leur prix dépend de la taille de l'installation et des fonctionnalités requises. «Pour l'achat de licences, il faut compter entre trente et deux cents francs par appareil ou utilisateur, selon les produits et les fonctionnalités souhaitées», estime Stephan Zwettler. «A cela vient s'ajouter l'infrastructure (entre dix mille et vingt mille francs), l'installation et les prestations de mise en place et de formation (entre dix mille et trente mille francs). Enfin, il faut ajouter un coût de maintenance annuel de dix à cinquante francs par appareil ou par utilisateur.» «En mode SAAS (produit loué sans aucune installation nécessaire dans l'entreprise), il faut compter de vingt à cent cinquante francs annuels par appareil ou par utilisateur. A cela il faut ajouter environ cinq mille francs de prestation de mise en place, de configuration et de formation. Cette formule convient très bien pour une PME aux besoins standard de sécurité.»

Une autre approche: le TEM

Si certains voient le BYOD comme moyen de réduire les coûts, Toni Lazazzera promeut une autre approche: la gestion globale des dépenses de télécommunication (ou TEM, *Telecom expense management*). Le TEM vise à donner un tableau de bord de ces outils et des indicateurs simples et facilement exploitables pour gérer les dépenses. Ses avantages? D'abord, l'outil permet de réduire massivement le nombre de factures de son opérateur – une facture suffit plutôt qu'une par centre de coût ou par site. Le TEM permet également d'obtenir des rapports précis sur les coûts engendrés par tel utilisateur ou par tel département. Pas forcément dans un esprit de contrôle: on peut aussi miser sur l'autodiscipline.

«Un collaborateur peut par exemple charger beaucoup de données avec son smartphone, alors que son abonnement de base ne comprend pas le chargement», explique Toni Lazazzera. «Cela engendre des factures substantielles et il ne s'en rend pas forcément compte. Mais une fois qu'il s'en aperçoit, il peut adapter ses habitudes. A l'Aéroport International de Genève, lorsqu'on a introduit ce type de rapports individualisé, les coûts ont subitement chuté de moitié.»