Les enjeux opérationnels du Bring Your Own Device

Le 19 juin 2012, Kurt Salmon, en partenariat avec le cabinet d'avocats Féral-Schuhl / Sainte-Marie, recevait dans ses locaux une vingtaine de clients conviés à une réflexion sur le thème des enjeux opérationnels et juridiques du Bring Your Own Device (BYOD).

Nadjim Aït-Meddour, Associé chez Kurt Salmon, a interrogé Philip Bessière, Senior Manager, Jean-Philip Vial, Manager et Olivier de Courcel, Avocat associé du cabinet Feral Schuhl-Sainte Marie, sur cette tendance dont les implications suscitent nombre d'interrogations chez les décideurs informatiques. Réponses sur un des sujets les plus délicats du moment.

Le BYOD : définition et conséquences

Le BYOD, qui s'inscrit dans le thème de la mobilité, est le principe qui consiste pour les employés à utiliser leur matériel personnel (ordinateur, tablette, smartphone) pour un usage professionnel.

D'un point de vue opérationnel et technique, il s'agit d'une transition entre une situation où la frontière entre le monde personnel et professionnel était matérialisée par des équipements distincts, à un contexte où celle-ci est maintenant de type «logique» (présence de données personnelles et professionnelles sur un même équipement).

D'un point de vue juridique, il constitue un renversement de perspective : alors que jusqu'à présent les entreprises devaient encadrer l'utilisation de l'équipement professionnel par leurs employés à titre personnel, elles doivent maintenant définir le champ possible de leur propres interventions sur du matériel appartenant aux employés.

Facteurs à l'origine de la tendance

L'inclination des employés à utiliser leur matériel personnel est sous-tendue par plusieurs facteurs :

- la maturité technologique d'abord, qui a rendu accessible au plus grand nombre des innovations autrefois réservées aux seules entreprises : matériel, connexions haut-débit et sans fil, applications locales ou virtualisées

- l'explosion de l'équipement grand public : la « consumérisation » de l'informatique a fait entrer dans les foyers des ordinateurs portables, des smartphones et des tablettes dont le niveau de sophistication et de performance surpasse largement celui de l'entreprise

- une mutation vers les usages mobiles et connectés renforcés par un effet de génération, qui se traduisent dans l'entreprise par une surutilisation du mail, l'édition intensive de documents électroniques, et un recours fréquent à la téléconférence audio ou vidéo

L'apparition de nouveaux risques

L'introduction d'appareils personnels dans le monde de l'entreprise n'est néanmoins pas anodine. Sur le plan financier, la latitude laissée aux employés dans le choix de leur équipement peut aboutir à des coûts supplémentaires sur les activités de support, si celles-ci ne sont pas clairement délimitées pour pouvoir maîtriser l'hétérogénéité du parc qui en résulte.

L'absence de frontière nette entre la vie et privée et professionnelle peut aussi aboutir à un accroissement des risques psycho-sociaux : si la présence d'outils professionnels sur un équipement personnel peut améliorer la productivité, elle peut aussi résulter en une augmentation du stress induit par la poursuite du travail en dehors des repères habituels de l'entreprise.

Ainsi, selon une étude d'IDC et Bouygues Telecom, 61% des personnes équipées d'un smartphone déclarent « télétravailler », alors que le niveau de télétravail officiel, soumis à une réglementation très encadrée en France, n'est que de 9%.

Le BYOD tend à renforcer ce télétravail caché en augmentant dans le temps et dans l'espace l'introduction dans la sphère privée des sollicitations d'ordre professionnel : s'il est facile d'éteindre son téléphone mobile d'entreprise en sortant du bureau, il l'est moins de ne pas répondre à son patron sur son téléphone privé, par exemple au restaurant ou sur la route des vacances.

Il en résulte donc pour les entreprises un risque sur la réclamation d'heures supplémentaires pour les salariés soumis à ce régime. La jurisprudence indique en effet qu'en cas de litige, elles sont susceptibles d'être réclamées dans le cas où l'employeur ne pouvait pas ignorer qu'elles étaient effectuées (par exemple dans le cas d'emails envoyés tard).

La possibilité et l'incitation à effectuer du travail à distance peuvent amener également l'employeur à des entorses de fait à la législation du travail sur le temps de repos minimum. Le contexte créé est d'autant plus délicat à adresser dans le cas des cadres au forfait, qui disposent d'une plus grande autonomie, notamment dans l'organisation de leur temps de travail.

Enfin, en cas d'installation sur un équipement personnel d'un système de géolocalisation, même s'il est nécessaire à la mission de l'employé, ou de toute autre application qui permet de contrôler l'activité de celui-ci, l'employeur doit veiller à informer tant les instances représentatives du personnel que les employés eux-mêmes.

Les problématiques de mise en œuvre et comment les accompagner

Pourvu de mettre sous contrôle les risques évoqués, les avantages pour l'entreprise et le salarié restent manifestes. La mise en œuvre du BYOD doit s'accompagner d'une démarche autour de ses trois problématiques principales

1. Définir le périmètre cible

L'entreprise devra segmenter et définir les populations cibles de sa politique BYOD afin de privilégier les populations dont les usages mobiles sont avérés : en priorité, le top management, les forces commerciales, les cadres en situation de mobilité.

Ces populations sont les plus à même de demander à bénéficier des avantages du BYOD, par rapport à des fonctions plus sédentaires, dont les usages ne nécessitent peu ou pas de mobilité (comptables, contrôleurs de gestion, développeurs,...).

L'étude des populations cible doit amener les décideurs à identifier leurs objectifs, qui détermineront si leur politique BYOD est basée sur le volontariat ou l'incitation ; et à se demander s'ils doivent et peuvent imposer le BYOD à tous les utilisateurs de leur entreprise : si la législation oblige les employeurs à fournir à ses employés les moyens de travail, c'est l'objet de la mission qui fonde la différence éventuelle d'attribution entre les employés.

Si une incitation est souhaitée, elle impliquera probablement une contrepartie financière de la part de l'employeur. Celle-ci ne sera pas nécessairement requise si la politique de BYOD se fonde sur le volontariat et si les outils nécessaires à la réalisation de la mission sont fournis par ailleurs.

2. Limiter le parc des appareils et assurer le support

Si l'entreprise ne peut imposer un matériel donné (ce qui serait contraire au choix de leur équipement laissé aux employés), elle peut cependant définir des recommandations afin de limiter le nombre des références à homologuer ou supporter.

Des mesures d'incitation peuvent être prises pour favoriser l'équipement en terminaux « validés » par l'entreprise (ce qui suppose une capacité de veille au sein de la DSI), notamment pour des employés ne disposant pas à titre privé d'équipements de dernière génération. Les services de support peuvent également ne s'adresser qu'à certains types de matériel.

Pour mettre le support sous contrôle, les entreprises peuvent définir différentes stratégies de mise en œuvre, qui peuvent être combinées : limité à une durée fixée par incident (payant au-delà), aux applicatifs (excluant les terminaux), soumis à un seul engagement de moyen, self-care (outils d'autodiagnostic et mise à disposition de ressources en ligne), obligation de souscription à un contrat de support. Il peut être également envisagé d'externaliser le support à un opérateur téléphonique, assurant déjà celui-ci sur un grand nombre de terminaux.

Enfin, il incombe au support de mettre en œuvre des moyens techniques afin de vérifier que les terminaux personnels respectent effectivement les obligations prévues dans la charte BYOD. D'une façon plus générale, dans tous les cas où ses services auront accès au contenu de l'équipement personnel de l'employé (prise de contrôle à distance, effacement de données, etc...), le consentement préalable des employés paraît indispensable. L'entreprise devra veiller à en garder la trace écrite.

3. Sécuriser et garder le contrôle des données

L'entreprise se doit dans ce nouveau contexte de conserver la propriété et la sécurité de ses données. Plusieurs points d'attention doivent être considérés :

- L'utilisation par l'employé d'un outil de travail personnel ne doit pas venir appuyer une revendication individuelle de droits d'auteur ou de droits de propriété industrielle en contradiction avec le contrat de travail et la mission éventuellement créatrice ou inventive confiée au salarié ;

- la présomption de caractère professionnel s'applique à l'utilisation de la messagerie d'entreprise ainsi qu'aux autres données sauvegardées sur un ordinateur fourni par celle-ci, mais elle ne s'appliquera pas sur un équipement appartenant à l'employé, ce qui pourrait faire obstacle à l'obtention de preuves en cas de litige.

Si la jurisprudence ne fournit pas encore toutes les réponses, une séparation claire et explicite entre les données personnelles et professionnelles sur le même équipement devrait néanmoins faciliter la prévention des litiges.

La sécurité des données d'entreprise sur un équipement personnel doit être assurée en les soumettant aux mêmes exigences que celles s'appliquant au matériel d'entreprise : cloisonnement, sauvegarde, présence d'un certificat, chiffrement, effacement à distance. Le cloisonnement des données et des applications d'entreprise à l'intérieur du terminal constitue donc un prérequis fondamental à la mise en œuvre réaliste d'une politique BYOD.

La technologie et ces nouveaux usages devançant la législation, il revient aux entreprises de mener une réflexion afin d'adopter une position en réponse aux questions principales qui se posent : à qui appartiennent quelles données ? Comment procéder en cas de perte ou vol du matériel et données, involontaire ou non ? Quelles sont les données à caractère personnel nouvelles auxquelles l'employeur va accéder ?

La charte BYOD : un élément clé de la politique

Pour établir et partager les droits et les obligations de l'employé et de l'entreprise, la charte BYOD constitue un élément clé de la démarche. Elle peut être une extension de la charte informatique existante, et également l'occasion de réviser celle-ci afin d'y intégrer les évolutions récentes.

Quel que soit le format, la charte aura pour objet de définir un cadre d'utilisation responsable, dans lequel seront précisés les conditions d'usage des appareils personnels en intégrant la ségrégation des données privées et professionnelles. Son élaboration doit être faite de manière concertée entre la direction informatique, les instances représentatives du personnel et les représentants des utilisateurs au sein des différents métiers les plus susceptibles de recourir au BYOD. De par le Code du travail une certaine publicité doit être assurée à la charte. Au titre de ses obligations légales l'entreprise devra également, le cas échéant, mettre à jour ses déclarations CNIL et veiller au respect des prescriptions de la Loi informatique et libertés.

En conclusion : anticiper pour ne pas subir

L'enjeu principal du BYOD pour l'entreprise est d'anticiper et d'accompagner la tendance, au risque sinon de la subir. Si 60% des entreprises françaises autorisent l'utilisation de terminaux privés selon une étude NetMediaEurope, peu d'entre elles ont mis en place une politique réellement réfléchie d'encadrement des nouveaux usages qui en découlent.

Si le BYOD a souvent pour origine la motivation de quelques passionnés de nouvelles technologies, la banalisation des équipements mobiles individuels et leur utilisation dans un contexte professionnel ne semble pas être un effet de mode. Il s'agit plutôt d'une transformation des usages impliquant une modification de la manière dont les entreprises doivent envisager l'équipement de leurs salariés.

Au delà de l'adaptation nécessaire de celles-ci pour conserver la sécurité de leurs données, les bénéfices à en retirer ne sont pas négligeables : augmentation de la satisfaction des employés, productivité accrue, économies potentiellement importantes sur les coûts… autant de raisons de traiter le sujet comme une opportunité, et d'en faire une force.

Olivier Faivre, Consultant Senior Kurt Salmon

Contacts :

Nadjim Ait-Meddour
Associé
nadjim.ait-meddour@kurtsalmon.com
Tél.: +33 1 55 24 31 03

Philip Bessiere
Senior manager
philip.bessiere@kurtsalmon.com
Tél.: +33 1 55 24 33 43

Jean-Philippe Vial
Manager
jean-philippe.vial@kurtsalmon.com
Tél.: +33 1 55 24 35 45

Olivier DE COURCEL
Avocat Associé Feral-Schuhl / Sainte-Marie
Tél.: +33 1 70 71 22 02
odecourcel@feral-avocats.com