Le Bring Your Own Device face au droit du travail

publié le **06/03/2013**, vu **3347 fois**, Auteur : Murielle Cahen

Alors que les auteurs s'accordaient encore récemment à dire que le BYOD (« Bring Your Own Device », traduire « Apportez votre propre matériel ») était un flou juridique, l'état du droit a changé avec l'introduction dans le code du travail d'une section intitulée « Télétravail ». Ces dispositions semblent pouvoir s'appliquer utilement au BYOD mais en partie seulement.

L'acronyme désigne une pratique nouvelle qui consiste à utiliser son matériel personnel dans le cadre professionnel, c'est-à-dire pour son travail. Par matériel, il faut évidemment entendre les appareils électroniques, mais surtout les smartphones, les ordinateurs personnels, qui sont les deux moyens de communication les plus fréquemment utilisés dans le monde de l'entreprise, et enfin les clés USB.

Car l'un des problèmes majeurs fréquemment relevés par la doctrine, mais également par les auteurs en général, puisque le débat dépasse largement la sphère juridique, porte sur la sécurisation de l'échange des données. Les failles pour l'entreprise sont multiples lors du recours au BYOD mais ne sont pas insurmontables pour autant, pas plus, en tout cas, que dans le cadre d'un réseau classique.

Face à l'absence de cadre juridique, les entreprises qui optent pour le BYOD s'adaptent pour le moment comme elles le peuvent afin de se prémunir des éventuels risques relatifs à la pratique. Sont en cause principalement les échanges de données qu'il convient de sécuriser, la question de la charge de cette mesure n'étant pas clairement tranchée, pas plus que celle de la responsabilité. De même, l'adaptabilité des matériels utilisés par les employés et les risques qu'ils représentent en termes de fuites d'informations ou d'introduction dans les réseaux des entreprises sont autant de difficultés que les entreprises doivent appréhender en amont d'un éventuel recours au BYOD. Le droit du travail ne vient pas faciliter la tâche puisqu'il impose une séparation entre la vie privée et la vie professionnelle, il conviendra de revenir sur ce point.

La question se pose de savoir comment il est possible pour une entreprise et ses employés de recourir au BYOD tout en limitant la prise de risques et sans déséquilibrer les responsabilités en jeu.

I - Les ressources à la disposition des entreprises face aux risques du BYOD

A - Une sécurisation nécessaire de la pratique

La sécurisation doit viser à prévenir des intrusions externes, les échanges de données aussi bien personnelles que relatives à la société elle-même ou encore à prévenir la fuite de données

confidentielles.

Le risque majeur réside sans doute dans l'intégrité des systèmes informatiques de l'entreprise. Le BYOD suppose que les appareils utilisés peuvent aussi bien se connecter au réseau de l'entreprise qu'à n'importe quel autre. Ils deviennent alors des vecteurs de choix pour des attaques extérieures s'ils ne sont pas correctement configurés et sécurisés. De l'intégrité des systèmes dépend également la préservation de la confidentialité des informations circulant sur le réseau de l'entreprise. Il est également fréquemment recommandé de définir de façon stricte le périmètre de la confidentialité au sein de l'entreprise pour que les informations utilisées par l'employé sur son propre matériel ne dépassent pas cette limite. Le salarié engagera sa responsabilité si une telle fuite d'information surviendrait de son fait ou par sa négligence, mais n'exclut qu'elle soit atténuée si l'employeur n'a pas non plus pris les mesures nécessaires pour prévenir le risque.

Dans le même sens, la CNIL recommande également de veiller à sécuriser les échanges de données personnelles soumis à la loi informatique et liberté. En effet, l'usage de telles ressources par l'employé depuis son terminal personnel présente là encore le risque d'une fuite d'information.

B - Un choix réservé à l'entreprise

Trois cas sont classiquement recommandés par la doctrine en la matière, mais quoi qu'il en soit, il est particulièrement important, dans l'intérêt de l'entreprise, de recourir à l'une de ces solutions. L'entreprise peut soit décider l'interdiction pure et simple du BYOD, soit inclure dans les contrats de travail les stipulations nécessaires ou encore adapter sa charte informatique en fonction du BYOD.

L'interdiction stricte du BYOD est donc possible et peut prendre plusieurs formes. Elle peut tout d'abord être incluse dans le règlement intérieur ou dans la charte informatique, selon les conditions d'adoption imposées par le droit du travail et qui seront exposées ensuite. Elle peut également être stipulée dans les contrats de travail, mais ce qui pose le problème de la modification des contrats existant.

La voie de la négociation est également ouverte aux employeurs en incluant les règles relatives au BYOD au contrat de travail. La faculté est tout à fait possible, mais est soumise à une difficulté, qui serait d'ailleurs la même dans le cas de l'interdiction : les contrats de travail existants devraient alors être modifiés en conséquence. Une modification du contrat de travail ne peut toutefois pas intervenir sans l'accord du salarié ce qui obligerait l'employeur à renégocier individuellement tous les contrats de travail en cours.

Finalement, les chartes informatiques des entreprises sont assimilées au règlement intérieur qui résulte du pouvoir de décision de l'employeur. En pratique, elle devra être annexée au règlement intérieur et répondra aux règles de validité de celui-ci et qui sont prévues par l'article L1321-4 du code du travail.

II - L'applicabilité des principes du droit du travail au BYOD

A - L'applicabilité partielle des dispositions sur le télétravail

La loi Warsmann du 22 mars 2012 inclut dans le code du travail une section intitulée « Télétravail » dont les trois articles, L1222-9 à L1222-11, comportent plusieurs dispositions importantes du point de vue du BYOD. Néanmoins, le BYOD n'est pas directement visé par ces dispositions et il faudra attendre que les juges se prononcent sur l'étendue de leur applicabilité.

Quoi qu'il en soit pour le moment, l'article L1222-9, étant rédigé dans des termes généraux, nous apprend deux choses importantes quant à son applicabilité au BYOD. Rien ne s'oppose à ce qu'il s'applique au BYOD dans la mesure où celui-ci permet effectivement l'exécution de son travail par le salarié en dehors des locaux de l'entreprise. Cependant, le BYOD n'est pas systématiquement une « forme d'organisation du travail » au sens du télétravail puisqu'il ne se fait pas forcément « de façon régulière » mais peut être tout à fait incident. En revanche, s'il se fait de façon régulière alors le contrat de travail devrait être modifié et cette modification devrait emporter le consentement du salarié.

De même, si le BYOD se fait de façon régulière, il emporte alors des conséquences pour l'employeur, en plus de l'inscription au contrat de travail. L'article L1222-10 du code du travail prévoit ces obligations et notamment celle, qui n'est pas sans conséquence, « de prendre en charge tous les coûts découlant directement de l'exercice du télétravail, notamment le coût des matériels, logiciels, abonnements, communications et outils ainsi que de la maintenance de ceux-ci ». À n'en pas douter, ces dispositions du code constitueront des avantages substantiels pour les employés recourant habituellement au BYOD.

B - Le principe de séparation entre la vie privée et la vie professionnelle

Les atteintes à la vie privée que peut provoquer le BYOD sont surtout relatives au contrôle du matériel utilisé par l'employé. Comment contrôler un ordinateur utilisé par l'employé dans le cadre de son activité professionnelle, mais dont il serait propriétaire ? Dans un arrêt rendu le 23 mai 2012, la chambre sociale de la Cour de cassation a décidé qu'un employeur ne pouvait contrôler le dictaphone personnel d'une salariée en son absence ou sans l'avoir dûment appelée. L'arrêt est confirmé par un arrêt du 12 février 2013 où elle a jugé qu'un employeur ne pouvait pas contrôler le contenu d'une clé USB personnelle connectée à l'ordinateur professionnel en dehors des mêmes conditions que dans l'espèce précédente.

Le dernier risque du BYOD qu'il convient, pour l'employeur, de prévenir est relatif au temps de travail. Le recours au BYOD ne doit pas revenir à empiéter de façon démesurée sur la vie privée de l'employé. De même, il ne doit pas non plus avoir pour conséquence, d'un point de vue quantitatif, de le surcharger en travail.