Chronique du droit des nouvelles technologies

# Le Bring Your Own Device, un vaste défi juridique

*Toute entreprise, grande ou petite, dépend de l'informatique, domaine sujet à un renouvellement constant. Ces nouveautés techniques entraînent inévitablement de nouvelles questions juridiques impactant le quotidien des salariés et des employeurs. La présente rubrique, à paraître tous les mois, a pour objectif de couvrir les sujets d'actualité et les évolutions en droit des nouvelles technologies au niveau de la législation luxembourgeoise et européenne.*

**Nouvelle façon de percevoir l'organisation de l'IT au sein de l'entreprise, le Bring Your Own Device (ci-après «BYOD») peut être décrit comme le fait pour un travailleur d'utiliser son propre équipement informatique (smartphone, ordinateur portable, tablette électronique, clé-USB, etc.) à des fins professionnelles, plutôt que d'utiliser l'équipement qui lui était jusqu'alors traditionnellement mis à disposition par l'employeur. Le terminal personnel est alors utilisé par les travailleurs afin d'accéder, de stocker ou de traiter des informations appartenant à l'organisation pour laquelle ils travaillent.**

De plus en plus d'entreprises ont recours à un modèle BYOD, sur demande des travailleurs eux-mêmes, ou sur demande de l'entreprise pour des raisons de facilité, par exemple dans un contexte de télétravail. Il n'est ainsi pas rare de voir une organisation supprimer sa flotte entière de Blackberry et de la «remplacer» par un logiciel à installer sur les smartphones personnels de ses travailleurs, afin que ces derniers puissent accéder à certaines informations de l'entreprise, comme par exemple leurs emails professionnels.

Une telle façon de procéder présente de nombreux avantages. Ainsi, outre la diminution des coûts liés à l'achat et à la gestion d'un parc de terminaux mobiles, le BYOD permet généralement d'augmenter la productivité des travailleurs, qui apparaissent plus efficaces sur un environnement informatique qui leur est familier.

Le BYOD est néanmoins également synonyme de risques – techniques et juridiques –, tant pour l'entreprise que pour ses travailleurs (1.). Par exemple, le BYOD amplifie considérablement les risques liés au vol de données confidentielles, à l'atteinte à la vie privée du travailleur ou encore à la violation par l'employeur des dispositions relatives au droit du travail. Bien qu'il soit encore impossible de supprimer purement et simplement ces risques de type juridico-techniques, il existe des manières de parvenir à les réduire au maximum (2.). La technique de conteneurisation, ainsi que la mise en place d'une charte BYOD en font partie.

## 1. De quelques risques technico-juridiques liés au BYOD, pour l'entreprise et pour le travailleur

### La sécurité des réseaux et la confidentialité des données de l'entreprise

Le BYOD présente tout d'abord des risques considérables pour la sécurité des réseaux et des systèmes de l'entreprise. En effet, d'un point de vue technique, les équipements personnels des travailleurs ne présentent pas toujours les mêmes garanties de sécurité que celles offertes par les équipements de l'entreprise. En outre, les terminaux personnels utilisent bien souvent des systèmes d'exploitation hétérogènes, ce qui rend la sécurisation plus compliquée. La potentialité de brèches et d'atteintes au réseau et/ou au système de l'entreprise sont partant plus élevées.

Le BYOD pose ensuite problème au niveau de la confidentialité des données de l'entreprise. En effet, dès lors que le salarié a accès et stocke potentiellement, sur son propre équipement, des données appartenant à l'entreprise, les risques d'atteinte à la confidentialité de ces données, voire de vol de celles-ci, par le travailleur lui-même ou par un tiers, sont également amplifiés.

La question se pose par exemple de savoir ce qu'il se passe en cas de perte de l'équipement personnel du salarié, ou en cas de vol par ce dernier. Une solution pourrait consister en la mise en place par l'employeur d'un système d'auto-effacement («auto-wiping») de la mémoire du terminal. Le risque existe cependant qu'une telle solution efface également le contenu privé du téléphone, ce qui pourrait avoir pour conséquence d'engager la responsabilité de l'employeur.

### La protection de la vie privée

Bien qu'il l'utilise dorénavant à des fins professionnelles également, le travailleur va bien sur continuer à utiliser son terminal à des fins personnelles. Des données professionnelles et privées vont alors se côtoyer sur le même appareil, ce qui constitue une porte ouverte aux atteintes à la vie privée du salarié. Par exemple, afin de sécuriser les appareils personnels, l'équipe IT de l'entreprise va souvent réquisitionner un accès à distance à l'équipement du travailleur.

En outre, dans l'hypothèse où l'employeur désire mettre en place un monitoring afin de veiller à ce que ses données ne soient pas volées, il est souvent difficile de ne pas accéder à des données privées également, un tel accès étant, en principe, interdit.

Un arrêt récent de la Cour de cassation française a néanmoins reconnu le droit à l'employeur d'accéder au contenu d'une clé-USB personnelle du salarié qui était connectée sur l'ordinateur mis à disposition du salarié par l'employeur et qui n'était pas expressément identifié comme privé.

Une telle solution semble pouvoir s'appliquer également à d'autres types de BYOD. Ainsi, dès lors que le terminal personnel du travailleur est connecté au réseau de l'entreprise, l'employeur semble avoir le droit de pouvoir accéder tout contenu dudit terminal qui n'est pas expressément identifié comme étant privé.

### La protection des données à caractère personnel

Le BYOD pose également des questions sur le plan de la protection des données à caractère personnel. Ainsi, les données de nature professionnelle (contrats, listes de clientèle, etc.) – stockées et accédées depuis le terminal privé des salariés – vont presque toujours contenir des données à caractère personnel.

L'employeur, en principe considéré comme responsable du traitement, dès lors qu'il détermine les moyens et les finalités du traitement de ces données, va ainsi devoir mettre en place les dispositifs techniques et juridiques afin de rester en contrôle de ces données et de respecter les obligations qui lui incombent en vertu de la législation applicable sur la protection des données à caractère personnel. Lorsque l'employeur n'adresse pas de manière adéquate les failles de sécurité possibles qui vont de pair avec le BYOD, il risque d'engager sa responsabilité, en ce compris sa responsabilité pénale dans certains cas.

### Les atteintes au droit du travail

Les frontières entre temps de travail et temps libre se réduisent considérablement avec le BYOD. En effet, dès lors que l'employé devient capable de travailler 24 heures sur 24, vacances et weekends compris, il devient compliqué, voire impossible, de respecter les limites légales imposées par le Code du travail en matière d'heures et de jours de travail. En outre, si l'employeur met en place un système de monitoring contrôlant l'utilisation que fait le travailleur de son terminal, les règles strictes du Code du travail et de la législation sur la protection des données à caractère personnel, prévoyant notamment la nécessité d'obtenir une autorisation préalable de la part de la Commission Nationale pour la Protection des Données (ci-après, «CNPD»), devront être observées.

### Le respect de la régulation du secteur financier

Dans l'hypothèse où l'entreprise est active dans le secteur financier, une couche supplémentaire de règles doit être prise en compte dans l'implémentation d'une solution de type BYOD. Dans son rapport annuel 2012, la CSSF a tâché de rappeler les règles qui devaient trouver à s'appliquer en la matière. Ainsi, la CSSF a insisté sur le fait qu'en conformité avec le principe de prudence qui leur est applicable, les professionnels du secteur financier doivent maintenir leur activité sous contrôle, tant d'un point de vue technique qu'opérationnel.

Sur base de cela, la CSSF a tiré une série de conclusions. Parmi celles-ci, on relèvera notamment qu'il est interdit de travailler sur base d'un modèle de télétravail de manière permanente en utilisant le BYOD. De même, sont applicables au BYOD les exigences faites en matière d'accès à distance des emails professionnels (telles qu'énoncées dans son rapport annuel 2005), ou encore les exigences applicables aux accès à distance de manière général (telles qu'énoncées dans son rapport annuel 2007).

Enfin, une institution financière qui veut mettre en place un modèle de type BYOD devra préalablement effectuer une analyse de risques et mettre en place une politique de sécurité.

### La problématique des droits de propriété intellectuelle

Le BYOD peut poser un certain nombre d'interrogations sur le plan du droit de la propriété intellectuelle. À titre exemplatif, les logiciels utilisés en interne par une entreprise (comme par exemple, les logiciels permettant d'accéder aux emails professionnels) sont généralement pris en licence par lesdites entreprises. Une telle licence est bien souvent limitée à certains types de terminaux et à un certain nombre d'utilisateurs. Dans l'hypothèse de la mise en place d'une solution BYOD, l'employeur devra donc veiller à respecter les termes de la licence et à ne pas excéder les limites d'utilisation que cette dernière prévoit.

En outre, bon nombre d'applications disponibles sur Internet sont données en licence gratuitement lorsqu'utilisées à titre privé, mais deviennent payantes lorsqu'elles sont utilisées à titre professionnel, ce qui peut donner lieu à une situation confuse lorsque le terminal privé est également utilisé à titre professionnel, et que lesdites applications sont donc également utilisées sur le terminal privé à des fins professionnelles.

## 2. De quelques «best practices» dans l'implémentation d'un modèle BYOD

### D'une sécurisation technique…

Afin d'éviter une partie des problèmes énoncés ci-dessus – principalement en matière de sécurité des données de l'entreprise et de protection de la vie privée du travailleur –, il est tout d'abord important d'adopter des mesures techniques présentant le plus de garanties possibles en termes de sécurité. En voici quelques exemples.

La prise de mesures de sécurité dites «simples» s'avère tout d'abord être le moins que l'on puisse faire. Ainsi, la mise en place de mots de passe sûrs, d'une protection antivirus adéquate, d'une technique de chiffrement intégral des disques durs, ou encore d'un contrôle des applications installées sur le terminal, sont autant de choses qu'il est indispensable de réaliser.

La mise en place d'un système de «Mobile Device Management» (ci-après, «MDM») par l'entreprise peut également s'avérer être nécessaire. Cet outil précieux, qui permet la gestion à distance d'une flotte entière de terminaux mobiles, rendra notamment possible le blocage ou l'effacement du contenu des terminaux à distance, la réalisation de backups ou la restauration des terminaux, voire même l'installation d'applications à distance.

Enfin, comme l'a recommandé la CNIL – l'autorité française pour la protection des données, la mise en place d'un système de «conteneurisation» peut s'avérer être une solution à privilégier. Une telle technique consiste en le fait de créer un espace hermétique sur les appareils personnels des travailleurs qui contiendra les applications et les usages professionnels. Les contrôles et accès éventuels effectués par l'entreprise sur le terminal privé ne concernent alors plus le terminal dans son ensemble, mais uniquement le compartiment dédié aux opérations professionnelles. Les risques d'atteintes à la vie privée du travailleur, ainsi que les risques de vol des données de l'entreprise, s'en trouvent considérablement réduits.

### …à une sécurisation juridique

Le BYOD n'est jusqu'à ce jour spécifiquement pris en compte par aucun instrument légal. Comme vu plus haut, il pose pourtant bon nombre de risques juridiques, couvrant une multitude de domaines du droit.

Afin de se couvrir au mieux contre ces risques juridiques, la solution classiquement conseillée consiste en la mise en place d'une «charte BYOD». Celle-ci va permettre d'encadrer au maximum l'utilisation du BYOD au sein de l'entreprise, en définissant notamment les droits et les obligations de l'entreprise et de ses travailleurs. Afin d'être pleinement efficace, la charte BYOD va devoir contenir et traiter un certain nombre de points, dont les principaux sont les suivants.

Dans un premier temps, la charte BYOD va devoir régler la question de savoir quels sont les travailleurs de l'entreprise ayant le droit d'utiliser leur terminal personnel selon un modèle BYOD. En outre, la charte BYOD devra également régler la question de savoir quel type de terminal peut être utilisé par les travailleurs dans un modèle BYOD.

Une fois les travailleurs et les terminaux éligibles définis, la charte va devoir définir les obligations de ses travailleurs par rapport au BYOD afin de garantir la sécurité, notamment en termes d'installation de logiciels antivirus ou de pare-feu, en matière d'utilisation de mots de passe particuliers, de confidentialité des obligations qui sont la propriété de l'entreprise, etc.

Si un MDM est mis en place par l'employeur, les travailleurs devront en être informés, et les interactions que pourra avoir ce MDM avec les terminaux privés devront idéalement être décrites.

La charte BYOD sera également l'endroit pour régler des questions d'ordre pratique telles que le partage des coûts de l'utilisation du terminal (coûts d'acquisition, de maintenance, des communications électroniques, etc.), ou la répartition des éventuelles assurances (l'assurance professionnelle couvre-t-elle d'éventuels dommages qui seraient causés au terminal personnel?).

La politique de sécurisation des données de l'employeur devra être décrite dans la charte. Ainsi, s'il a l'intention de mettre en place un système d'effacement automatique des données en cas de perte ou de vol du terminal, cette information devra être présente dans la charte.

La charte BYOD devra également contenir des dispositions en matière d'heures de travail, afin de ne pas dépasser les limites légales que le Code du travail prévoit. Ainsi, la charte pourra par exemple stipuler qu'à partir d'une certaine heure, l'utilisation des applications professionnelles sur les terminaux est interdite. Ceci pourra par ailleurs être accompagné d'une mesure technique visant à couper tout accès aux applications professionnelles sur le terminal personnel après une certaine heure. Une solution identique peut être mise en place concernant les weekends ou les jours de congés.

Si l'employeur désire mettre en place une surveillance de l'utilisation que font ses travailleurs de leur terminal – une telle surveillance ne pouvant être mise en place que dans certains cas strictement définis dans le Code du travail –, la charte devra également traiter de cette question, et des informations particulières sur cette surveillance devront absolument être présentes dans la charte. En outre, l'employeur sera tenu d'obtenir une autorisation préalable auprès de la CNPD en vertu de la législation sur la protection des données à caractère personnel.

La charte BYOD devra enfin prévoir des sanctions en cas de non-respect par les travailleurs de celle-ci.

Afin de rendre cette charte obligatoire pour les travailleurs de l'entreprise, il est important de noter qu'une certaine procédure devra être scrupuleusement respectée. Cette procédure varie en fonction du nombre de travailleurs présents dans l'entreprise concernée.

Ainsi, conformément à l'article L. 414-1 du Code du travail, pour les entreprises employant plus de 15 salariés, une consultation des membres de la délégation sera nécessaire. Leur avis ne sera néanmoins pas contraignant pour l'employeur. Pour les entreprises employant plus de 150 salariés, la mise en place de la charte devra être soumise à l'avis du comité mixte, qui dispose d'un véritable pouvoir de codécision, conformément à l'article L. 423-1 du Code du travail.

Une fois cette procédure d'adoption effectuée, l'employeur s'assurera de remettre un exemplaire de la charte BYOD à chacun de ses travailleurs existants, en plus de l'afficher publiquement dans les locaux de l'entreprise. En outre, une référence directe à la charte BYOD dans les contrats de travail – stipulant que celle-ci fait partie intégrante dudit contrat – conclus avec les nouvelles recrues s'avérera également utile.

## Conclusion

Bien qu'il soit synonyme de bien d'avantages et d'économies pour l'entreprise, le BYOD présente néanmoins une multitude de risques juridiques et techniques. Fort heureusement, il est possible de prévenir ces risques, dans une certaine mesure, par la mise en place de solutions techniques et juridiques.

D'un point de vue juridique, ces risques couvrent un large éventail de domaines, si bien qu'il est conseillé de faire appel à un professionnel du droit afin d'encadrer l'implémentation d'un modèle BYOD dans une organisation, notamment par la rédaction d'une «charte BYOD».

D'un point de vue technique, il est important de garder à l'esprit que la mise en place de solutions techniques vise principalement à prévenir la survenance des risques juridiques. Dès lors, l'aspect légal doit avant tout être pris en compte dans l'implémentation de pareilles mesures. Ainsi, technique et droit doivent être pensés dans une perspective de complémentarité, en matière de BYOD plus qu'ailleurs.

*Vincent WELLENS (cf. portrait)*
*Avocat à la Cour*
*Partner chez NautaDutilh Avocats Luxembourg S.à r.l.*
*vincent.wellens@nautadutilh.com*

*Nicolas RASE*
*Associate chez NautaDutilh Avocats Luxembourg S.à r.l.*
*nicolas.rase@nautadutilh.com*
*www.nautadutilh.com*