BYOD
Un défi juridique à anticiper

Septembre 2013

Cabinet d'Avocats MATHIAS

Le Cabinet Mathias publie ce Livre blanc à destination des entreprises et des administrations, des employeurs comme des employés, tous concernés par le Bring Your Own Device.

Il nous paraît en effet important de partager notre expérience et notre savoir-faire à travers ce guide pratique afin de vous permettre de gérer au mieux les nombreux enjeux juridiques de ce phénomène.

Le Cabinet Mathias conseille ses clients dans le cadre de la réalisation de leurs projets notamment dans le secteur des technologies avancées, de l'Internet, de la propriété intellectuelle et de la protection des données. Nous accompagnons nos clients tant en conseil qu'en contentieux.

Résumé

Le Bring Your Own Device (BYOD) consiste à apporter ses outils informatiques personnels au sein de l'entreprise (Smartphones, tablettes, Personal Computer…) et à les utiliser dans le cadre de ses activités professionnelles. Refusé par certains, il est aussi encouragé par d'autres.

Des entreprises l'adoptent dans une logique de productivité et d'économie liée à la fourniture ou bien encore à la maintenance des outils informatiques.

Ce phénomène, auquel les entreprises et administrations ne peuvent échapper, bouleverse leur mode d'organisation et les oblige à repenser la protection de leurs systèmes d'information.

En l'absence d'un cadre juridique précis sur ce phénomène, l'insécurité juridique accentue le flou autour du Bring Your Own Device.

Il est par ailleurs essentiel que la position de l'entreprise sur le BYOD soit clairement définie à la fois à travers les contrats de travail et la charte informatique ou encore le règlement intérieur. Il s'agit donc bel et bien de mettre en place une politique de gestion des risques.

Bring Your Own Device" (BYOD) refers to the practice of having employees bring their own electronic devices such as Smartphones, tablets and laptops at work and use them for business purposes.

Whilst some companies deny their employees this right, others actively support this new concept. For companies that allow it, it is not only a way to improve productivity but also to reduce acquisition and maintenance costs.

This concept changes the way a company is organised and compels them to rethink how they manage information security.

However, in the absence of any clear legal framework, there is increasing uncertainty surrounding this approach.

Therefore, it is critical that the companies elaborate a clear policy on the BYOD concept. This position must be clearly defined whether through the employment contracts, the charter for the use of IT or the company policies. Then, the aim is to implement a risk management policy.

Sommaire

Le Bring Your Own Device : connaître le contexte

Un enjeu de taille a fait son apparition ces dernières années : le *Bring Your Own Device* (BYOD), ou littéralement « Apportez Votre Propre Outil ». Ce concept consiste pour les salariés d'une entreprise à apporter leurs propres outils de travail.

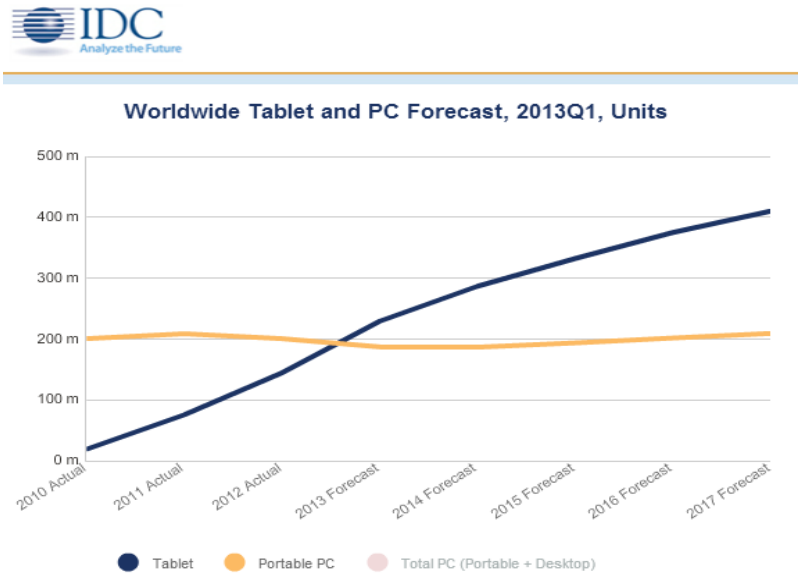
Le cabinet américain Gartner définit quant à lui le BYOD comme étant un phénomène perturbateur où les employés apportent leurs outils technologiques personnels dans l'entreprise et souhaitent être connectés à tout et partout. Cela, sans qu'aucune responsabilité ou surveillance ne soit définie[1].

Bien sûr, il pourrait s'agir d'appareil divers et variés pouvant aller de la voiture au téléphone portable. Mais c'est surtout avec l'essor des technologies avancées que ce phénomène s'est développé. Il n'est donc pas étonnant que l'entrée sur le marché du travail de la génération Y soit un corollaire de cette mouvance vers la connexion des salariés *at Any Time, Any Where, with Any Device* (ATAWAD).

L'arrivée des Smartphones et surtout des tablettes a conduit à ce que les salariés communiquent et travaillent sur plusieurs canaux différents.

A titre d'exemple, les ventes des tablettes ont explosé et ont été multipliées par 6,6 entre 2010 et 2012 allant jusqu'à 128.3 millions d'appareils vendus. En 2013, l'accélération sera telle que le nombre de tablettes vendues devraient atteindre 229,3 millions[2].

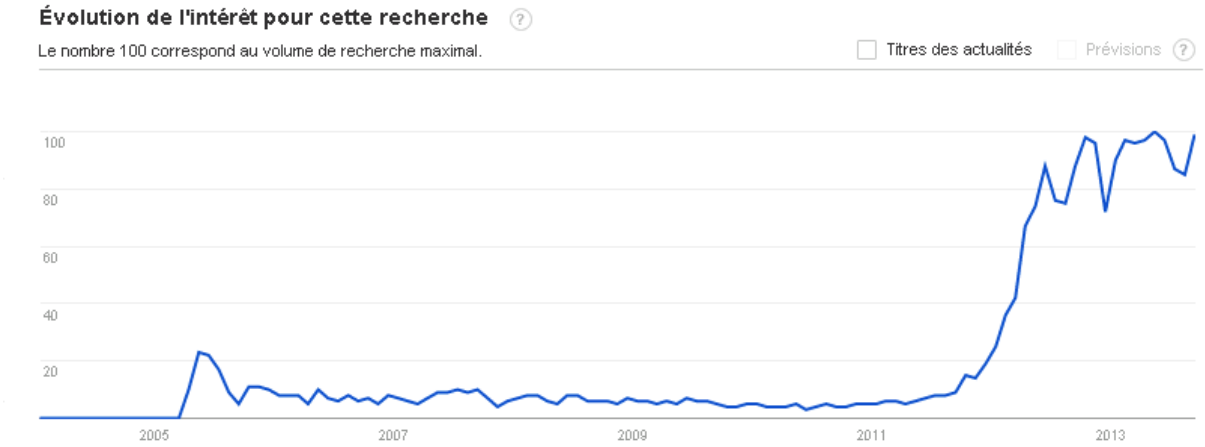
En ce qui concerne les Smartphones, la barre symbolique des 1 million d'appareils vendus devrait être franchie cette année[3]. C'est également en 2013 que les Smartphones devraient supplanter la vente des mobiles standards. En 2017, toujours d'après IDC, les livraisons de Smartphones devraient atteindre les 1,7 milliards.



[1] Gartner, http://www.gartner.com/technology/topics/byod.jsp
[2] IDC Worldwide Tablet Tracker, May 28, 2013
[3] IDC WorldWide Mobile Phone Tracker, September 4, 2013

Auparavant, la pratique du BYOD était plus souvent celle des cadres. Mais, avec la popularisation croissante des technologies avancées, il en va différemment aujourd'hui puisque tous les salariés et toutes les entreprises sont concernés.

Les études sur le BYOD en sont la preuve : il y a encore quelques années, la question du BYOD n'était quasiment pas abordée. Aujourd'hui, elle intéresse de plus en plus. Les recherches sur Google (Google Trends) le démontrent parfaitement :



Il s'agit là d'un phénomène mondial qui est plus ou moins bien accepté selon les pays. Une étude a été menée récemment par Dell en ce sens et montre que les Etats-Unis, la région de Pékin et l'Australie encouragent fortement le recours au BYOD.

A l'inverse, les Etats européens de l'enquête (France, Allemagne et Royaume-Uni) sont en bas du classement en ce qui concerne l'encouragement à l'utilisation des outils propres aux salariés[4].

Il n'est donc pas étonnant qu'en France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) se prononce formellement contre le BYOD. Son Directeur Général Patrick Pailloux a ainsi fait savoir qu'il fallait « *oser dire non et résister à l'usage sans règle des technologies de l'information*[5] ».

Le BYOD a un effet positif sur l'entreprise

Il peut cependant exister un intérêt pour les entreprises à avoir recours au BYOD, notamment en ce qui concerne la productivité. L'employé moyen qui utilise ses propres outils pour le travail gagne 37 minutes par semaine. Et pas moins de 53% des utilisateurs

[4] Dell Quest Software, *Dell unveils Global BYOD Survey Results : Embrace BYOD or be Left Behind*, January 22, 2013
[5] ANSSI, communiqué de presse, *Patrick Pailloux, directeur général de l'ANSSI, ouvre les assises de la sécurité 2012*, du 3 octobre 2012

d'appareils personnels disent avoir augmenté leur productivité en innovant dans leurs méthodes de travail grâce à leurs propres moyens technologiques[6].

D'après la dernière étude de Dell Software sur le sujet, les entreprises avec un programme BYOD déjà en place devraient connaître le plus de bénéfices. L'étude confirme également l'amélioration de la productivité des employés et nous apprend que 70% des entreprises adeptes du Bring Your Own Device voient leurs temps de réponse aux clients diminuer.

Par ailleurs, c'est également l'image de l'entreprise qui est impactée de manière positive. L'usage d'outils personnels peut motiver de nouveaux collaborateurs à rejoindre l'entreprise[7] et l'effet sur les clients de l'utilisation de ces technologies avancées donne une image de modernité qui est loin d'être négligeable.

Le CYOD et le COPE comme alternatives

La DSI peut également prendre les devants du BYOD à travers le biais de deux autres concepts : celui du Choose Your Own Device (CYOD) et celui du COPE (Corporate Owned, Personally Enabled).

Le but premier pour le DSI est de connaître l'ensemble des équipements présents et avec lesquels les salariés travaillent. Or, cela peut s'avérer quelque peu compliqué du fait de la multiplication des types de matériels.

A travers le CYOD, un encadrement de la part de la DSI peut être envisagé tout en laissant une certaine liberté aux salariés. Ces derniers peuvent ainsi choisir le terminal qu'ils souhaitent dans une liste proposée par l'entreprise. La question du non-accès des salariés à leurs données et applications par ce biais pourrait cependant ici être un facteur de refus de la méthode.

Et c'est ce à quoi répond le concept du COPE. Dans ce cas, l'employé peut utiliser son matériel professionnel à des fins personnelles. Là aussi, c'est donc l'entreprise qui choisit et fournit les outils mais le salarié pourra y installer les applications et les données personnelles qu'il souhaite. Toutefois, ce choix devra être validé avec le gestionnaire de la paye puisque cela peut être qualifié d'avantage en nature.

Un processus déjà en marche

En règle générale, c'est à l'employeur qu'il appartient de fournir à ses salariés tous les moyens dont ils ont besoin pour la bonne réalisation de leurs tâches. Mais avec la popularisation croissante des technologies avancées, le BYOD s'impose clairement même si des solutions alternatives existent. Dans la plupart des cas, les différents outils ont tendance à être utilisés à la fois pour des fins privées et professionnelles.

---

[6] CISCO, *L'impact financier du BYOD, les bénéfices d'une stratégie BYOD pour les entreprises multinationales*, mai 2013

[7] OSIATIS, the IT services experts, livre blanc : *byod, menace ou opportunité pour la DSI*, février 2013

La question n'est donc plus celle de savoir s'il faut autoriser les salariés à apporter leurs propres outils, mais plutôt celle de savoir comment faire pour encadrer cette interpénétration des moyens technologiques relevant de la sphère professionnelle et de la sphère privée.

Une étude britannique a fait savoir que 31% des adeptes du BYOD n'ont reçu aucune consigne concernant cette pratique[8]. Or, une réflexion sur l'utilisation de ces outils, sur la sécurité, sur les différents aspects des Ressources Humaines mais aussi une réflexion juridique devront être engagées.

Atteintes à la vie privée

L'arrivée de ce nouveau phénomène dans le monde du travail a certes des avantages mais il peut aussi représenter un danger, notamment en ce qui concerne le respect du droit au respect de la vie privée. Les composantes de celle-ci sont nombreuses et c'est tout particulièrement le respect de la vie personnelle au sein de l'entreprise qui est concernée.

En 2012, le président-directeur général d'une compagnie américaine spécialisée dans la gestion d'émail est parti en vacances avec sa famille. Sa fille de 5 ans s'est alors amusée avec le Smartphone de son père et a entré 5 codes PIN incorrects. La capacité pour l'entreprise d'effacer à distance les données s'est alors déclenchée et le PDG a perdu toutes les photos qu'il avait pu prendre avec son Smartphone lors de son voyage.

Ironie du sort, c'est lui-même qui avait joué un rôle essentiel dans la mise en place des règles concernant le Bring Your Own Device.

Le recours au BYOD conduit à ce qu'il n'y ait plus de frontière claire entre usage professionnel et personnel. C'est pourquoi il faudra définir un cadre juridique pour éviter de faire courir des risques aux employés.

Avec un appareil appartenant à l'entreprise, il est beaucoup plus aisé de se conformer aux règles s'intéressant à la vie privée. Les salariés s'attendent en effet moins à un respect de l'intimité lorsqu'ils utilisent le matériel de la société. Cela s'avère différent quand il s'agit d'appareils personnels.

C'est d'ailleurs cette vision que semble avoir la jurisprudence. Lorsque le matériel est fourni au salarié par l'entreprise, les tribunaux ont largement admis que les données présentes sur les postes de travail du salarié sont présumées être des données professionnelles. Si celles-ci ne sont pas clairement identifiées comme personnelles sur le terminal, l'employeur est censé pouvoir y accéder librement et en faire l'application qu'il souhaite.

Mais cette jurisprudence est-elle transposable dans le cas du Bring Your Own Device ? C'est-à-dire lorsque le terminal utilisé appartient au salarié ? Comment accéder aux terminaux personnels des salariés sans leurs autorisations ?

A ce jour, il n'y a pas encore de jurisprudence spécifique au BYOD mais il est possible d'imaginer la réponse qu'apporteront les juridictions.

[8] BAE system Detica, BYOD : the cost of Complacency, 2013

Certaines décisions rendues par la Chambre sociale[9] font en effet ressortir que les objets personnels, tels un dictaphone ou bien encore un sac, appartenant au salarié pouvaient être vérifiés seulement en sa présence et avec son accord. En 2005, cette même Chambre avait fait savoir que le contenu identifié comme personnel sur un matériel fourni par l'entreprise n'était accessible à l'employeur qu'en *présence du salarié* ou si celui-ci avait été *dûment appelé*, sauf en cas de *risque ou évènement particulier*[10].

La possibilité que la Cour passe d'un droit d'accès de principe de l'employeur à un droit d'accès par exception est fortement probable. Tout comme le contenu sur un matériel fourni par l'entreprise est supposé être professionnel, celui stocké sur un appareil appartenant à l'employé est présumé personnel.

Mais d'autres questions se posent également : l'entreprise peut-elle tracer ses employés ? Comment peut-elle assurer la protection de ses données personnelles ? Comment la responsabilité de l'entreprise peut-elle être dégagée ?

Un des enjeux pour les entreprises est donc clairement de parvenir à mettre en place des règles quant à la gestion des données personnelles dans le cadre du BYOD.

Sécuriser les données

Cette frontière floue entre sphère professionnelle et privée peut également faire courir des risques important à l'entreprise. Ce sont notamment les atteintes aux données des différentes sociétés qui représentent un des risques majeurs. Et il est certain que le recours au BYOD augmente la probabilité de ces atteintes.

D'une part, le Bring Your Own Device conduit à une multiplication des portes d'entrées aux chevaux de Troie et autres virus. Ces failles conduisent alors à une augmentation des attaques sophistiquées. Les hackers étudient de près les habitudes personnelles des salariés et c'est de cette manière qu'ils infectent leurs outils. Une fois le matériel de retour sur le lieu de travail, il est aisé de pénétrer le réseau informatique de l'entreprise ou de l'administration. Il est évident que les dirigeants, les cadres, qui détiennent des informations sensibles seront des cibles appréciées des hackers.

Il est donc clairement plus intéressant de sensibiliser le personnel et d'encadrer le BYOD que de nettoyer le réseau de l'entreprise après chaque infection.

Les outils de travail sont par ailleurs d'éventuels lieux de stockages de contenus parfois illicites (musiques, films…) mais peuvent également participer à la fuite d'informations confidentielles de l'entreprise.

[9] Cass.soc., 11 février 2009, n°07-42.068 ; Cass.soc., 23 mai 2012, n°10-23.521
[10] Cass.soc., 17 mai 2005, n°03-40.017, M. X. c/ Société Cathnet-Science

D'autre part, la mobilité même de ces outils constitue un danger. Leur facilité de transport conduit à une plus grande probabilité de perte ou de vol.

Dans un tel contexte, c'est donc la manière dont les employés utilisent leurs appareils qui est tout particulièrement importante. Il faut aussi noter qu'avec la popularité croissante d'applications tierces (à l'image de Dropbox par exemple), tous ces risques sont multipliés.

Il est donc essentiel pour les sociétés de faire preuve d'une certaine fermeté. Il leur faut alors préciser quel type de données peut être consulté et stocké mais aussi indiquer la manière dont celles-ci doivent l'être sur telle ou telle application.

Comme l'illustrent le Mobile Device Management (MDM) et la virtualisation, il existe certaines solutions afin de pallier ces risques.

Avec l'adoption du MDM, les entreprises peuvent choisir efficacement quelles applications peuvent être rendues disponibles à leurs employés.

En 2012, le cabinet américain Gartner a fait savoir que d'ici 2017, 65% des entreprises devraient avoir adopté un système MDM.

Les sociétés qui adoptent une approche « virtuelle » sont plus à même d'assurer qu'il n'y ait plus de données sur l'appareil dans le cas où celui-ci est perdu ou volé. Il est en effet possible d'y accéder via internet et il peut être éteint voire détruit à distance.

Peu importe la méthode choisie, la société se doit de reconnaitre que les utilisateurs sont amenés à stocker certaines données de l'entreprise sur leurs outils.

La question de savoir si les données de l'entreprise sont distinctes des données personnelles se pose alors.

Ici, l'enjeu est donc de sensibiliser les employés et d'assurer qu'ils fassent toutes les démarches nécessaires pour assurer la sécurité de leurs appareils. Par exemple la mise à jour de leurs mots de passe, l'installation de l'antivirus, etc. Ce genre d'obligations doit être intégré dans tout programme BYOD et toutes règles qui s'y attachent.

Les enjeux quant à la propriété intellectuelle

Le BYOD implique d'anticiper plusieurs problématiques quant au droit de la propriété intellectuelle, notamment quant à la propriété des créations au sein de l'entreprise et à l'éventuelle contrefaçon de logiciels.

Auparavant, la propriété du contenu sur les appareils appartenant à l'entreprise s'établissait aisément. Ainsi, la création d'un contenu sur le matériel de l'entreprise mettait l'employeur dans une situation de force en ce qui concerne la réclamation du droit de propriété intellectuelle.

Aujourd'hui, ce n'est plus aussi simple. Alors que l'employeur peut prétendre à la propriété intellectuelle développée dans le cadre de l'emploi par un utilisateur, qui est titulaire des

droits de propriété intellectuelle lorsque l'utilisateur crée un « bien » en utilisant un outil personnel en dehors des heures de travail ? Avec l'arrivée du BYOD, il y a de plus en plus de situations floues.

Ainsi, les sociétés et administrations devront être conseillées quant aux contrats de travail existants afin de s'assurer que toute œuvre ou innovation créée par un employé sur un outil BYOD, que ce soit au travail ou en dehors, soit propriété de l'entreprise ou de l'administration. Il existera toujours des exceptions à la règle posée mais ne pas réagir à cette situation conduira à une prise de risque plus grande encore pour la société.

Par ailleurs, il est probable que les licences des différents logiciels d'une société ou d'une administration ne puissent pas répondre à une transition vers le BYOD. En effet, les modalités des licences existantes peuvent être accordées pour un nombre limité d'utilisateurs ou d'appareils.

Les licences ne peuvent alors valoir que dans le cadre des outils qui sont la propriété de l'entreprise ou de l'administration ou que cette dernière loue.

A fortiori, elles ne peuvent pas être étendues aux Smartphones et tablettes appartenant aux salariés. Cela pourrait en effet caractériser une contrefaçon de logiciels.

Il est donc nécessaire pour les entreprises et administrations de réviser leurs contrats de licences.

La conservation des données

Les sociétés et administrations doivent se soumettre à de nombreuses obligations de conservation des données pour les litiges ou à des fins réglementaires.

Les employeurs doivent comprendre que les technologies avancées impactent ces obligations. Dès lors que les données de l'entreprise et de l'administration sont stockées sur un outil personnel, se soumettre à de telles obligations devient un véritable défi.

Vérifier les polices d'assurances

Que se passe t-il si l'appareil personnel du salarié est perdu ou volé ? Est ce que cette perte ou ce vol sera couvert par l'assurance de la société ou de l'administration? Qui est alors responsable ?

Pour répondre à ces questions, il est essentiel de s'adresser directement à son assureur pour mettre à jour toutes les règles et mettre en place celles qui seraient pertinentes.

Il faut en effet être conscient que de nombreuses normes vont s'appliquer aux équipements loués par l'entreprise et l'administration ou lui appartenant mais ne vont pas s'étendre à ceux qui appartiennent aux salariés.

Les Ressources Humaines sont les plus concernées par le BYOD

C'est sans doute dans le domaine des ressources humaines qu'il y a le plus de questions juridiques qui se posent.

- Lorsqu'un utilisateur cesse son travail en tant qu'employé, quelles sont les responsabilités à mettre en avant ?

- A qui le BYOD peut-il s'appliquer ? Tous les employés ou seulement ceux qui remplissent certains critères ?

- Quelles sont les mesures de sécurités minimum et obligations qui devront être mises en place pour les mots de passe et les mises à jour obligatoires ? Jusqu'où les mesures de sécurité peuvent-elles aller ?

- Faut-il autoriser l'accès à des parties tierces telles que Dropbox ? Si oui, sur quelles bases et comment les contrôler ?

- Qu'en sera-t-il de la maintenance des matériels du BYOD ? Qu'en sera-t-il de la maintenance des différentes applications ?

- Quel contenu et utilisation seront autorisés ? L'accès à des contenus « inappropriés » dans le cadre privé est une chose mais le fait que l'utilisateur apporte son matériel au sein de l'entreprise en est une autre.

- Quels sont les autres domaines impactés indirectement par le BYOD ? Des règles peuvent être mise en place dans le cadre de la politique internet, des mails, de la sécurité des données, etc.

- Selon la politique du BYOD appliquée, est-ce que la société va attribuer une allocation pour le matériel ?

- Comment contrôler le temps de travail ? Par exemple, certaines entreprises et administrations choisissent de bloquer le transfert des e-mails après une certaine heure.

- Etc.

Les conséquences pour les entreprises et les administrations

Certaines pensent que le BYOD n'est qu'un enjeu technologique. C'est loin d'être le cas.

Ce phénomène touche le monde du travail en son entier et lorsqu'un programme pour son encadrement est mis en place, il doit impliquer à la fois les représentants de la technique, du management, du droit, de la finance et des ressources humaines.

Les risques avec l'application du BYOD ne sont pas négligeables et il faudra donc faire en sorte que :

- les changements nécessaires quant aux contrats de travail soient réalisés,

- des relations de travail efficaces entre la technique, les finances et le management soient mises en place en mettant en œuvre un programme qui permette d'atteindre les objectifs de la société tout étant en conformité avec les dispositions légales et réglementaires,

- les parties tierces soient identifiées et travailler étroitement avec elles (assurance, les vendeurs de programme pour les licences, les autorités administratives qui peuvent avoir un impact sur l'usage du BYOD, etc.),

- un cadre juridique soit mis en place pour la protection des intérêts légitimes de la société face aux droits des utilisateurs individuels. Et ce, tout particulièrement en ce qui concerne la sécurité des données, de la vie privée, des informations confidentielles et des droits de propriété intellectuelle.

Comme nous l'avons déjà fait remarquer, le BYOD est une tendance qui s'impose, que l'entreprise le veuille ou non. Les employeurs qui prennent les devants en mettant en place un encadrement et des procédures propres au Bring Your Own Device pour la gestion des risques éventuels sont ceux qui vont bénéficier des avantages du BYOD.

Ceux qui ignorent cette tendance mettent en danger leurs entreprises, d'autant plus que c'est aussi l'image de la société qui est susceptible d'en pâtir. Il est en effet plus difficile d'imaginer la réussite future de la société.

Et en l'absence d'anticipation de l'employeur ?

Au-delà d'une résolution plus aisée des éventuels conflits, la mise en place d'un cadre juridique bien spécifique à l'usage du BYOD au sein de l'entreprise et de l'administration permet d'avoir une réponse plus adaptée à la situation que celle imposée par le droit commun.

Ce sont en effet les principes généraux du droit de la responsabilité qui s'appliquent en l'absence de règles préalablement définies. Ainsi :

- Si l'ordinateur d'un salarié est à l'origine d'un dommage à autrui (autre salarié ou employeur) alors le salarié est responsable. Si un appareil personnel blesse quelqu'un au travail, le régime juridique des accidents du travail aura à s'appliquer même si l'employeur n'est pas le propriétaire de l'appareil apporté sur le lieu de travail dans le cadre du BYOD.

- Si l'ordinateur personnel du salarié est volé ou endommagé, alors l'employeur sera présumé responsable. Il devra alors indemniser le salarié. Afin de limiter sa responsabilité, l'employeur aura à démontrer la faute du salarié.

- Si l'ordinateur du salarié cause des dommages au système de l'entreprise (par le biais de virus par exemple), il n'est même pas certain que celui-ci voit sa responsabilité engagée. La Cour de cassation fait en effet savoir que la responsabilité civile du salarié envers son employeur suppose non pas une simple erreur involontaire mais bien « *une faute lourde assimilable au dol* ». Il faudrait donc que l'employeur parvienne à démontrer l'intention de nuire du salarié.

La mise en place d'une Charte informatique ou la révision de celle-ci permettrait de régler plus facilement de nombreuses situations. Et ce d'autant plus que la jurisprudence reconnait le caractère contraignant d'une telle Charte[11].

Réviser la Charte et/ou les contrats de travail

On a pu le constater, la tendance vers le BYOD soulève de nombreuses questions juridiques. Il faut savoir qu'anticiper tout litige peut permettre de simplifier l'utilisation du BYOD.

Pour cela, il faut aller à la base du travail, c'est à dire au droit : le but est l'encadrement de l'utilisation des équipements personnels au sein de l'entreprise.

Pour ce faire, il n'est que trop conseillé de procéder à une révision de la Charte informatique en vue d'intégrer les terminaux personnels des salariés dans son périmètre.

Ce sera par ailleurs l'occasion pour l'entreprise d'aborder la question de la frontière entre l'espace privée et l'espace professionnel sur les terminaux personnels.

Il faudra alors prévoir précisément les situations dans lesquelles l'entreprise pourrait être amenée à supprimer ou récupérer les données sur le terminal personnel, par exemple en cas de départ du salarié (décès, licenciement, démission, etc.).

Bien entendu, tout ce qui s'attache à la propriété intellectuelle, aux informations confidentielles ou bien encore à la responsabilité devra être prévu.

[11] Cass.soc., 15 décembre 2010, n°09-42.691, M. X c/ Société Coca-Cola

BYOD	Ce qui doit être prévu
Assurance et responsabilité	Identifier clairement dans le programme BYOD si l'utilisateur ou la société sera responsable pour la perte ou le vol du matériel
	Identifier clairement si l'utilisateur ou la société est responsable pour la maintenance des appareils et des outils nécessaires à la protection du système (antivirus…)
Respect de la vie privée	Mise en place de procédure pour la séparation des données personnelles et professionnelles
	Traiter les atteintes à la sécurité, des logiciels malveillants, de la perte ou du vol
	Est-il possible d'accéder aux ordinateurs des salariés sans leurs autorisations ?
	Prévoir la procédure à appliquer en cas de départ du salarié
	Prévoir la procédure à appliquer pour accéder aux terminaux personnels en cas de risque ou d'urgence
Surveillance du lieu de travail	Mise en place d'une politique de surveillance des données
	Informer les utilisateurs d'outils personnels du suivi ou de l'enregistrement des communications de l'appareil
	Informer les employés des terminaux acceptés et des réseaux consultables
Données à caractère personnel	Garantir une sauvegarde des données tout en faisant en sorte que les données pertinentes ne soient pas supprimées.
	Mise en place de la protection des données à caractère personnel
Licences	Les conditions de licence des logiciels du BYOD reflètent-elles les la politique de BYOD de l'entreprise ? L'utilisation de logiciel sur un matériel BYOD est-elle réduite lorsque la compagnie n'a pas acquis de licence ?
Informations confidentielles	Mise en place de mesures de sécurité telle que la capacité à effacer des données à distance et procédure de « déclassement »
	Comment protéger les mots de passe dans le cadre du BYOD ?

Il faudra ainsi penser à adapte les contrats de travail à toute nouvelle embauche et y inclure toutes les clauses contractuelles dédiées à la problématique du BYOD.

Pour ce qui est de la Charte, une fois son contenu défini, il faut suivre une procédure bien précise et notamment informer et consulter au préalable les instances représentatives du personnel.

Parfois, l'entreprise ou l'administration aura déjà mis un certain nombre de règles en place qui peuvent concerner directement ou indirectement le BYOD notamment les règles quant aux mots de passe ou aux réseaux sociaux.

Les sociétés ou administrations ayant prévu ce type de règles doivent donc revoir leurs règles existantes et déterminer si elles impactent la mise en œuvre de la stratégie liée au BYOD et si elles font la distinction entre outils personnels et outils professionnels.

En effet, le point crucial est la cohérence entre les règles existantes et les nouvelles règles liées au BYOD.

Si la Charte informatique et les contrats de travail permettent d'encadrer l'utilisation faite par les employés de leurs propres outils dans le cadre professionnel, cela ne concerne pas, en revanche, les tiers de l'entreprise ou de l'administration. Il faudra ainsi veiller à prévoir des dispositions quant au BYOD dans les accords avec les consultants ou les employés des prestataires…

Sensibiliser le personnel de l'entreprise et l'administration

On conclura sur la nécessité de sensibiliser le personnel. En effet, il est indispensable d'instaurer au sein de l'entreprise ou de l'administration une véritable « culture juridique » puisque, par nature, la pratique du Bring Your Own Device concerne tous les salariés (employés, cadres, dirigeants, etc.).

Des formations, des séminaires de sensibilisation devront ainsi être organisés de manière récurrente.

Les points essentiels à prévoir dans la Charte

- Les employés concernés par l'usage du BYOD ;
- les matériels, le type de connexion, les systèmes d'exploitation et les applications ;
- le respect de la propriété intellectuelle ;
- les sites et les réseaux consultables et utilisables dans le cadre professionnel ;
- les modalités de contrôle et les sanctions possibles en cas de non-respect de la Charte ;
- le respect des horaires de travail ;
- les éventuelles participations financières de l'employeur pour le matériel, etc.

Ce Livre blanc est purement indicatif et non exhaustif. Il ne constitue aucunement un conseil juridique.

Si vous souhaitez de plus amples informations au sujet du BYOD, n'hésitez pas à poser vos questions à l'adresse suivante : contact@avocats-mathias.com