Bring your own device : Les recommandations de la CNIL

[DONNEES PERSONNELLES]
CNIL, fiche pratique, 19 février 2015

La communication de la CNIL sur le « BYOD » (Bring your own device) intéressera les entreprises, de plus en plus nombreuses, qui incitent leurs salariés à utiliser leurs terminaux personnels (ordinateurs, smartphones, tablettes) pour accéder dans le cadre de leur activité professionnelle aux systèmes d'information de l'entreprise. Côté employeur, l'encouragement de cette pratique répond à un objectif de baisse des coûts des services informatiques et d'amélioration (supposée) de la productivité. Beaucoup de salariés y voient également un moyen de gagner en autonomie et en confort de travail.

Le développement du BYOD, aux Etats-Unis d'abord et aujourd'hui en Europe, soulèvent néanmoins plusieurs questions à la frontière du droit des données personnelles et du droit du travail. La CNIL tente d'y répondre en mettant désormais à disposition des utilisateurs des recommandations qui, même si elles n'ont pas valeur contraignante, constituent un vade-mecum des bonnes pratiques à mettre en œuvre.

La CNIL rappelle tout d'abord que le BYOD n'exonère pas les employeurs de leur obligation de fournir à leurs salariés le matériel et les ressources nécessaires à l'exécution de leurs tâches professionnelles. Il faut en déduire qu'un employeur ne saurait « imposer » le BYOD en refusant de mettre à la disposition des salariés les outils informatiques dont ils ont besoin dans le cadre de leurs fonctions.

L'un des problèmes les plus sensibles liés au BYOD est celui de la sécurité des données personnelles de l'entreprise stockées sur les terminaux appartenant aux utilisateurs. En tant que responsable de traitement au sens de la loi Informatique et Libertés, l'entreprise a l'obligation d'adopter des mesures permettant d'assurer la confidentialité et le maintien de l'intégrité de ses données. La CNIL livre à cet égard plusieurs conseils pratiques à l'attention des directions informatiques (création d'une bulle de sécurité permettant de cloisonner séparément les données de l'entreprise et celles du propriétaire du terminal, mise en place d'un accès sécurisé à l'espace entreprise via un dispositif robuste d'authentification, chiffrement des flux d'informations, procédure d'alerte obligatoire en cas de perte ou vol du terminal).

L'instauration d'une charte interne contraignante informant les salariés des mesures de gestion des risques en matière de sécurité est encouragée.

La CNIL souligne ensuite que la pratique du BYOD doit être conciliée avec l'impératif de protection de la vie privée des salariés qui utilisent leurs équipements personnels en partie à des fins professionnelles. Il serait donc contraire au principe de proportionnalité que l'entreprise accède, même sous couvert d'un risque de sécurité, aux éléments personnels du salarié (photos, annuaire, agenda privé) stockés sur son équipement. Si la CNIL admet la mise en œuvre d'une mesure d'effacement à distance des données, en particulier en cas de perte de ou de vol de l'équipement du salarié, cette mesure doit respecter l'intégrité des données n'appartenant pas à l'entreprise.

Enfin, la CNIL donne une indication intéressante sur le régime déclaratif du BYOD. Elle considère que cette pratique peut être couverte par une déclaration normale des traitements de gestion du personnel, à condition que cette déclaration intègre une finalité touchant à la sécurité et au fonctionnement des systèmes d'information. En revanche, la CNIL exclut que le BYOD puisse entrer dans le champ d'application de la norme simplifiée n°46 relative à la gestion des ressources humaines puisque, en matière d'outils et moyens informatique, cette norme vise uniquement les ressources appartenant à l'entreprise.

Grâce à cette première fiche pratique publiée par la CNIL, les entreprises qui recourent au BYOD disposent désormais de recommandations claires de l'autorité de protection des données leur permettant de se mettre en conformité.

Hélèna DELABARRE