# Protéger les données des collaborateurs en mobilité

## CONTRAINTES ET DEFIS

**Les données numériques véhiculent un grand nombre d'informations de grande valeur, voire confidentielles. La révolution digitale permet à tous, notamment responsables et dirigeants d'être extrêmement mobiles. Ils peuvent avoir accès, en permanence, au système d'information de l'entreprise et peuvent ainsi travailler en tout lieu. Si cet accès permanent aux données de l'entreprise fait naître des réelles opportunités, il génère aussi de nombreux risques.**

Les nouveaux défis sécuritaires imposent aux entreprises de se réorganiser en profondeur. Quelles sont les contraintes ? Quelles sont les bonnes pratiques à adopter ? Autant de questions auxquelles Matthieu Bourgeois, associé du département IT/ Propriété Intellectuelle du cabinet SIMON ASSOCIES a accepté de répondre.

**Quelles sont les nouvelles sanctions et obligations de sécurité posées par le Règlement communautaire sur la protection des données ?**

Le nouveau règlement communautaire ( Règlement Général sur la protection des données – « **RGDP** ») prévoit une obligation de sécurité à la charge du responsable de traitement et du sous-traitant, comme le faisait déjà la Loi Informatique et Libertés, actuellement en vigueur, mais de manière plus précise par rapport à cette dernière puisque l'article 32 du RGDP donne une liste illustrative (c'est-à-dire non obligatoire et non limitative) des mesures de sécurité qui peuvent être mises en œuvre, à savoir :

- La pseudonymisation
- Le chiffrement
- Tout autre moyen « permettant de garantir la confidentialité, l'intégrité, la disponibilité » des données, et parmi lesquelles il faut considérer que figurent très certainement l'identification/ authentification des utilisateurs ainsi que la mise en place de contrôles d'accès avec une gestion stricte des droits.

Il s'agit là des mesures devant être mises en place « avant » l'atteinte.

« Après » l'atteinte, tout responsable de traitement devra procéder à une notification auprès de l'autorité de contrôle (la CNIL, pour la France), ainsi que, si l'atteinte engendre « un risque élevé pour les droits et libertés d'une personne physique » (on pensera, par exemple, à une divulgation non autorisée de données bancaires), le responsable de traitement devra alors procéder à une notification à l'ensemble des personnes concernées par la violation de leurs données.  A titre d'exemple, Orange a dû, il y quelques années, effectuer une notification de ce type auprès de plusieurs centaines de milliers de personnes dont les données avaient fait l'objet d'un accès par un tiers non autorisé, et cette notification avait engendré des frais, pour l'opérateur, de plusieurs millions d'euros.

**Matthieu Bourgeois**

Le nouveau règlement prévoit des sanctions, en cas de non-respect des obligations de mise en place de sécurité préventives ainsi que d'absence de notification lorsque celle-ci est requise, pouvant aller jusqu'à 2% du chiffre d'affaires mondial réalisé par le responsable de traitement/ sous-traitant défaillant ou 10 millions d'euros (le plus élevé des deux plafonds étant retenu).

**Côté solutions de sécurisation en mobilité, comment protéger les données et les collaborateurs ?**

L'entreprise devra mettre en œuvre des mesures techniques (tel que, par exemple, le chiffrement du canal de communication entre le mobile et le système d'information de l'entreprise, la conteneurisation des données accessibles via le mobile à travers un dispositif sécurisé, séparant ces données professionnelles des éventuelles autres données personnelles dans l'hypothèse où le salarié utiliserait ce mobile à des fins pro/perso...) mais également des mesures juridiques (comme, par exemple, la mise en place d'une charte informatique qui posera des règles strictes d'utilisation des terminaux nomades – tels que les mobiles, les tablettes... - et précisera notamment les règles applicables en cas de vol ou perte du terminal).

Une charte informatique présentera l'avantage d'offrir à l'entreprise des recours efficaces contre ses éventuels collaborateurs malveillants. A cet égard, une décision peut être citée : dans un arrêt du 22 octobre 2014, la Cour de Cassation a confirmé la condamnation – prononcée par la Cour d'Appel de Bordeaux – d'un salarié ayant appréhendé un grand nombre de fichiers informatiques de son entreprise peu avant de quitter celle-ci pour rejoindre un concurrent, sur le fondement de l'abus de confiance. Dans cette affaire, la présence d'une charte informatique, ratifiée par le salarié et lui interdisant toute utilisation des données de l'entreprise à des fins personnelles, n'a pas été étrangère à la solution retenue (Cour de Cassation, chambre criminelle, 22 octobre 2014, pourvoi no 13-82630).

**Est-ce qu'une nécessaire réorganisation des entreprises s'impose en réponse aux contraintes réglementaires ?**

Oui, sans aucun doute. Sur le plan organisationnel, il est indispensable de mettre en place un processus de pilotage de la sécurité des données, qui implique notamment :

- De dégager une classification des données à protéger, qui seront ensuite soumises à des restrictions d'accès ou d'usage adapté
- De se doter de moyens de détection des atteintes possibles, ainsi que d'outils permettant de réagir et d'en limiter rapidement les effets préjudiciables
- De nommer un Responsable de la Sécurité des Systèmes d'Informations (« RSSI ») ou équivalent, disposant de moyens humains et financiers adaptés, nouant un partenariat fort avec la direction de l'entreprise
- De mettre en place des processus visant à impliquer le RSSI et ses équipes dans tous les nouveaux projets, afin que les éventuels risques soient identifiés et donnent lieu systématiquement à une réponse adaptée

Il faudra bien entendu, aussi, impliquer le délégué à la protection des données (en anglais « Data Protection Officer », aussi appelé « DPO »), lorsque l'entreprise sera dans l'obligation d'en désigner un (ce que le RGDP exige lorsque les activités de l'entreprise « consistent en des opérations des traitement qui, du fait de leur nature, de leur portée et/ ou de leur finalité, exigent un suivi régulier et systématique à grande échelle des personnes concernées »), pour que celui-ci soit systématiquement associé aux projets mettant en œuvre des traitements de données à caractère personnel et puisse se prononcer sur leur conformité.

*> Par Sabine Terrey*