Droit :

07/09/16

5.1 : Obligation de securiser les données numériques

Le**service informatique doit appréhender les risques**et prendre les mesures nécessaires pour garantir la continuité et la qualité du service, la sécurité et la confidentialité des données, la réversibilité des solutions, etc. :  
• Obligation de protéger les données.  
• Obligation de contrôler les accès aux données à caractère personnel et aux données sensibles  
• Obligation d’organiser la collecte de la preuve numérique dans le cadre de la politique de sécurité informatique.  
• Obligation de protéger le système d’information et de sécuriser les échanges afin de réduire les risques de piratage, les erreurs et malveillances diverses.

Si l’employeur peut mettre en place une **cybersurveillance de**l’activité des salariés, celle-ci est encadrée par la législation qui précise les conditions de mise en place, de consultation des dossiers et d’usage de la messagerie professionnelle, etc. tout en respectant la vie privée du salarié.

Les règles d’utilisation des outils informatiques (accès aux réseaux, messagerie, etc.) mis à disposition du salarié sont en général précisées dans une charte dont la valeur juridique dépend des conditions de son élaboration.

* La protection du patrimoine informationnel, l’archivage électronique et la sécurité des supports, la protection des données à caractère personnel, la lutte contre la criminalité informatique.

L’obligation de sécuriser des données numériques

* Nom, prenom, statut matrimonial, ddn, email, ip, statut matrimonial, numéro sécu, numéro tel, num cb, plaque immatriculation, empreinte genetique et empreinte bio.