Notions juridiques en relation avec la sécurité informatique

Table des matières

1 Notions juridiques

1.1 Articles de loi

La **loi Godfrain** réprime les actes de criminalité informatique et de piratage. Ses principaux articles sont :

- 323-1 : accès non autorisé et maintien frauduleux au SI = **2 ans de prison et 30,000€ d'amende**
- 323-2 : entraver ou fausser le fonctionnement d'un SI = **5 ans de prison et 75,000€ d'amende**
- 323-3 : introduction, modification ou suppression frauduleuse de données d'un SI = **5 ans et 75,000€ d'amende**

Les lois contre les atteintes à la personnalité ont les articles suivants.

- 226-15 : secret des correspondances = **1 an de prison et 4,500€ d'amende**
- 226-13 : secret professionnel = **1 an de prison et 15,000€ d'amende**

Les articles sur l'exploitation sexuelle des enfants et la pédopornographie prévoient **5 ans de prison et 75,000€ d'amende**.
Les données personnelles d'un utilisateur doivent être explicitement nommées telles qu'elles. Jurisprudence : les initiales de l'utilisateur dans le nom de fichier ne suffit pas.
La consultation de données personnelles (mails, fichiers…), nécessite la présence du salarié ou d'un représentant et ne peut avoir lieu qu'en cas de risque ou d'événement particulier.
Les administrateurs ne peuvent accéder aux données personnelles que si c'est le seul moyen d'assurer le bon fonctionnement du SI. Ils ont alors un devoir de secret professionnel.
La surveillance d'un utilisateur ne peut être mise en place que s'il est suspecté d'activités déloyales ou illégales. Il doit en être averti.
Le mot de passe peut être demandé à un utilisateur que si et seulement si cela est nécessaire à la poursuite de l'activité de l'entreprise.
Les logiciels sont couverts par les droits d'auteurs. Un utilisateur copiant un logiciel mis à sa disposition par son employeur commet une contrefaçon.

1.2 CNIL (Commission Nationale Informatique et Libertés)

Une donnée a un caractère personnel si elle identifie ou permet d'identifier, directement ou indirectement, une personne.
Une donnée est sensible si elle fait apparaître directement ou indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales, ou relatifs à

la santé ou à la vie sexuelle.
La **CNIL** est une autorité administrative indépendante chargée : d'informer des :

- droits et des devoirs
- de recenser les fichiers
- de garantir les droits d'accès
- de contrôler et d'instruire les plaintes
- de réglementer et de prospecter

Tous les fichiers doivent faire l'objet d'une déclaration simplifiée ou d'une autorisation pour les fichiers sensibles ou à risque.
La durée de conservation est de :

- 1 an pour les données relatives au trafic
- 3 mois pour les données permettant d'assurer la sécurité.

Le **CIL** (correspondant Informatique et Libertés) veille au respect des lois Informatique et Libertés à l'intérieur d'une entreprise.
La sanction pour l'infraction à la déclaration ou la conservation des fichiers est de **150,000 à 300,000€**

1.3 RSSI (Responsable de la Sécurité des SI)

Le **RSSI** doit avoir :

- les compétences techniques et connaissances judiciaires
- l'autorité et les moyens nécessaires pour accomplir sa mission
- une délégation précise (par ex la sécurité du SI) et permanente (pas de CDD)
- un transfert de responsabilité pénale

Même s'il peut encore être attaché au **DSI** (Directeur du SI), il est maintenant généralement rattaché à la direction générale.
Les administrateurs systèmes et tous les usagers du SI, dont les développeurs, doivent se plier aux règles dictées par le **RSSI**. Les projets informatiques doivent prendre en compte, dès la conception, les règles en vigueur au sein de la société.