THEME D5 La sécurité des systèmes d'information

Fiche D 512

D 5.1 L'obligation de sécuriser des données numériques

Mots clés : 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.

Fiche synthèse

Idée clé →	Le patrimoine informationnel, composé de toutes les données numériques de l'entreprise, est crucial pour la continuité de ses activités. Il appartient donc aux responsables des services informatiques de faire en sorte que toutes les données numérisées dans le SI soient protégées.
Donner du sens →	Les conséquences d'une trop faible protection du SI peuvent être graves : perte d'exploitation, dégradation de l'image de marque mais également sanctions judiciaires en cas de manquement à la loi notamment relative à la protection des données à caractère personnel.

Le patrimoine informationnel de l'entreprise correspond à l'ensemble des informations commerciales, sociales, financières, technologiques… détenues par l'entreprise et numérisées dans son SI. Ces données numériques doivent faire l'objet d'une grande vigilance de la part des responsables informatiques en premier lieu mais également de tous les collaborateurs de l'entreprise : la sécurité du SI devenu le support de ces données et informations, n'est plus l'apanage des services informatiques.

1. Les risques en matière de données numériques

- ✓ La mise en place d'une politique de sécurité globale doit être précédée par l'identification des risques dont les données et informations qui composent le patrimoine informationnel peuvent être la cible d'agissements frauduleux ou malveillants ou de simples négligences. Pourtant, ces données numériques stockées dans le SI et qui forment le patrimoine informationnel, sont cruciales. Leur perte, leur altération ou destruction peut avoir de graves conséquences pour l'entreprise.
- ✓ Le patrimoine informationnel doit être protégé contre les :
  - risques internes à l'entreprise dus aux agissements des collaborateurs : sécurisation insuffisante des accès au SI, non-respect des habilitations, divulgation ou perte volontaire ou par négligence d'informations confidentielles voire sensibles, mais également en raison de la défaillance des équipements matériels
  - risques externes à l'entreprise dus à des tiers souvent malveillants : altération, vol, destruction des données à la suite d'une intrusion informatique ; espionnage économique, perturbation des traitements etc.
- ✓ Les activités illégales commises à l'encontre des SI à l'aide des technologies de l'information et de la communication relèvent de la criminalité informatique. L'entreprise doit être vigilante vis-à-vis des délits commis grâce à des technologies (logiciel malveillant, de piratage…) ou commis sur des supports technologiques (SI).
- ✓ Des solutions techniques (*data leak protection*) peuvent permettre de protéger le SI : audit de sécurité régulier du SI afin d'identifier les failles, sécurisation du réseau informatique contre des attaques (antivirus, pare-feu, anti *spams*), mise en place d'un contrôle d'accès aux informations (avec différents niveaux d'habilitation), mise en place de moyens d'identification et d'authentification des utilisateurs, procédures de chiffrement des données et cryptologie, recours aux signatures électroniques etc.

Des solutions juridiques peuvent également protéger l'entreprise, son SI et son patrimoine informationnel.

2. La protection des données numériques par la charte ou le contrat

- ✓ Dans le cadre de sa politique de sécurité, l'entreprise doit identifier tous les acteurs concernés afin de déterminer les responsabilités, les risques et afin d'optimiser la sécurité.
  - Les acteurs internes :
    Tous les collaborateurs de l'entreprise sont concernés par la sécurité informatique (du DSI au simple utilisateur du réseau interne par exemple). La charte informatique répertorie notamment les règles en matière de sécurité informatique. Cette charte intégrée dans le

règlement intérieur s'impose à tout salarié de l'entreprise. Par ailleurs, les contrats de travail peuvent comporter des clauses explicites en matière de sécurité informatique : restitution des mémoires externes en cas de départ de l'entreprise, sort des mémoires des ordinateurs personnels des salariés dans le cadre du Byod…

- Les acteurs externes :
  Les relations avec les partenaires (infogérant, sous-traitant…) peuvent être encadrées par des clauses contractuelles spécifiques. Il est, par exemple, important que, dans le cadre d'une étude de faisabilité, une clause prévoit le sort des données confiées au partenaire potentiel si la relation contractuelle n'aboutissait pas (clause de réversibilité).

3. La protection du SI et de ses données numériques par la loi

La loi pénale sanctionne :

- ✓ Toute introduction illégale dans un ordinateur : le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un STAD est puni d'un 1 de prison, et de 15 000 euros d'amende.
- ✓ Toute atteinte aux systèmes ou aux données :
  - Perturbation des traitements : « Le fait d'entraver ou de fausser le fonctionnement d'un STAD est puni de 3 ans d'emprisonnement et de 30 000 euros d'amende » (L 323-2).
    L'entrave peut découler de l'insertion d'une bombe logique, de la destruction de fichiers, de programmes ou de sauvegarde, d'un encombrement de la capacité mémoire qui provoquent une perturbation du système. Cela a pour conséquence de faire produire au système un résultat différent de celui qui était attendu : blocage d'appel d'un programme, d'un fichier, altération de l'un des éléments du système.
  - Altération de fichiers: le fait d'introduire frauduleusement des données dans un STAD ou de supprimer ou de modifier les données qu'il contient est puni de 3 ans d'emprisonnement et de 45 000 euros d'amende (L 323-3).
    Toute manipulation de données qu'il s'agisse de les introduire, de les supprimer, de les modifier ou de les maquiller provoque une altération des fichiers.
  - Modalités de la répression
    L'article L 323-7 punit la tentative de délits informatiques des mêmes peines que celles des délits auxquels elle se rapporte afin de dissuader les fraudeurs dès le stade de l'essai, L 323-4 prévoit que la participation à un groupement formé ou à une entente établie en vue de la préparation caractérisée par un ou plusieurs faits d'une ou plusieurs infractions est punie des mêmes peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

4. Les obligations légales à la charge de l'entreprise

- ✓ En matière de protection des DCP
  Les DCP sont distinctes des autres informations présentes dans le SI de l'entreprise. Tout responsable de traitement a l'obligation légale (loi Godfrain) de les protéger. Le non-respect serait une faute sanctionnée par les autorités et la justice. La protection des données à caractère personnel est un droit fondamental pour les personnes et une obligation pour les entreprises (loi informatique et libertés de 1978 rénovée en 2004 ; convention européenne des droits de l'homme, TFUE de 2007).
  Une donnée à caractère personnel (DCP) est *« toute information relative à une personne physique, identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou 1 ou plusieurs éléments qui lui sont propres »* (nom, numéro de sécurité sociale, numéro de carte bancaire…).
  *Certaines de ces données (c'est notamment le cas pour les informations relatives à l'origine raciale ou ethnique, à la santé ou à la sexualité, les informations relatives à l'ADN, les empreintes digitales ou échantillons biologiques) sont des informations sensibles.
  Différentes obligations pèsent sur le responsable de traitement lors de la collecte et du traitement des DCP * :

- Obligation de loyauté
  - la collecte et le traitement de données personnelles doivent être effectués de façon licite et loyale.
  - les finalités du traitement doivent être « déterminées, explicites et légitimes ».
  - le responsable du traitement doit déclarer son fichier à une autorité administrative indépendante, la Commission Nationale Informatique et Liberté (CNIL). Certains fichiers requièrent même une autorisation expresse de la CNIL (traitement prévu à des fins de recherche dans le domaine de la santé par exemple).
- Obligation de sécurité :

  Mise en œuvre des mesures techniques pour protéger les DCP (changement régulier de mot de passe, procédure rigoureuse pour créer et supprimer les comptes utilisateurs, sécurisation des postes de travail, identification des personnes habilitées à accéder aux fichiers…
- Obligation lors du traitement de données à caractère personnel
  - Obtention du consentement préalable de la personne dont les DCP sont collectées (sauf exception) et information de ces personnes sur leurs droits d'opposition, d'accès, de rectification et de suppression
  - Interdiction de collecter des données sensibles (relatives aux mœurs, opinions politiques, origine ethnique, religion, appartenance syndicale… Voir supra) sauf consentement expresse de l'intéressé
- Obligation d'archiver les DCP de sorte à les conserver intactes dans le temps
  - En cas de conservation en interne, il convient d'élaborer une charte concernant les bonnes pratiques à adopter
  - En cas de conservation externe, le tiers archiveur doit prendre toute mesure propre à garantir que les DCP figurant dans les documents archivés soient accessibles aux seules personnes habilitées et que celles-ci ne soient pas modifiées ou endommagées.

✓ En matière de preuve numérique :

Dans un contexte de dématérialisation des processus et des informations, la preuve numérique devient primordiale. L'organisation de la collecte de la preuve numérique est une obligation légale :

- Obligation de conservation des contrats électroniques B to C : la loi du 21 mars 2004 prévoit que les contrats portant sur une somme supérieure à 120 euros doivent être conservés durant 10 ans.
- Les durées de conservation sont variables selon les documents (30 ans à 6 mois).
- Pour être admis en tant que preuve le document archivé doit être la copie numérique du document original.

NB : *Les entreprises confient très souvent l'archivage à un tiers. Dans ce cas elles recourent aux conventions de preuve afin de définir les modalités des preuves admissibles dans le cadre de leurs relations (EDI et l'enregistrement des preuves).*

**Constitue un traitement de données à caractère personnel, toute opération ou ensemble d'opérations portant sur des données personnelles, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction".*

En résumé :

Le SI est devenu stratégique et les données qu'il contient doivent être protégées dans l'intérêt de l'organisation afin qu'elle puisse poursuivre son activité et dans l'intérêt de toutes les personnes concernées.

Les exemples pour illustrer :

La Cnil vient de publier un guide destiné à la gestion des risques et comportant une méthodologie de gestion des risques liés au traitement des DCP.

Des spécialistes du droit proposent un service d'audit aux entreprises :

http://www.colbert-avocats.com/services/expertise-sectorielle/audit-informatique-et-libertes.html?lang=US