SSI : quand sécurité rime avec responsabilité !

Marie Barel - Juriste,
consultant spécialisé TIC/SSI

LinKS Conseil

Introduction : le contexte actuel

- Des professionnels de la SSI dans la tourmente

  - Nouvelles lois, nouvelles contraintes et nouvelles sources de responsabilité
  - La nécessité d'appréhender de nouveaux risques faisant appel à des compétences plus larges
  - Des responsabilités en cascade : civile ou pénale, personnelle ou du fait d'autrui, avec ou sans faute, ...

Analyse de cas (1)

- **Scenario 1** : responsabilité *du fait d'un préjudice causé à un tiers* au travers du système d'information

- Exemple de la défaillance de la sécurité du système causant une perte de données à caractère personnel
  - Longue chronique d'actualités sur ce sujet : pour une gestion responsabilisante
  - Art. 34 de la LIL (modifiée par la loi du 6.8.2004) / art.226-17 CP (5 ans d'emprisonnement et 300.000 euros d'amende)
  - **L'affaire Kitetoa** : la sécurité du système comme condition de l'incrimination d'accès frauduleux ?

Analyse de cas (2)

- **Hypothèse de l'attaque par rebond** : exemple de serveurs de messagerie mal configurés utilisés comme relais pour la propagation d'un virus dissimulé dans un mail à caractère de *spam*

  - Responsabilité pénale et intention délictueuse
  - Responsabilité civile en vue de la réparation du dommage : la faute non intentionnelle
  - Organisation de la preuve de son innocence et posture de « poursuivant »

Analyse de cas (3)

- **Scénario 2** : responsabilité engagée *du fait des agissements d'un salarié*

- L'employeur, responsable civilement : l'affaire LUCENT TECHNOLOGIES

  TGI Marseille, 11 juin 2003 / CA Aix-en-Provence, 13 mars 2006 (confirmation) – http://www.legalis.net/jurisprudence-decision.php3?id_article=1611

- La responsabilité du commettant du fait de ses préposés : article 1384 alinéa 5 du Code civil
  - Conditions d'exonération (AP, 19 mai 1988): le salarié a agi …
    - i – *hors des fonctions* auxquelles il est employé,
    - ii – *sans autorisation* et
    - iii – *à des fins étrangères* à ses attributions.
  - Crim., 23 juin 1988 : est dans l'exercice de ses fonctions le salarié qui a trouvé dans son emploi « *l'occasion et les moyens de sa faute* ».
- De l'importance de la qualité des chartes d'usage des ressources informatiques

Analyse de cas (4)

- Comportement *délictueux* du salarié accompli dans le cadre de son emploi
- Une hypothétique condamnation de l'entreprise et son dirigeant sur le fondement de l'obligation de surveillance et de contrôle interne : des conditions difficiles à remplir
  - Preuve de la participation intentionnelle de l'employeur à la commission de l'infraction
    - Salarié ayant agi à l'insu de ce dernier : exit la coaction
    - La complicité écartée faute d'une « *participation volontaire et consciente de l'aide apportée* » (T.corr. Lyon, 19 déc. 1983), « *une simple négligence ne pouvant être assimilée à une participation intentionnelle* » (Crim., 6 déc. 1989)
  - Exemple du téléchargement d'images pédophiles par un salarié sur l'Internet : **Tribunal correctionnel du Mans, 16 février 1998**
    - Intérêt à « se placer du côté des poursuivants » en dénonçant les agissements délictueux : l'abstention ou le silence « en connaissance de cause » susceptible de se transformer en « aide ou assistance »

Analyse de cas (5)

- **Scenario 3** : responsabilité engagée *du fait des mesures de cybersurveillance* opérées sur le réseau d'entreprise
  - La licéité des contrôles : un fragile équilibre entre respect des droits du salarié et droit de surveillance de l'employeur

    - Exemple du contrôle de la messagerie : **TGI Paris, 2 nov. 2000 ; CA Paris, 17 déc. 2001 (affaire du laboratoire PNMH – Charte Renater)**
      - Notion d'**interception illégale** de correspondances (art.226-15 C.Pén.) et accès au contenu des messages
      - **Limites de la mission de contrôle** des administrateurs réseaux en charge des opérations de surveillance

    - Divulgation de contenu et devoir de confidentialité

    - Question en suspens : comment réagir face à la constatation de faits graves ou répétés, préjudiciables à l'entreprise (voire à un tiers) et nécessitant des mesures d'investigation *non contradictoires* ?

Analyse de cas (6)

- Exemple de l'opération commando « bureau propre » : **Cass.soc., 17 mai 2005** - http://www.droit-tic.com/juris/aff.php?id_juris=29
  - Faits de l'espèce :
    - Découverte de photos *érotiques** dans le tiroir du bureau d'un salarié *absent*
    - Recherche sur le disque dur du PC de fichiers de nature similaire
    - « Ensemble de dossiers totalement étrangers (aux) fonctions figurant sous un fichier intitulé 'perso' » et ayant motivé un licenciement pour faute grave
  - Attendu de principe : « *l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus dans le disque dur de l'ordinateur qu'en présence de ce dernier ou celui-ci dûment appelé* », à moins que cela ne soit justifié par un *« risque ou évènement particulier. »*
    - Respect du contradictoire
    - Sauf (// jurisprudence en matière de fouille sur le lieu de travail) :
      * atteinte à la sécurité de l'entreprise
      * degré de gravité certain
      * caractère d'urgence

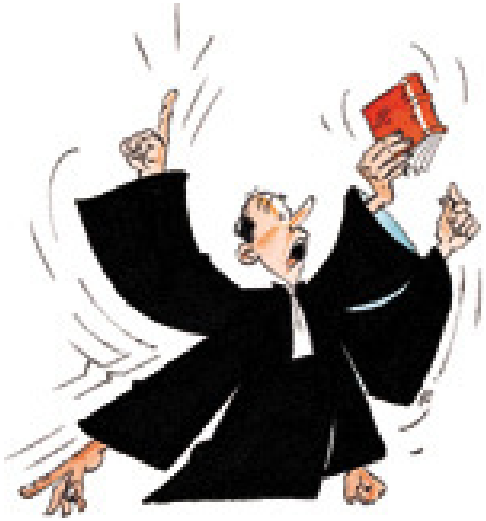
Remarque : sur la possession et la consultation d'images érotiques ou pornographiques.

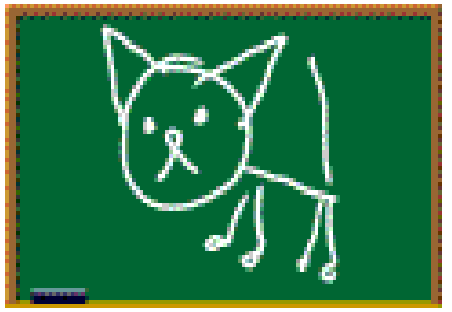
Analyse de cas (7)

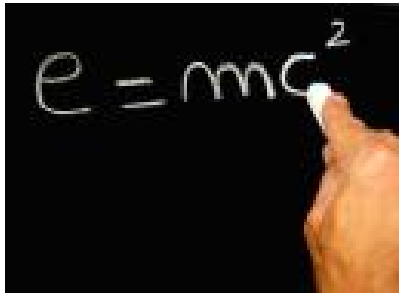
- **Scenario 4** : responsabilité engagée *du fait d'un défaut de conformité à la réglementation*

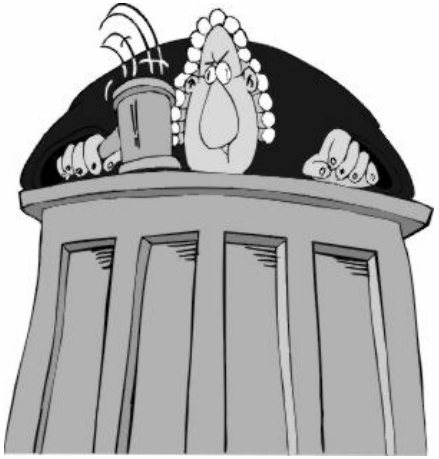
  - Exemples divers
    - Dispositions relatives à la collecte, la conservation …, les flux transfrontaliers de données à caractère personnel (loi n°2004-801 du 6 août 2004, article 14)
    - Obligations en matière de conservation des données techniques de connexion (loi du 15 nov. 2001 ; décret d'application du 24 mars 2006)
    - Règles en matière de contrôle l'export, (parfois) l'import, la fourniture et l'usage de biens de cryptologie (Loi n°2004-575 du 21 juin 2004 « LCEN », Titre III, chapitre 1er)
    - …
  - DSI/RSSI en charge de l'application des textes : conditions d'une délégation de pouvoir valide et d'un transfert de responsabilité du chef d'entreprise vers les *managers* de niveau intermédiaire.
    - Autorité
    - Compétences
    - Moyens
  - Délégation précise et ayant un caractère de permanence, information sur les conséquences de la délégation
  - Sub-délégation possible **(Crim, 30 octobre 1996)**

Bilan : « responsables mais pas coupables » ☹









Conclusion : gardez la maîtrise !

- PGRJ (Politique de Gestion des Risques Juridiques)
  1. Cartographie dans toutes les ressources de l'entreprise des risques potentiels et obligations au regard des spécificités de l'activité
  2. Définition du niveau de risque acceptable (stratégie, environnement technique, commercial, humain)
  3. Traitement du risque (réduction) et gestion du risque résiduel (assurance e.g.)

  - Outils : Tableau de bord des risques juridiques, Chartes, Veille, Formation et sensibilisation des collaborateurs, …
  - Ressources spécialisées : CIL & co

CONTACT

Marie BAREL, *Links conseil*

Expertise TIC/SSI

marie.barel@legalis.net