

*Revue d'actualité juridique
de la sécurité du Système d'information*

Me Raphaël PEUCHOT, avocat associé
FOURMANN & PEUCHOT

16 mars 2011

THÈMES ABORDÉS :

1. Cloud computing : les limites juridiques de l'offre technique
2. Cybersurveillance des salariés : nouvelles avancées
3. Usurpation d'identité : « *ça n'arrive pas qu'aux autres* » !
4. Preuves sur Internet : les règles de validité
5. Contrats informatiques : quelles limitations de responsabilité ?
6. Introduction frauduleuse de données sur le SI : affaire Kerviel

1. Cloud computing : les contraintes juridiques

Rappel : le cloud induit une diffusion de l'information et des données sans localisation possible par le client...voire même par le cloud provider ...

Deux questions : - le recours au cloud est-il totalement légal ?
- quelles précautions contractuelles prendre ?

- **Légalité du recours au cloud computing**

1/Règles légales applicables

Loi Informatique et Libertés du 6/01/1978 (modif. 6/08/2004)

Dir. CE 95/46 du 24/10/1995

2/Principes

- **art. 68** : l'export de données à caractère personnel hors de la CE n'est possible que si le pays de destination des données « *assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard des traitements dont ces données font l'objet ou peuvent faire l'objet* ».
- critères d'appréciation: lois en vigueur, mesures de sécurité, caractéristiques du traitement (finalité, durée, origine et destination des données).
- si export vers un pays conforme: simple déclaration à la CNIL
- sinon – **art. 69** : autorisation préalable de la CNIL sur la base d'un contrat ou de règles internes dans le cas de transferts de données intra-groupe (BCR)

3/ Application au cloud

- en présence d'un flux de données transfrontière: définition même de la technique du cloud.
- Y-a-t-il néanmoins « transfert » de données au sens de la loi ?
- qui est « responsable du traitement » ? Qui est « sous-traitant »
- en présence de données personnelles : même si le flux ne porte pas prioritairement sur de telle données, l'export d'une seule donnée à caractère personnelle impose le respect de la loi.

- **Précautions contractuelles**

- clause de confidentialité stricte
- clause de sécurité des données : intégrité, disponibilité, auditabilité
- localisation géographique des données : exclusions géographiques
- modalités de restitution: délai, format, transfert à tiers
- déterminer la loi applicable
- modalités techniques envisageables, sous réserve : cryptage, anonymisation

2. Cybersurveillance des salariés

- **Cour d'appel de Lyon 31 mars 2010**
 - les messages classés dans « éléments envoyés » ne présentent pas, de ce seul fait, un caractère personnel et sont donc présumés professionnels.
 - liberté de consultation de l'employeur : contrôle de routine de l'adm. réseau.
- **Cassation Soc. 9 février 2010**
 - les connexions à des sites, dont la liste est portée dans un répertoire « favoris » sont présumées à caractère professionnel.
 - assimilation progressive du régime des connexions à celui des fichiers : double régime selon l'identification du caractère « personnel ».

- **Cass. Soc. 14 avril 2010**

- le fait de recevoir des courriels à caractère pornographiques sur son ordinateur professionnel n'est pas constitutif d'une faute du salarié dès lors qu'ils n'ont été ni sollicités ni enregistrés.
- un licenciement pour faute grave doit répondre à la commission d'une faute du salarié.
- préconisation : bien libeller la charte informatique pour organiser les contrôles et prévoir les obligations des salariés.

- **Cassation Soc. 15 déc. 2010**

- l'utilisation de la messagerie pour l'envoi et la réception de message à caractère pornographique et la conservation sur son disque dur d'un nombre conséquent de tels fichiers (« collection ») constitue un manquement délibéré et répété du salarié à l'interdiction posée dans la charte informatique.
- licenciement pour faute grave.
- attention aux définitions : « pornographique », « nombre conséquent »

- **Cour d'appel de Dijon, 14 sept. 2010 : géolocalisation**

- faits : conduite véhicule de société hors des horaires autorisés + infractions au code de la route.

- la géolocalisation des salariés impose le respect de deux obligations légales:

- . L'information préalable des salariés : art. L. 1222-4 CT : « *Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance* ».

- . La déclaration des traitements de données à la CNIL : sauf norme simplifiée n°51 (finalités du traitement, données traitées, destinataires, durée de conservation).

3. Usurpation d'identité

- **Exemples de circonstances d'usurpation**

- RP
- Tribunal de grande instance de Paris, 24 nov. 2010

- **Législation applicable**

- art. 226-4-1 Code pénal: « *Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15.000 € d'amende* ».

- difficultés d'application probables

4. Preuves sur internet

- **Présomption de validité d'une signature dite « électronique »**

- articles 1316-1 du Code civil : « *L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ».

- Cassation 1^{ère} Ch. 30 sept. 2010

- **Constat d'huissier sur internet**

- conditions de validité

- modalités des constats sur le réseau informatique d'une entreprise

5. Clauses limitatives de responsabilité

- **Cassation Com. 29 juin 2010**

- faits : limitation de l'indemnité de responsabilité au montant du coût de la prestation.

- est réputée non écrite la clause limitative de réparation qui contredit la portée de l'obligation essentielle.

- précautions contractuelles:

- . Exiger en amont de la négociation la police d'assurance RC

- . Exclure toute clause limitative de responsabilité,

- . À tout le moins, la plafonner au montant de la couverture d'assurance

6. Affaire Kerviel

- **Tribunal correctionnel de Paris, 5 octobre 2010**
 - faits : introduction de données fictives sur le réseau informatique de la banque
 - infraction pénale : art. 323-3 CP : « *Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75.000 € d'amende* ».
 - élément matériel / élément moral de l'infraction

Merci de votre attention !