CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Sécurité des Applications Web
Conférence CLUSIF
15 décembre 2011

Les enjeux réglementaires de la protection des informations en ligne

Garance MATHIAS
Avocat

Dématérialisation des données et informations

- Tous les domaines d'activité font appel à des applications web (télémédecine, administrations, banques, entreprises…)

- Modernisation des systèmes d'informations

- Plusieurs problématiques quant :
  - Au respect des droits des patients, administrés, clients…
  - À la sécurité et confidentialité des données
  - À la pérennité et interopérabilité des systèmes d'informations

L'information est une « notion fuyante »

Notion non définie juridiquement

Difficultés à distinguer l'information de son support matériel

Quid de l'identité numérique.

Quid de l'intelligence économique.

Information versus Sécurité et Vie privée : Comment concilier ces deux aspects ?

La définition du patrimoine informationnel

Selon le CIGREF, le patrimoine informationnel est l'ensemble des données et des connaissances, protégées ou non, valorisables ou historiques d'une personne physique ou morale.

L'information est omniprésente, dans tous les systèmes, dans toutes les applications.

Les enjeux juridiques sont cruciaux.

Le patrimoine informationnel de l'entreprise

Protection juridique : propriété intellectuelle, clause de non-concurrence, clause de confidentialité

Protection organisationnelle : sécurisation des locaux de l'entreprise

Protection logique : sécurité des systèmes informatiques

Protection humaine : développement d'une culture de protection, vigilance accrue par rapport au personnel

Enjeux de la protection des informations en ligne

- Risques économiques et financiers (restauration des données par exemple)
- Risque en termes d'image (clientèle)
- Perte de la confidentialité des informations
- Risque de responsabilité civile du fait de préjudices causés à des tiers

ETAT DES LIEUX

- Le risque légal est la conséquence du risque opérationnel
- Le risque métier est de fait induit par le risque informationnel
- La sécurité des systèmes d'information vise 4 grands objectifs:
  - Disponibilité
  - Intégrité des données
  - Confidentialité
  - Preuve

L'évaluation des risques pesant sur les systèmes d'information permet de réduire les risques métiers et les risques légaux.

Le patrimoine informationnel de l'entreprise

Mesures de sécurité indispensables visant la protection des informations:

- Dès la création ou la collecte
- Pendant la phase de transmission
- Pendant la phase de conservation / archivage

La politique de sécurité doit être définie tant pour la prévention que pour la protection.

Protection des informations à travers les contrats

Responsabilité du chef d'entreprise face à son patrimoine:

-Outils juridiques: la politique de sécurité des systèmes d'information et d'archivage, les chartes d'utilisation des communications électroniques, les contrats de travail, les contrats avec les prestataires de services, les obligations de confidentialité et les conditions destinées à l'usage du chiffrement

- Droits de propriété intellectuelle susceptibles de protéger l'information (droit d'auteur, droit des brevets d'invention, droit des marques, droit des dessins et modèles)

Protection de l'information et vol

Article 311-1 du code pénal:

« *Le vol est la soustraction frauduleuse de la chose d'autrui*. »

MAIS

Pas de reconnaissance de « vol d'informations » ni par le législateur, ni par les tribunaux.

Possible sanction du recel d'informations sur le fondement de **l'article 321-1 du code pénal**:

« *Le recel est le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit.*

Constitue également un recel le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit.

Le recel est puni de cinq ans d'emprisonnement et de 375000 euros d'amende. »

Protection offerte à certaines catégories de données

- Données à caractère personnel (Loi Informatique et Liberté)

- Données relatives à certains types d'activité (défense nationale)

- Etc.

Protection de l'identité numérique

- Éléments d'authentification: ID, adresse IP, email, password, nom, prénom…

- Données : personnelles, administratives, bancaires, professionnelles…

- Signes de reconnaissance: photographies, logos, graphismes…

- Traces numériques: tags, liens, publications…

L'usurpation d'identité

Selon l'article 226-4-1 du 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.*

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. »

Cette infraction est venue combler un vide juridique

La tentative est punie au même titre de que l'usurpation elle-même.

Les dispositions de la Loi Informatique et Liberté portant sur la sécurité

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès (article 34 de la loi).

Article 226-17 du Code pénal : *Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.*

En quoi consiste cette obligation?

Prendre toutes précautions utiles

Au regard de la nature des données

Et des risques présentés par le traitement

Pour préserver la sécurité des données et, notamment, empêcher qu'elles soient:

- Déformées
- Endommagées
- Ou que des tiers non autorisés y aient accès

Qu'est ce qu'un tiers non autorisé ?

Des personnes externes à l'organisme

Des personnes internes à l'organisme

Le cas particulier des professions soumises à une obligation de secret professionnel

Les autorités judiciaires ou administratives peuvent elles être des tiers non autorisés lorsqu'elles ne sont pas habilitées à recevoir les données ?

L'information et la gestion des applications web

Les moyens à la disposition des personnes dont les données personnelles font l'objet d'un traitement

L'enjeu des données à caractère personnel et de leur transfert

Droits d'opposition, d'accès et de rectification

Loi Informatique et Libertés:

-Information de la personne concernée de ses droits et de leurs modalités d'exercice lors de la mise en œuvre du traitement, y compris *« lorsque les données à caractère personnel n'ont pas été recueillies auprès d'elle »*.

- Le responsable du traitement doit fournir toutes ces informations dès l'enregistrement des données ou lors de la première communication des données.

Les enjeux des transferts de données à travers les applications web

Au niveau national:

- Respect du secret bancaire ou médical
- Respect de la Loi Informatique et Libertés
- Le comité d'entreprise doit être consulté par l'employeur en cas d'introduction d'une nouvelle technologie dans l'entreprise (art. L.2323-13 du code du travail)

Au niveau international:

- Selon la localisation des données, des lois étrangères peuvent trouver à s'appliquer (par exemple le Patriot Act)
- Intra-UE : informations sur la déclaration CNIL + information de la personne concernée si transfert à destination d'un responsable de traitement
- Hors UE dans des pays de niveau de protection suffisant suivant le régime intra-UE
- Hors UE dans des pays n'offrant pas un niveau de protection suffisant : autorisation CNIL sur présentation du contrat de transfert + éventuelle autorisation de la personne concernée

La CNIL impose une sélection, toutes les données des salariés ne peuvent pas être transférées sans nécessité (notamment coordonnées bancaires, situation familiale, etc.)

Les failles de sécurité

Article 38 de l'ordonnance du 24 août 2011 : l'obligation d'une notification des failles de sécurité

« *En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit, sans délai, la Commission nationale de l'informatique et des libertés. Lorsque cette violation peut porter atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique, le fournisseur avertit également, sans délai, l'intéressé.* »

Notion de « fournisseur de services de communications électroniques »?

- Nécessaires précisions par les Tribunaux.

Exceptions:

« *La notification d'une violation des données à caractère personnel à l'intéressé n'est toutefois pas nécessaire si la Commission nationale de l'informatique et des libertés a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation.* »

Sanctions en cas de violation de l'obligation de notifications du ressort de la CNIL:

- 150.000 €
- 300.000 € en cas de récidive

Risque d'image:

- Possibilité de publication de la décision de la CNIL

Les données de connexion

Notion des données de connexion: les informations produites ou nécessitées par l'utilisation des réseaux de communication électroniques, qu'il s'agisse des communications téléphoniques ou des connexions au réseau Internet (données de trafic, de localisation, de facturation, etc.)

Article II de l'article 6 de la LCEN: obligation pour les fournisseurs d'accès à Internet et les fournisseurs d'hébergement de détenir, de conserver les données de nature à permettre l'identification de toute personne physique ou morale ayant contribué à la création d'un contenu mis en ligne ;

Article II bis de l'article 6 de la LCEN: obligation de mise à disposition de ces données aux agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales en charge de la lutte contre le terrorisme.

Le décret du 25 février 2011 vise à organiser la conservation et la communication des données permettant d'identifier toute personne ayant contribué à à la création d'un contenu mis en ligne.

Tous les hébergeurs de blogs, forums, réseaux sociaux, de manière générale, tous les acteurs du WEB 2.0 sont soumis à ces obligations.

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CONCLUSION / QUESTIONS