Forum annuel CERT-IST 2010
3 juin 2010

INCIDENTS DE SECURITE : cadre juridique et responsabilités de l'entreprise

Eric A. CAPRIOLI - François COUPEZ

Avocat associé **Avocats à la Cour**
Docteur en droit

Le cabinet Caprioli & Associés est une société d'avocats en droit des affaires (privé et public) située à Paris et à Nice.

- Il est **spécialisé dans** :
  - L'informatique, les technologies de l'information et des communications électroniques
  - La sécurité des systèmes d'information et la dématérialisation
  - les propriétés intellectuelles (droit d'auteur, marques, dessins, brevets, logiciels, bases de données, …)

- Adresses : **6, rue Saulnier, 75009 Paris**
  9, avenue Henri Matisse, 06200 Nice
- Site Web : **www.caprioli-avocats.com**
- Mél : **contact@caprioli-avocats.com (Nice)**
  paris@caprioli-avocats.com (Paris)

Notion d'« Incidents de sécurité » ici :

- = Menace concrétisée affectant le fonctionnement d'un SI (selon DICP)
- Cet incident peut concerner tout type de données *a priori* **mais aussi le SI en lui-même** (323-1 et s. C. pénal – non traité ici)
- **Certaines données sont juridiquement plus protégées que d'autres**…
- … mais tout incident peut avoir des conséquences juridiques **plus indirectes**

Le secteur le plus régulé : le secteur financier

- En France, article 14 du Règlement n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement
- Un niveau de sécurité :
  - ✓ « *jugé souhaitable par rapport aux exigences* » du métier
  - ✓ périodiquement apprécié avec les actions correctrices entreprises
  - ✓ qui préserve « en toutes circonstances » l'intégrité et la confidentialité des informations
- Des exigences également en matière de secret professionnel
- Ailleurs, des règlementations (GLB Act, etc.) et des régulateurs (SEC, FSA, etc.) tout aussi exigeants

Les obligations de confidentialité par secteurs

- Secret professionnel (secret médical, secret bancaire, etc.)
- Des textes spécifiques, un SI qui doit prendre en compte ces impératifs :
  - ✓ messageries des avocats, conservation des données médicales, etc.
- SANCTIONS en cas d'atteintes
  - ✓ pénale : un an d'emprisonnement et 15 000 € d'amende, soit **75 000 € pour une personne morale** (art. 226-13 du Code pénal)
  - ✓ sanction des régulateurs des domaines concernés **pouvant aller jusqu'au retrait de la possibilité d'exercer**

De façon générale, dans les autres secteurs, cela dépend du type d'information accédée : les données à caractère personnel

Si les données accédées étaient des DCP

- La loi de 1978 modifiée dite « Informatique et Libertés » s'applique aux **données à caractère personnel**…
  - ✓ toute information relative à une **personne physique**
  - ✓ identifiée ou susceptible de l'être, **directement ou indirectement**
- … qui sont **traitées**, collectées, enregistrées, utilisées, etc. (**définition TRES large**) de façon automatisée ou non…
- … contenues ou appelées à figurer dans des **fichiers**…
- et dont le responsable est celui qui détermine les **finalités et les moyens**

Ex : plaques minéralogiques, données biométriques… adresse IP ?

Si les données accédées étaient des DCP

- Entre autres obligations, le responsable de traitement doit préserver la sécurité, la confidentialité et l'intégrité des DCP

« *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*** »

- ✓ Sanction pénale (art. 226-17 C. pén : 5 ans / 300 000 euros **et 1 500 000 EUR pour une entreprise**)
- ✓ **Sanctions de la CNIL, notamment pécuniaires**

- **Des sanctions peu appliquées en pratique ?**

La Data Breach Notification

- **Aux USA : la sanction par « mise au pilori »**
- En découle des coûts importants (200 $ par information concernée) , une perte de clientèle, des risques de procès…

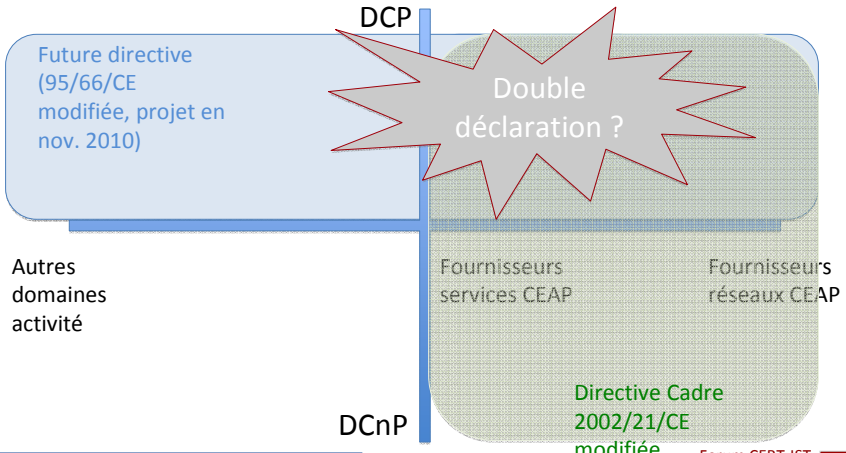
Les suites de l'exemple américain

- Un Etat (Californie) en 2003, 45 Etats US en 2010, une réglementation qui a essaimé à l'international.
- Les exemples européens en quelques traits :
  - ✓ Allemagne : notification *immédiate,* « significant harm », données sensibles, protégées, etc.
  - ✓ Espagne : procédure de notification et de gestion des incidents avec registre interne
  - ✓ Autriche : notification (au choix de la seule entreprise), « ***systematic*** *and seriously wrongful use of* », sauf effort disproportionné par rapport au coût ou aux risques
  - ✓ etc. (débats en Belgique, annonce aux Pays Bas, etc.)
  - ✓ Les directives européennes du Paquet Télécom (2002/58 et 2002/21 modifiées)
- **Une impossible harmonisation des procédures au niveau international ?**

Les conséquences à l'international

- Une **balkanisation** de l'obligation de notification
  - ✓ Notifier oui, mais auprès de qui ? Plusieurs fois ? **Quid du droit applicable, des personnes concernées ?**
  - ✓ Seulement les données personnelles accédées ?
  - ✓ Pour toutes les DCP ? Seulement les données financières ? Sensibles ? Secrètes ?
  - ✓ Et si elles étaient chiffrées ? Et s'il n'y avait pas eu de conséquences à cet incident ?
- Conséquences
  - ✓ Obligation de notifier les clients **individuellement** dans certains cas
  - ✓ **Coût** important (plusieurs millions de dollars) et atteinte à l'image de l'entreprise
  - ✓ **Des procédures (contrôles internes, remontée d'incident, organisation, gestion de crise, etc.) derrière la procédure de notification !**

Une harmonisation difficile, l'exemple européen



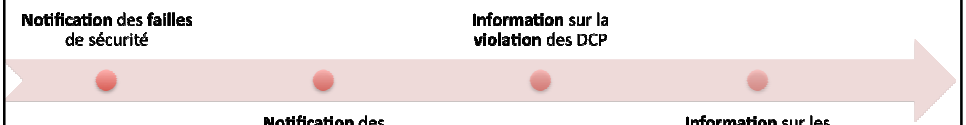
En France, le projet de loi « visant à mieux garantir le droit à la vie privée à l'heure du numérique »

- Adopté au Sénat le 23 mars 2009 en 1ère lecture
- Comporte de nombreux articles, dont l'article 7 :
  - ✓ Modifie l'article 34 et **renvoie à un décret d'application**
  - ✓ **Rend obligatoire la notification des violations du traitement des DCP**
  - ✓ **Information du CIL et de la CNIL**
  - ✓ **Information des personnes prévue**
- L'opposition du gouvernement : les raisons
- **Vers une obligation en 2011 en France ?**

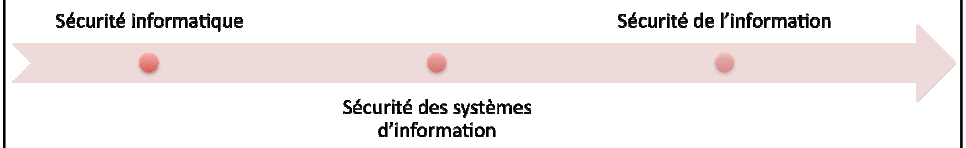
Enseignements tirés des exemples étrangers

- Le seul risque de compromission des données ? (FSA – Merchant Security 06/08)
  - ✓ Contrôle de routine et nombreux manquements à la sécurité, procédures peu sécurisées (messagerie instantanée ou webmail non interdits, etc.)
  - ✓ sanction de 77 000 EUR (110 000 EUR en l'absence d'accord)
  - ✓ Aucun incident relevé
  - ✓ Une application discutable en France, sauf milieu financier
- Même en l'absence de préjudice ?
- Cas les plus divers (installation de logiciels de P2P, perte ou vols d'ordinateurs, déchets électroniques non « nettoyés », piratage interne, externe, etc.)
- Y compris des hypothèses de notifications plus fantaisistes (cas en Allemagne)
- Multiplication des cas en France prévisible : que faudra-t-il faire ?

A noter : le glissement sémantique



Qui en rappelle un autre…



Que faire : ce que prévoit la directive 2002/58

- Elle s'applique aux violations de données personnelles (sur papier ou électroniques) en cas d'accès non autorisé, illicite ou de perte
- La « notification » **de toute violation de DCP** aux autorités oui, mais pas forcément aux victimes personnes physiques (**seulement si la violation affecte négativement leurs DCP ou leur vie privée**)
  - ✓ atteinte physique, humiliation significative, atteinte à la réputation
- Les informations notifiées : les points de contact mis en place… **La charrue avant les bœufs ?**
- L'exception à la notification : DCP rendues « **techniquement incompréhensibles** »
- L'exception de l'exception : prouver ***a posteriori*** l'efficacité du dispositif, ***« à la satisfaction de l'autorité compétente »***

Que faudra-t-il faire : ce que prévoit la directive

- Le reste ? Circonstances ? Formats ? Procédures ?
- Sera détaillé par l'Union Européenne en procédure de comitologie avec consultation
  - ✓ de l'ENISA
  - ✓ du Groupe dit « de l'article 29 » (rassemblant les « CNIL européennes »)
  - ✓ du Commissaire Européen à la Protection des Données
- Appui sur « d'éventuelles normes européennes ou internationales existantes »
- **Rien n'était lancé au 1er avril 2010**

Limiter les risques :

- Chiffrer / Anonymiser / Détruire / Ne pas collecter… **ou en tout cas cibler les données à caractère personnel conservées**
- **Renforcer les contrôles internes et la traçabilité**
- **Responsabiliser et sanctionner les fautifs**
  - ✓ Renforcer au besoin (et surtout faire appliquer) les chartes internes
  - ✓ Renforcer les garanties juridiques afférentes aux contrats d'externalisation (cloud computing, etc.)
- **Etablir et répéter les procédures d'urgence**

Pour finir, gare aux conséquences juridiques « indirectes » de l'incident de sécurité !

- Mise en cause de la responsabilité contractuelle ?
  - ✓ Une entreprise du secteur industriel passe un contrat pour une solution anti-virus ;
  - ✓ Infectée par un virus, elle le résilie de façon anticipée ;
  - ✓ Rapport sur la connexion à des sites pornographiques et pirates
  - ✓ CA Paris 4 mai 2007 : « *Considérant que la société DMS, en laissant son personnel se connecter à de tels sites,* ***a rendu, par sa faute, inefficace la protection que la société Normaction s'était engagée à lui fournir*** *de sorte qu'elle ne pouvait invoquer la défaillance de la protection anti-virus comme un juste motif de la résiliation des contrats* »
  - ✓ **« Que cette résiliation intervenue à son initiative lui est donc imputable »**

Les conséquences juridiques indirectes de l'incident de sécurité : la coupure d'accès à internet

- ✓ Lois « favorisant la diffusion et la protection de la création sur internet » du 12 juin 2009 (Hadopi 1) et « relative à la protection pénale de la propriété littéraire et artistique sur internet » du 28 octobre 2009 (Hadopi 2)
- ✓ La « riposte graduée » : un concept **inadapté aux entreprises** ?
- ✓ L'applicabilité aux entreprises ? **Le gouvernement l'affirme !**
- ✓ Une obligation : la **sécurisation** du réseau de l'entreprise
- ✓ L'injonction de sécurisation… au maximum ?
- ✓ Une sanction : la **coupure** de l'accès à l'internet !
- ✓ **Des logiciels de sécurité labellisés… pour les entreprises ??**

Avez-vous des questions ?

Merci de votre attention !

Eric A. CAPRIOLI
Avocat associé
Docteur en droit
e.caprioli@caprioli-avocats.com

François COUPEZ
Avocat à la Cour
f.coupez@caprioli-avocats.com

Société d'avocats
6 rue Saulnier, 75009 Paris / Tél. 01 47 70 22 12
9 avenue Henri Matisse, 06200 Nice / Tél. 04 93 83 31 31
www.caprioli-avocats.com
mél : contactparis@caprioli-avocats.com