Confidentialité et cryptographie en entreprise

D’un « domaine réservé » à un autre !

Marie BAREL – Expert juridique SSI

1. Introduction

- La **fuite d'informations confidentielles**, un risque majeur pour l'entreprise
  - Une menace à la fois interne et externe (intelligence économique)
  - Des conséquences importantes
    - Perte de chiffre d'affaires, anéantissement de l'avantage technologique liés aux investissements R&D, affectation de la confiance des clients, etc.
    - Risque juridique : manquement à l'obligation de sécurité des données à caractère personnel (art. 226-17 C.Pénal)
- La **cryptographie** : **la réponse technique** à la problématique de la confidentialité des données

Agenda

- Introduction
- Vue synoptique de la réglementation en matière de cryptographie
  - Rappel historique des évolutions législatives
  - Etat de la réglementation en vigueur (loi du 21 juin 2004)

1. Cryptographie en entreprise : un domaine à réglementer !
2. Conclusion

2. Vue synoptique de la réglementation

2.1 Rappel historique

1. Le décret-loi de 1939 : « domaine réservé »

- La Science du Secret, un art ancien
- **Principe d'interdiction** : régime des «matériels de guerre, armes et munitions»

Ex. arme de 2ème catégorie : « équipements de brouillage, leurres et leurs systèmes de lancement »

- *Sauf dérogation gouvernementale autorisant la « déclassification » de certains matériels commerciaux*

2. Vue synoptique de la réglementation (2)

2.1 Rappel historique (suite)

2. Premier « tournant » : la « LRT » de 1990

- Distinction entre cryptographie à des fins de **confidentialité** et cryptographie à des fins d'**authentification** ou d'**intégrité > deux régimes distincts :**
  - Régime d'autorisation préalable des services du Premier Ministre
  - Régime de déclaration préalable
- Une **vision qui demeure sécuritaire**
  - Motifs de la loi de 1990 : « (…) pour préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat. »
  - Maintien d'un **contrôle étatique fort** (SCSSI) : obstacle aux écoutes administratives ou judiciaires, risque d'utilisation à des fins malveillantes (crime organisé, terrorisme), …
- Un **échec prévisible**
  - Contexte international : la France sur la même ligne que la Russie, la Chine, la Corée du Nord ou l'Iran s'agissant de l'utilisation des moyens de cryptologie !
  - Contexte technologique : facilité d'accès aux moyens de chiffrement (exemple de PGP ; plus récemment, Windows Vista®)

2. Vue synoptique de la réglementation (3)

- 2.1 Rappel historique (suite)

3. La loi sur les télécoms de 1996

- Un dispositif plus libéral mais aussi très formaliste : six régimes fonction des fonctionnalités, de la nature des actes et de la taille de l'algorithme >

• Liberté	• Déclaration simplifiée	• Substitution de la procédure de déclaration à la procédure d'autorisation
• Dispense de formalité préalable	• Déclaration préalable	• Autorisation préalable

- Mise en place du **système de « tiers de confiance »**
- Une loi **vivement critiquée** **et appelant de nouveaux assouplissements**
  - Complexité du dispositif et position isolée de la France sur la scène internationale
  - Pratique de la SCSSI

2. Vue synoptique de la réglementation (4)

- 2.2 Le régime issu de la LEN (> 2004)

- **Ce qui change…**
  - L'accent mis sur les '*moyens*' et non plus les '*prestations de cryptologie*' (cf. définition art.28 L.1990 remplacé par art. 29 LCEN)
  - Plus de distinction entre systèmes de cryptographie ni de référence à la taille des clés de chiffrement (objet de critiques)
  - **Libéralisation complète** de l'utilisation des moyens de cryptologie et aussi, quelle que soit la nature des opérations envisagées, de l'ensemble des moyens ou services« assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité »

UTILISATION

$$H_0^{(N)} || H_1^{(N)} || H_2^{(N)} || H_3^{(N)} || H_4^{(N)}$$

- **La liberté d'utilisation des moyens de cryptographie devient totale, tant pour les personnes physiques (usage personnel) que pour les personnes morales**

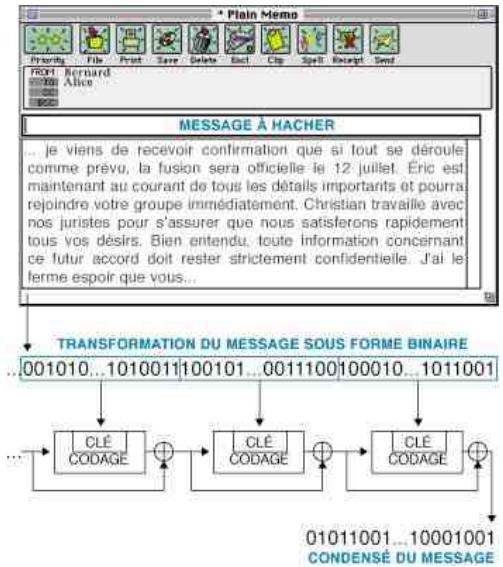
<table>
<tr><th colspan="4">AVANT</th><th>APRES</th></tr>
<tr><td>Authentification
Contrôle d'Intégrité</td><td colspan="3">Confidentialité
Longueur de clé</td><td rowspan="3">LIBRE
(art.30-I LEN)</td></tr>
<tr><td rowspan="2">LIBRE</td><td>< ou = 40 bits</td><td>< ou = 128 bits</td><td>> 128 bits</td></tr>
<tr><td>LIBRE</td><td>LIBRE *</td><td>AUTORISEE **/
LIBRE ***</td></tr>
</table>

***A condition**,
soit que lesdits matériels ou logiciels aient préalablement fait l'objet d'une déclaration par leur producteur, un fournisseur ou un importateur,
soit que lesdits matériels ou logiciels soient exclusivement destinés à l'usage privé d'une personne physique ;
Sinon, une déclaration d'utilisation personnelle doit être adressée à la DCSSI

****A condition** que lesdits matériels ou logiciels aient fait l'objet d'une autorisation de **fourniture en vue d'une utilisation générale**.

Sinon, une demande d'autorisation d'utilisation personnelle doit être adressée à la DCSSI.

*** Lorsque la clé est gérée par un tiers de confiance, l'utilisation de moyens de chiffrement offrant des services de confidentialité reposant sur des clés strictement supérieure à 128 bits est LIBRE. Le tiers de confiance est un organisme agréé par la DCSSI pour gérer les clés des utilisateurs ; il doit remettre les clés aux autorités judiciaires et de sécurité sur requête de leur part.



FOURNITURE

- **Simplification et allègement du dispositif**

AVANT				APRES	
Authentification Contrôle d'Intégrité	Confidentialité *Longueur de clé*			Authentification Contrôle d'intégrité	Confidentialité
Déclaration simplifiée	< ou = 40 bits	< ou = 128 bits	> 128 bits	**LIBRE (art. 30, II)**	**DECLARATION PREALABLE** <dossier technique + code source des logiciels utilisés> **(art.30, III)**
	Déclaration	Déclaration	**Autorisation**		

NB : Moyens pouvant être exemptés de contrôle *quelle que soit la longueur de clé* sous certaines conditions (D. n°99-200 du 17 mars 1999) :

Cartes à puce personnalisées, Équipements de réception de télévision de type grand public, Moyens matériels ou logiciels spécialement conçus pour assurer la protection des logiciels contre la copie ou l'usage illicite, Moyens de cryptologie utilisés dans les transactions bancaires, Radiotéléphones portatifs ou mobiles destinés à l'usage civil, station de base de radiocommunication cellulaires civiles, …

NB : les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur fourniture peut être dispensée de toute formalité préalable, sont fixées par un décret en Conseil d'Etat.

IMPORTATION

- **Simplification et allègement du dispositif**

AVANT (valable uniquement pour les pays extérieurs à l'UE)				**APRES**	
Authentification Contrôle d'Intégrité	Confidentialité *Longueur de clé*			Authentification Contrôle d'intégrité	Confidentialité
LIBRE	< ou = 40 bits	< ou = 128 bits	> 128 bits	**LIBRE (art. 30, II)**	**DECLARATION PREALABLE** <dossier technique + code source des logiciels utilisés> **(art. 30, III)**
	LIBRE	LIBRE *	**AUTORISATION**		

***A condition**,
soit que lesdits matériels ou logiciels aient préalablement fait l'objet d'une déclaration par leur producteur, un fournisseur ou un importateur,
soit que lesdits matériels ou logiciels soient exclusivement destinés à l'usage privé d'une personne physique ;
Sinon, une déclaration d'utilisation personnelle doit être adressée à la DCSSI

NB : Moyens pouvant être exemptés de contrôle *quelle que soit la longueur de clé* sous certaines conditions (D. n°99-200 du 17 mars 1999) :

Cartes à puce personnalisées, Équipements de réception de télévision de type grand public, Moyens matériels ou logiciels spécialement conçus pour assurer la protection des logiciels contre la copie ou l'usage illicite, Moyens de cryptologie utilisés dans les transactions bancaires, Radiotéléphones portatifs ou mobiles destinés à l'usage civil, station de base de radiocommunication cellulaires civiles, …

NB : les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur importation peut être dispensée de toute formalité préalable, sont fixées par un décret en Conseil d'Etat.

Nota bene : sur l'allègement du dispositif

- Le régime de déclaration préalable : **plus qu'une simple formalité de dépôt légal**
  - **Envoi d'un dossier détaillé au moins 1 mois avant l'opération envisagée**
    - **Partie administrative**
    - **Partie technique**
      - **Contenu à l'identique de celui relevant du régime d'autorisation (arrêté du 17 mars 1999)**
        - **Pouvant représenter plusieurs semaines de travail d'un ingénieur spécialisé**
        - **Comprenant notamment : description complète des procédés de cryptographie employés et de la gestion des clés mises en œuvre par le moyen**
  - **Délai de réponse de la DCSSI : 1 mois (4 mois dans le cas du régime d'autorisation)**

EXPORTATION

	7 Destinations *	Autres destinations
AUTHENTIFICATION CONTRÔLE D'INTEGRITE	**LIBRE (art. 30, I)**	
CONFIDENTIALITE	Licence Générale Communautaire **DECLARATION** (obligation de reporting post-export)	Licence d'exportation (individuelle, globale ou générale) **AUTORISATION**

***** Australie, Canada, Japon, Nouvelle Zélande, Norvège, Suisse, USA

NB : Un décret en Conseil d'Etat (à venir) fixe les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur exportation peut être soumise

- soit au régime déclaratif et aux obligations d'information prévues (dossier technique + dépôt de sources)
- soit sont dispensés de toute formalité préalable.

- **Amendement en cours de la législation européenne (consultation à Bruxelles) : renforcement des contrôles pour les biens en transit sur le territoire de l'UE + extension de la liste des Etats bénéficiant de la licence générale communautaire**

TRANSFERT
(intra-communautaire)

- **La notion de transfert désigne le "passage de frontière" entre deux États membres de la Communauté européenne** ; il ne s'agit plus d'exportation/importation stricto sensu puisque les États membres sont dans un marché unique. La qualification d'exportation/ importation s'applique lorsqu'est concerné un État tiers à la Communauté européenne.

Authentification **Contrôle d'intégrité**	**Confidentialité**	
	(Depuis la France) **Vers un État membre de l'UE**	**Depuis un État membre de l'UE** (vers la France)
LIBRE (art. 30, II)	**AUTORISATION** **(art. 30, IV)**	**DECLARATION PREALABLE** **(art. 30, III)**

- **Rappel : le silence de la DCSSI vaut acceptation du dossier**

- **Appréciation du dispositif**
  - **L'arbitrage (attendu) des décrets en Conseil d'Etat fixant les exceptions au régime d'autorisation ou de déclaration préalable**
  - **Nouveaux assouplissements en cours de discussion à Bruxelles**

Sanctions encourues

- Sanctions administratives : interdiction de mise en circulation et retrait des marchandises

- Sanctions pénales :
  - 1 an d'emprisonnement / 15.000 € d'amende : produits soumis à déclaration
  - 2 ans d'emprisonnement / 30.000 € d'amende : produits soumis à autorisation
  - Peines complémentaires : confiscation, fermeture d'établissement, exclusion des marchés publics, …

- Circonstance d'aggravation de la peine lorsque le moyen de cryptologie a été utilisé pour préparer ou commettre un crime ou un délit ou en faciliter la préparation ou la commission (art. 132-79 C.Pénal)

3. Cryptographie en entreprise : un domaine à réglementer !

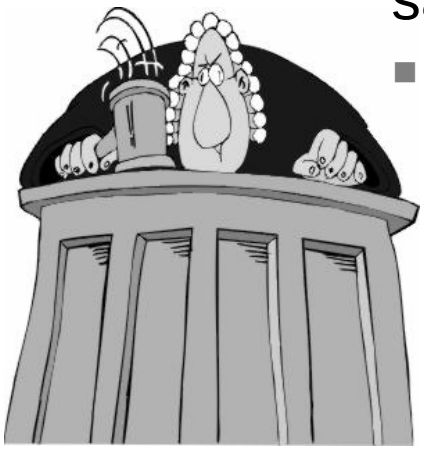
- La cryptographie au cœur d'intérêts et d'usages antagonistes :
  - Outil au service de l'entreprise : protection des « *assets business* »
  - *Barrière technique aux contrôles de l'entreprise : usage des moyens de chiffrement à des fins privées du salarié*
- Problématique des limites de la vie privée et de la surveillance sur le lieu de travail

  3.1 Etat de la jurisprudence depuis l'arrêt Nikon

  3.2 Rôle des chartes dans la garantie de libre accès aux données professionnelles

3.1 Etat de la jurisprudence depuis 2001

- La révision de l'arrêt Nikon (1)
  - Une jurisprudence à l'origine très protectrice des salariés :



    - Nikon, 2001 : un attendu de principe à l'interprétation rigide
      - Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée, celle-ci impliquant en particulier le secret des correspondances.
      - L'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur.
    - Cegelec, 2003 : plus loin que l'arrêt Nikon lui-même !
      - Ont le caractère de messages personnels les messages envoyés et reçus par un salarié sur une adresse électronique générique de l'entreprise dans le cadre de son travail, dès lors qu'ils sont consultables sur son seul poste
    - Lucent technologies, 2003 : responsabilité de l'employeur du fait des agissements personnels de ses salariés sur l'Internet

3.1 Etat de la jurisprudence depuis 2001

- La révision de l'arrêt Nikon (2)
  - Le retour à un compromis plus équitable :
    - Cathnet-Science, 2005 : conditions du contrôle en l'absence du salarié
      - Justification d'un « risque ou évènement particulier »
        - Mettant en cause la sécurité
        - Degré de gravité certain
        - Caractère d'urgence
    - Deux arrêts du 18 octobre 2006 : le PC du salarié frappé d'une présomption de caractère professionnel
      - Le pourvoi n°04-48.025 : interdiction de chiffrer, sans l'autorisation de l'employeur, l'ensemble des données du disque dur, l'utilisation de moyens de cryptographie constituant une entrave au contrôle que peut légitimement exercer l'employeur .

3.2 Rôle des chartes

- Le temps de la mise à jour
  - Règle de l' **identification positive**

pour les données privées du salarié

- règle de nommage des fichiers
- lieu de sauvegarde

  - **Garantie de libre accès** aux fichiers

présumés professionnels

- politique de classification des documents : règles d'utilisation des fonctions de sécurité et des moyens de chiffrement
- maîtrise de l'origine des moyens de chiffrement (confiance dans les outils, respect des règles de contrôle)
- transparence et collaboration avec les autorités de police et de justice (// article 37 dernier alinéa LEN)

La charte informatique du CNRS a été modifiée

Myriam Fodel et Gaëtane Manihiot, Direction des Affaires Juridiques du CNRS

La charte pour l'usage de ressources informatiques et de services Internet du CNRS, initialement élaborée en 1999, a été amendée en janvier dernier. Cette charte modifiée a été approuvée par le Comité technique paritaire réuni le 18 décembre 2006. La décision du Directeur Général du 18 janvier 2007, publiée au Bulletin officiel, en porte approbation.

Panorama des évolutions juridiques

Aperçu des modifications élaborées en conséquence

SI 59 (mai 2007)

4. Conclusion

- Confidentialité = Cryptographie + (?)
  - Sensibilisation des utilisateurs aux règles élémentaires de la SSI
    - Cas des utilisateurs nomades
    - Politique de classification et règles d'accès aux documents

Contact

Marie BAREL, juriste

Expertise TIC/SSI

marie.barel@legalis.net