

# La responsabilité juridique des RSSI

# La responsabilité juridique des RSSI



## Responsable de la sécurité informatique: le détective de l'info

Le responsable de la sécurité de l'information est un des employés les plus importants d'une entreprise. Les tâches qui lui incombent sont grandes: il doit à la fois garantir la sécurité vis-à-vis des menaces extérieures, mais également lutter contre un danger beaucoup plus sournois: le manque de vigilance de certains utilisateurs. Explications. *Par David Naudin*

**Informatique ou information?**

Précisons sémantiquement: la sécurité informatique est une des composantes d'un domaine beaucoup plus large, celui de la sécurité de l'information. C'est très bien de protéger des fichiers sur un ordinateur, d'installer des antivirus, de mettre des pare-feu, mais si l'information se trouve également sur une feuille de papier posée négligemment sur un bureau, à la portée de l'importe qui, l'efficacité de votre travail est diminuée. *Exploite*



Normes ISO/IEC 27003:2010



## Introduction

**RSSI : quelles responsabilités civiles et pénales ?**

## RSSI et traitement des données à caractère personnel



- **Article 34 de la loi du 6 janvier 1978**  
**“Informatique & Libertés”**

**“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 226-17 du Code pénal**

**“Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l’article 34 de la loi n°78-17 du 6 janvier 1978 (...) est puni de cinq ans d’emprisonnement et de 300.000 euros d’amende”**

## La responsabilité juridique des RSSI

The screenshot shows the CNIL website interface. At the top, there are logos for CNIL, ESPEACE, and contact information: 'allo CNIL tél : 01 53 73 22 22' and 'lettre info CNIL je m'inscris'. A red banner reads 'L'informatique doit respecter l'identité humaine, les droits de l'homme'. The breadcrumb trail is 'Accueil > Dossiers > Internet-télécoms > Fiches pratiques > 10 conseils pour la sécurité de votre système d'information'. The main content area is titled 'Fiches pratiques' and features a red header for '10 conseils pour la sécurité de votre système d'information' dated '12 octobre 2009'. The text explains that the 'informatics and liberties' law requires data security measures. Two red boxes highlight the first two points: '1. Adopter une politique de mot de passe rigoureuse' and '2. Concevoir une procédure de création et de suppression des comptes utilisateurs'. A sidebar on the left lists various categories like 'Banque-Crédit', 'Collectivités locales', and 'Internet-télécoms'.

Source : [www.cnil.fr](http://www.cnil.fr)



1. Adopter une politique de mot de passe rigoureuse
2. Concevoir une procédure de création et de suppression des comptes utilisateurs
3. Sécuriser les postes de travail
4. Identifier précisément qui peut avoir accès aux fichiers
5. Veiller à la confidentialité des données vis-vis-vis des prestataires
6. Sécuriser le réseau local
7. Sécuriser l'accès physique aux locaux
8. Anticiper le risque de perte ou de divulgation des données
9. Anticiper et formaliser une politique de sécurité du système d'information
10. Sensibiliser les utilisateurs aux "risques informatiques" et la loi "informatique et libertés"

## La responsabilité juridique des RSSI

### LA CNIL EN CHIFFRES

#### 719 délibérations

En 2009, la CNIL a siégé 48 fois au cours de 35 séances plénières, 13 formations contentieuses. Ces réunions ont conduit à l'adoption de 719 délibérations.

Les délibérations de la CNIL sont disponibles sur le site Légifrance : [www.legifrance.gouv.fr](http://www.legifrance.gouv.fr)

La liste des délibérations adoptées en 2009 est disponible sur le site de la CNIL : [www.cnil.fr/deliberations/2009/](http://www.cnil.fr/deliberations/2009/)

#### 4 265 plaintes

#### 2 217 demandes d'accès aux fichiers de police et de gendarmerie

#### 68 185 déclarations de fichiers

En 2009, la CNIL a enregistré 68 185 nouveaux traitements de données personnelles.

Depuis 1978, ce sont au total 1 356 579 fichiers qui ont été déclarés à la CNIL.

#### 1 500 correspondants « Informatique et Libertés » représentant 6 000 organismes

#### Au titre du conseil et de l'expertise

7 avis sur projet de loi ou de décret  
1 recommandation

#### Au titre des contrôles et des sanctions

270 contrôles  
91 mises en demeure  
5 sanctions financières  
4 avertissements

#### Au titre de la simplification

7 autorisations uniques  
2 dispenses de déclaration  
1 avis sur un acte réglementaire unique

#### Au titre des formalités déclaratives

544 autorisations  
5 refus d'autorisation  
35 avis sur des traitements sensibles ou à risques  
900 autorisations relatives à des systèmes biométriques (700 en 2008)  
3054 déclarations relatives à des systèmes de vidéosurveillance (2 588 en 2008)

### LISTE DES SANCTIONS PRONONCÉES EN 2009

Date	Nom ou type d'organisme	Décision adoptée	Thème
Janvier 2009	KÉCULS RENNES	Avertissement	-Billetique - Restriction à la souscription du passe anonyme
Février 2009	DIRECTANNONCES	Sanction pécuniaire de 40 000 €	- Collecte déloyale d'annonces immobilières de particuliers
Mars 2009	Organisme public *	Avertissement	- Vote électronique (défaut de confidentialité et de sécurité des données)
Mars 2009	Organisme public *	Avertissement	- Vote électronique (défaut de confidentialité et de sécurité des données)
Avril 2009	Société JEAN-MARC-PHILIPPE	Sanction pécuniaire de 10 000 €	- Vidéosurveillance constante des salariés
Avril 2009	Groupement d'huissiers *	Non lieu à statuer (mise en conformité de l'organisme)	- Faille de sécurité
Mai 2009	OPTICAL CENTER	Sanction pécuniaire de 5 000 €	- Absence de prise en compte du droit d'opposition à recevoir de la prospection commerciale
Juillet 2009	Groupement d'huissiers *	Avertissement	- Faille de sécurité
Juillet 2009	SCP Huissiers	Sanction pécuniaire de 10 000 €	- Enregistrement de commentaires excessifs sur les débiteurs (santé, infractions...)
09/07/09	SCP Huissiers	Sanction pécuniaire de 10 000 €	- Enregistrement de commentaires excessifs sur les débiteurs (santé, infractions...)

\* Sanctions non rendues publiques.

Source : CNIL 30<sup>ème</sup> rapport d'activité 2009

## RSSI et Cybersurveillance des salariés



**RSSI et fraude(s) informatique(s) sur les traitements automatisés de données**

## Mais encore ?

**Contrefaçon de droits de propriété intellectuelle ou industrielle, Cryptologie, Correspondant Informatique & Libertés (« CIL »), Alertes éthiques professionnelles (ou whistleblowing), LCEN (article L 323-3-1 du code pénal), conservation des données de connexion internet (loi janvier 2006 « anti-terroriste »), etc.**

La responsabilité juridique des RSSI

**Nous vous remercions pour votre attention**

---

**François Herpe**  
Avocat  
[pherpe@cvs-avocats.com](mailto:pherpe@cvs-avocats.com)

