
# CONFORMITÉ LÉGALE DES SI

## Les risques sécuritaires et éthiques des Systèmes d'Information

Patrick KINEIDER
Dominique BERGEROT
Martine OTTER
Thêt SOK

Adeli
www.adeli.org

# Conformité légale des SI

## Enquête 2010 sur la connaissance et l'appropriation des questions juridiques et éthiques liées à l'informatique

***Cet ouvrage est une publication d'ADELI, diffusée auprès de ses adhérents.***

***ADELI***
***87, rue Bobillot***
***75013 Paris – France***
***www.adeli.org***
***Téléphone : 01 45 89 02 01***
***Adresse électronique : info@adeli.org***

Dépôt légal 2011
ISBN 2-9517899-3-9


**Couverture :**
Marie Bonvin

**Impression :**
Prestaprint – 20, avenue Édouard Herriot
92350 Le Plessis Robinson – France

10-31-1086

# Conformité légale des SI

**Sous la direction de Patrick Kineider,**
**avec le concours de**
**Dominique Bergerot,**
**Martine Otter,**
**Thet Sok**

# Ouvrages de référence publiés par ADELI depuis 1978

**Guide des certifications SI**

Guide des certifications SI – Comparatif, analyse et tendances – ITIL, Cobit, ISO 27001, eSCM…
Martine Otter, Jacqueline Sidi, Laurent Hanaud
Éditions Dunod © 2006, 2009 – ISBN 978-2-10-052941-4

Le Guide des Certifications SI est paru aux éditions DUNOD en septembre 2006 après la publication de l'ODOSCOPE en 2004. La 2è édition a été publiée chez DUNOD en 2009.
Ce panorama des certifications applicables aux systèmes d'information fournit une vision synthétique de 29 dispositifs utilisés en France.
Les référentiels analysés couvrent l'ensemble des domaines soumis à certification : entreprises, services, produits, processus et personnes. Il présente entre autres : ITIL, CobiT, ISO 9001, CMMI, eSCM-SP, PRINCE2, HAS, ITSEC, Six Sigma, ISO 27001, PMP. L'ouvrage présente des cartographies, des analyses et des tendances afin d'aider les auditeurs motivés par la bonne gouvernance du SI à s'y retrouver aisément ou à construire leur propre système.

**NORMAscope**

Mettre en œuvre l'ISO 9001:2000 et ses processus
Jacqueline Sidi
ADELI © 2001 – ISBN 2-9717899-0-4

Cet ouvrage dresse un tableau des normes de la famille ISO 9000 et de celles liées à l'ingénierie du logiciel et des systèmes.
Il s'efforce de répondre à un ensemble de questions pratiques :
À quoi servent les normes et comment s'en servir ?
Quelles normes pour quelles exigences de l'ISO 9001 ?
Quelles normes pour quels processus ?

**MÉTROscope**

Indicateurs et tableau de bord pour le développement de logiciels
Collectif, sous la direction de Gina Gullà-Ménez
ADELI © 2001

État de la normalisation et recueil d'expériences sur les pratiques en matière d'élaboration d'indicateurs et tableaux de bord dans le domaine du développement de logiciel. L'ouvrage est accompagné d'un glossaire.

**VAL€URoscope**

Analyse de la valeur appliquée aux projets Euro et An 2000
Gina Gullà-Ménez
ADELI ©1999

Le VAL€URoscope 2000 montre comment utiliser l'Analyse de la Valeur pour optimiser les opérations d'adaptation des logiciels à l'an 2000 et à l'Euro, sous la double contrainte de délai et de limitation des ressources.
Alors que le cap de l'an 2000 a été franchi par la plupart des entreprises sans trop de dommages, on peut se demander s'il ne l'a pas été à un coût trop élevé.
Cet ouvrage reste donc un support pertinent pour l'application d'une démarche d'Analyse de la Valeur au domaine des Systèmes d'information.

**AGLoscope**

Étude des ateliers de conception
Collectif, sous la direction de Geneviève Coullault
ADELI ©1998, ©1997, ©1996, ©1995

Panorama des outils d'aide à la conception des systèmes d'information de gestion, distribués en France.
Chaque année, l'AGLoscope contient des tableaux de synthèse, des descriptifs de nombreux produits et de témoignages d'utilisateurs.

**RÉALiscope**

Étude des environnements de développement
Collectif, sous la direction d'Yves Constantinidis
ADELI ©1998

Le RÉALiscope est le complément de l'AGLoscope, appliqué aux outils de réalisation : tableaux de synthèse, descriptifs de produits, etc.

**PÉRILoscope**

Maîtriser les risques des projets informatiques
Collectif, sous la direction de Jean-Marc Bost, en collaboration avec l'IQSL
ADELI ©1997

La maîtrise des risques n'élimine pas les effets du hasard mais les circonscrit grâce à des méthodes, tant statistiques que prédictives.
Écrit par une équipe de praticiens ayant l'expérience opérationnelle de la conduite de projet, cet ouvrage propose une démarche rigoureuse pour identifier, maîtriser et manager les risques.
Il contient un recueil complet des techniques et des outils de management des risques. Une bibliographie très fournie figure en fin d'ouvrage.

**ISO 9001 et développement de logiciel**

Collectif, sous la direction de Martine Otter en collaboration avec SYNTEC Informatique
Édition AFNOR ©1996 - ISBN 2-12-465012-2

Fruit de la confrontation de l'expérience d'entreprises déjà certifiées ou en passe de l'être, d'auditeurs et de responsables qualité dans le secteur de l'informatique, ce guide vise à transposer les concepts de la norme ISO 9001 aux activités de développement du logiciel.
Dans ce but, chaque chapitre de l'ouvrage explique et commente un chapitre de la norme ISO 9001.
Pour offrir une vision large du management de la qualité, une comparaison est également faite avec la norme ISO 9000-3 et le fameux guide anglais TickIT, utilisé par les auditeurs systèmes qualité.
Enfin, des exemples de procédures et des témoignages sur la démarche de certification viennent compléter l'ouvrage.

**MÉTHODOscope**

Étude des méthodes de conception
Collectif, sous la direction de Paul Théron
ADELI © 1985

Dès 1985, ADELI s'est signalée par la publication du Méthodoscope.
Il s'agissait d'une étude comparative des méthodes de conception de systèmes d'information de gestion.
Au-delà du positionnement relatif de LCS, MERISE et AXIAL, c'est l'établissement des critères de comparaison des méthodes autour d'un cycle de vie qui a constitué l'apport essentiel de cet ouvrage.

# Remerciements

Les membres du Groupe de Travail « Juridique et Internet du Futur » tiennent à remercier :

- les adhérents qui, malgré les nombreuses sollicitations auxquelles ils sont soumis, ont pris le temps de répondre à l'enquête à l'origine de ce document ;
- les membres du Comité d'ADELI, pour leur écoute, leur suivi régulier et leur appui.

***Patrick Kineider***
***et les membres du Groupe de Travail***
***« Juridique et Internet du futur »***

# Table des matières

# 1. Introduction

ADELI a créé, en 2009, le Groupe de Travail, dénommé « Juridique et Internet du Futur », ayant pour objectif, par l'observation et l'analyse d'événements techniques et sociétaux extérieurs, d'évaluer les risques d'atteinte aux données informatiques (professionnelles mais aussi personnelles), les socles et protections juridiques existants, leur connaissance et leur applicabilité.

Le forum « Juridique et Internet du Futur » et les blogs personnels ouverts sur le site Web d'ADELI conservent les traces des veilles technologiques et de nombreux échanges d'informations et de commentaires.

En juin 2010, le Comité a décidé de réaliser une enquête en ligne auprès d'entreprises et d'adhérents de l'Association, sur la connaissance et l'application sur le terrain de ce thème.

Le présent document traite de la conformité réglementaire et légale. Il décrit :

- le contexte juridique actuel (§ 2) ;
- la structure résumée des réponses aux divers domaines de l'enquête (§ 3) ;
- en Annexe, les réponses détaillées avec leurs commentaires éventuels, et de nombreuses références adéliennes (§ 4).

# 2. Contexte juridique

## 2.1. Préambule

Il y a une quinzaine d'années, le droit français sanctionnait la malveillance et l'ingérence dans les SI (attaques sur les systèmes, atteintes à la propriété intellectuelle des logiciels...).

Un tiers des questions de l'enquête concerne l'aspect juridique actuel de l'informatique, qui s'est notoirement élargi au-delà des domaines précédents, en raison de l'explosion d'Internet et des pratiques relationnelles associées ; cependant la loi Informatique et Libertés, dite « LIL » y occupe toujours une place privilégiée.

Actuellement coexistent deux types de lois :

- des lois de « protection des libertés » (en anglais : « privacy » ou confidentialité) telles que la Loi Informatique et Libertés ;
- des lois « sécuritaires » telles que l'HADOPI, la LCEN, la LOPPSI.
  Dans ce deuxième domaine, il arrive que des risques identiques soient couverts par plusieurs textes (par exemple, la LIL et la LOPPSI2).

Les paragraphes 2.2. à 2.4. récapitulent les éléments essentiels des lois constituant le socle juridique informatique actuel le plus important, que ce soit pour les utilisateurs privés ou ceux des systèmes informatiques d'entreprises.

## 2.2. Loi « Informatique et Libertés »

La LIL (Loi Informatique et Libertés), promulguée il y a plus de 30 ans, le 6 Janvier 1978, est censée protéger les « données nominatives », plus récemment appelées « données à caractère personnel », des accès et d'utilisations non spécifiquement autorisées par une déclaration (ces accès interdits sont le plus souvent de type commercial ou administratif).

Dès le départ, la « Commission Informatique et Libertés » (CNIL), indépendante, n'était manifestement pas dotée des moyens suffisants à l'exercice de ses missions ; après 2005, la montée en puissance d'Internet, et plus récemment des réseaux sociaux, est encore venue compliquer l'organisation de ses interventions.

La LIL est d'une grande utilité dans les domaines suivants :

- vie privée ;
- RH (ressources humaines), comptabilité, gestion dans l'entreprise ;
- police, justice ; santé.

Elle reste néanmoins réservée aux données de fichiers exploités en France. Il existe des organismes similaires à la CNIL dans d'autres pays européens (une trentaine), néanmoins, dans de nombreux litiges relatifs aux données sur Internet, c'est l'esprit du droit anglo-saxon, différent du droit français, qui continue à s'appliquer.

Une révision de la LIL en 2004 (« LIL2 »), a, entre autres, précisé les devoirs du responsable de traitement (dans la pratique, de l'employeur pour les fichiers de l'entreprise), en termes d'information des personnes figurant aux fichiers nominatifs. De plus, en 2003, une nouvelle fonction a été créée, afin de mieux assurer le respect de ces droits fondamentaux : le « Correspondant Informatique et Libertés » (CIL).

Malgré l'insuffisance des moyens de mise en œuvre (activité multipliée par 7, avec des moyens seulement doublés en 25 ans), cette nouvelle obligation légale constitue néanmoins, une reconnaissance d'un dispositif qui a déjà permis la diffusion de la culture informatique et libertés au sein de nombreux organismes publics et privés. Exemple de question : la « publicité ciblée » (voir § 4.3.2.4).

Le correspondant informatique et libertés (CIL) contrôle l'application de la loi dans l'entreprise. Il veille au respect des obligations pour les traitements concernés ; il est consulté avant la mise en œuvre des nouveaux traitements. Il tient un registre de ces traitements, un bilan annuel, une liste des failles de sécurité. Il est responsable vis-à-vis du responsable du service informatique et aussi de la CNIL ; il a une obligation de conseil et de contrôle de conformité (voir aussi : « les nouveaux statuts du CIL », § 4.3.2.1.)

Depuis fin 2010, la Commission européenne a engagé la révision de la directive européenne 95/46/CE pour la protection des données personnelles. Cette directive a été transposée en France en 2004 sous forme de révision de la Loi Informatique et Libertés.

Depuis, sont apparus les réseaux sociaux, de nouvelles technologies telles les puces RFID, la géolocalisation, le Cloud computing, les réseaux sans fil, la vidéo-surveillance et le profiling marketing. Les travaux européens prévoient dans les entreprises la création d'une fonction de Data Protection Officer (très proche du Correspondant Informatique et Libertés créé en France en 2003). Il est même envisagé de rendre obligatoire cette fonction dans l'entreprise.

De nouvelles règles participent au renforcement du droit des personnes et de la protection de leurs données personnelles :

- clarification et renforcement du concept du « consentement des personnes » ;
- renforcement du principe de data minimization (s'en tenir strictement aux seules données pertinentes et indispensables) ;
- formalisation d'un « droit à l'oubli » (purge des données à l'issue de la durée de conservation) ;
- définition standardisée des « données personnelles sensibles ».

D'autres mesures projetées visent une responsabilisation accrue des responsables de traitements :

- introduction du concept d'Accountability (« obligation de rendre des comptes ») ;
- instauration d'une notification des violations aux traitements de données personnelles.

De plus, l'applicabilité du texte doit être clarifiée quand les données personnelles sont hébergées dans un dispositif de type « Cloud computing », de même que la mise en place d'un processus de certification.

La publication de la révision de la directive européenne impliquera une évolution de la loi française Informatique et Libertés (LIL).

## 2.3. L'HADOPI et l'HADOPI2

La directive européenne 2001/29/CE a été transposée en France par la loi DADVSI, qui vise à protéger « les droits d'auteur et les droits voisins de la société de l'information ».

Cette loi a été promulguée le 3 août 2006. Elle est complétée par la loi HADOPI (encore appelée « Loi Création et Internet » ou « Loi n°2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet », qui comporte des sanctions en cas d'infractions.

Cette loi identifie et réprime le téléchargement illégal sur Internet et le partage des fichiers concernant des œuvres en infraction avec les droits d'auteur.

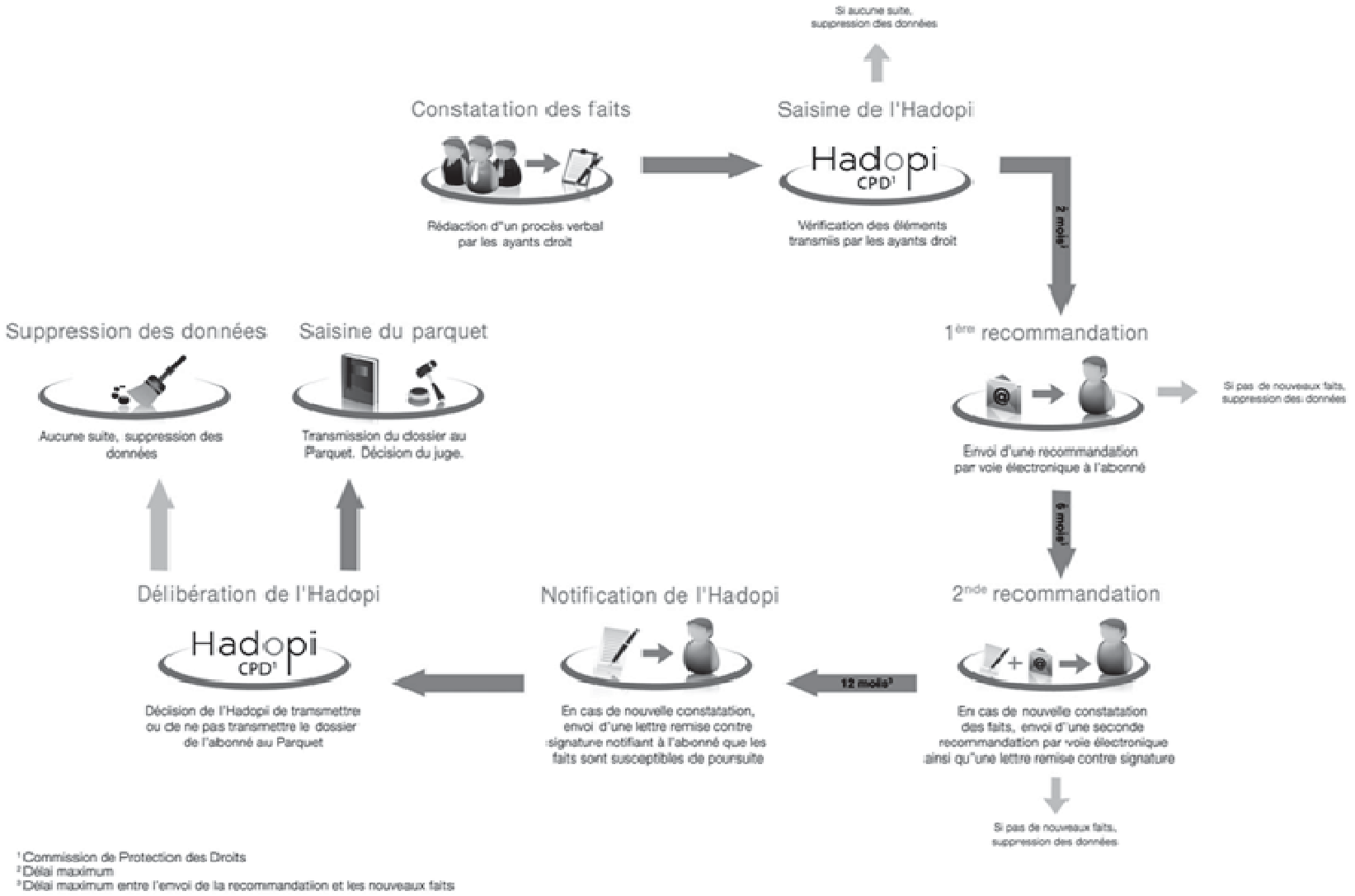
Elle installe une « Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet », organisme de régulation indépendant. Institué par le décret d'application du 31 décembre 2009, cet organisme est composé d'un collège et d'une commission de protection des droits, qui exercent depuis le 8 janvier 2010.

La loi du 12 juin 2009, outre qu'elle a fait l'objet de nombreuses critiques quant à son efficacité potentielle dans la société civile, a été promulguée après passage devant de nombreuses instances de l'État (CNIL, Sénat, Assemblée nationale, une commission mixte paritaire, second passage devant l'Assemblée nationale), et après la censure de certaines mesures par le Conseil Constitutionnel.

La loi Création et Internet :

- institue une autorité publique indépendante, la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI) ;
- instaure une censure administrative, réprimant spécifiquement le défaut de surveillance de l'accès à l'Internet contre l'utilisation de celui-ci par un tiers pour la copie et la diffusion d'une œuvre auprès du public sans l'accord de ses ayants droit ;
- met en œuvre ces sanctions selon la méthode de la « riposte graduée » (cf. figure 1 ci-après) : un courriel d'avertissement en guise de premier rappel à la loi, puis un courrier d'avertissement par lettre recommandée, et la coupure de la connexion Internet en dernier ressort.
  Au 4e trimestre, l'Autorité a envoyé plus de 100 000 courriels d'avertissement ; fin 2010 début 2011, l'étape des courriers recommandés, est franchie.
- fait de cette autorité un intermédiaire entre l'ayant-droit chargé de fournir les adresses IP des équipements informatiques suspectés de téléchargement illégal et le fournisseur d'accès à Internet, chargé d'identifier les abonnés et de procéder in fine à la coupure de leur accès à l'Internet.
  À noter qu'une censure du Conseil constitutionnel a interdit cette coupure, si elle n'est pas prononcée par un tribunal judiciaire après débat contradictoire ; il en est résulté une nouvelle version de l'HADOPI, l'« HADOPI2 ».

Figure 1- « riposte graduée »




*(© hadopi2.fer, avec autorisation de diffusion associative)*

## 2.4. Les autres lois sécuritaires

### 2.4.1. La loi « Confiance dans l'Économie Numérique »

La LCEN « Loi sur la Confiance dans l'Économie Numérique » du 21 juin 2004, fait suite aux directives européennes de 2000 et 2002 sur le commerce électronique et la protection des données privées.

Elle a pour fonction de limiter la responsabilité morale des hébergeurs en cas de gestion de données illicites, et interdit la prospection électronique auprès de particuliers sans avoir obtenu au préalable, leur consentement : c'est le classique « opt-in » (« autoriser la réception »), dont l'absence fréquente génère des « spams » commerciaux.

Un décret de 2007, revu afin de parfaire son applicabilité en février 2011, oblige les hébergeurs à conserver pendant un an, à compter de chaque activité d'un utilisateur, l'identifiant de la connexion à l'origine de la communication, les nom, prénom, adresse postale, adresse électronique, numéro de téléphone et le mot de passe utilisés par les utilisateurs de leurs services.

La Police, la Gendarmerie, la répression des fraudes, la Douane, le fisc, l'URSSAF pourront avoir accès à ces données dans le cadre d'enquêtes ; mais cette dernière édition a elle-même entraîné, pour des motifs d'atteinte à la confidentialité et de défaut de moyens, plusieurs recours devant le Conseil d'État.

### 2.4.2. La « LOPPSI »et la « LOPPSI2 »

La Loi d'Orientation et de Programmation sur la Performance de la Sécurité Intérieure, dans sa version de 2011, prévoit un ensemble de mesures dans tous les domaines afin de faciliter le travail policier et judiciaire pour la période 2009-2013 :

- caractérisation de l'usurpation d'identité sur Internet comme un délit ;
- blocage de sites Web à contenu pédopornographique ;
- liste noire non publique de certains sites, avec obligation de filtrage de l'adresse IP dans les connexions Internet privées.

Elle recoupe la LCEN et, d'une certaine manière, l'HADOPI2, en instaurant, de plus, un accès quasi illimité au titre de l'ordre public, des autorités dans les systèmes informatiques en vue de la prévention et/ou des enquêtes sur les crimes et délits informatiques.

## 2.4.3. Tableau chronologique des lois (1978-2011) et des risques couverts

Le tableau suivant montre l'évolution de l'ensemble des lois de 1978 à 2011. En début de période, la LIL suffisait au contexte informatique ; avec l'accroissement des échanges par le web, la LCEN et la LOPPSI ont complété le socle « préventif et répressif ».

Enfin, plus particulièrement axées sur les œuvres informatiques (musique, films), la DADVSI et surtout l'HADOPI ont un impact économique et culturel considérable. Certains risques couverts sont communs à plusieurs textes, par exemple, l'usurpation d'identité.

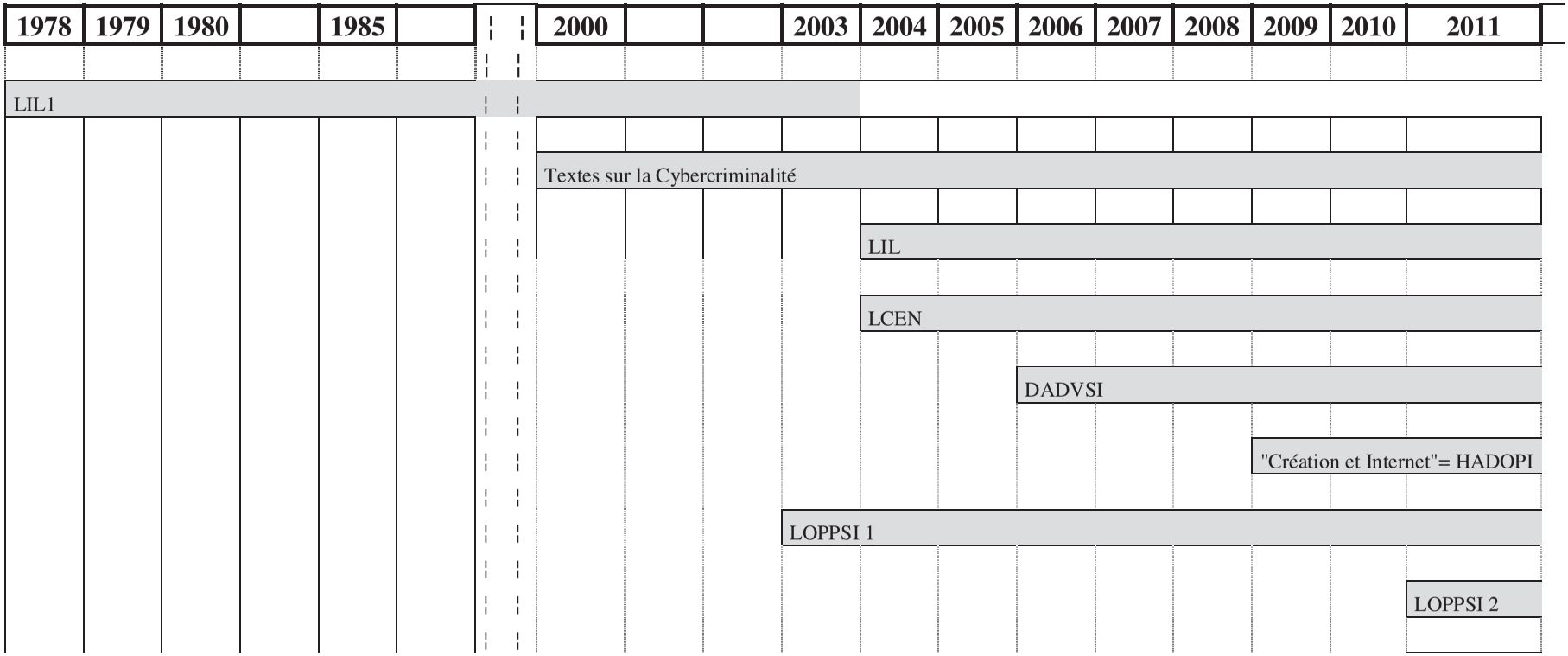
| Loi ou texte (forme abrégée) | Année promulgation | Type | Objet | Risque(s) couvert(s) | Population protégée |
|---|---|---|---|---|---|
| LIL1 | 1978 | Loi | • Protection des données personnelles | • Usurpation d'identité<br>• Utilisations non autorisées des fichiers<br>• Perte de confidentialité | Personnes physiques |
| Cybercriminalité | Après 2000 | Convention européenne +parties de lois françaises | • Prévention et répression des infractions pénales dans les SI | • ingérences ; attaques (virus, spams, phishing;..)<br>• utilisations contraires à l'ordre public, pédopornographie, terrorisme | Utilisateurs |
| LOPPSI1 | 2002 | Loi | • Texte d'orientation de LOPPSI2 (sécurité générale, sécurité routière, protection des données, accès administratifs aux fichiers) | • Utilisation des fichiers dans des recherches policières ou judiciaires | Personnes physiques |
| LIL2 | 2004 | Loi | • Protection des données personnelles avec information et attribution de droits à la personne concernée par ses propres données, rôle du CIL | • Usurpation d'identité<br>• Utilisations non autorisées des fichiers<br>• Perte de confidentialité | Personnes physiques |

| Loi ou texte (forme abrégée) | Année promulgation | Type | Objet | Risque(s) couvert(s) | Population protégée |
|---|---|---|---|---|---|
| LCEN | 2004 | Loi | • Hébergement de données<br>• Commerce électronique | • Responsabilité hébergeur<br>• Avis utilisateur obligatoire (commerce par messageries) =>prévention du spam | Hébergeur Utilisateurs |
| DADVSI | 2006 | Loi | • Protection des logiciels et œuvres numérisées | • Piratage au sens de la propriété intellectuelle | Ayants droits auteurs |
| HADOPI1- | 2008 | Loi | • Téléchargement illégal | • Atteinte au droit d'auteur : théorie | Ayants droits auteurs |
| HADOPI2 | 2009 | Loi | • Téléchargement illégal (procédure) | • Atteinte au droit d'auteur : procédure définitive | Ayants droits auteurs |
| LOPPSI2 | 2011 | Loi | • Sécurité générale, sécurité routière<br>• protection des données, accès administratifs aux fichiers | • Trafic de permis de conduire<br>• Vidéo-surveillance<br>• Lutte sites illégaux<br>• Accès si besoin police et justice à tous types de fichiers | Personnes physiques |

## 2.4.4. Tableau général des lois (1978-2011)

Ce tableau présente l'enchaînement chronologique des lois, en dehors des risques couverts.

Dans une première période, de 1978 à 2000, seule la LIL1 existait ; en 2000, ont été votés de très nombreux textes juridiques afin de couvrir les risques liés à l'utilisation d'Internet. On distingue une première vague sécuritaire en 2000 avec des textes sur la cybercriminalité et en 2003 la LOPPSI ; puis une seconde vague qui concerne les entreprises avec en 2004 la LIL2 et la LCEN pour favoriser le développement du e-commerce ; enfin, une troisième vague apparaît pour protéger le droit d'auteur et sanctionner le téléchargement illégal de fichiers musicaux ou vidéo, avec la DADVSI en 2006, l'HADOPI 1 et l'HADOPI 2, plus complètes, de 2009 à 2011.



# 3. L’enquête

## 3.1. Population visée

La population initiale visée consistait en un « panel » d'entreprises de l'industrie et des services liés à l'informatique et aux télécommunications.

Seuls, les adhérents d'ADELI ont été destinataires du questionnaire ; en effet, le Groupe avait envisagé la possibilité de contacter des entreprises de la profession informatique et télécommunications, mais peu d'adresses électroniques étaient disponibles ou pertinentes pour répondre, donc cette option a été abandonnée.

Nous avons utilisé l'outil « LimeSurvey », logiciel Open Source permettant de créer et de gérer des questionnaires en ligne de manière simple et efficace.

L'enquête comprenait 40 questions réparties en 3 domaines principaux (cf. §§ 3.3.1 à 3.3.3) :

- juridique et législatif (CNIL, LIL, CIL, LCEN..) ;
- qualité et sécurité des systèmes d'information ;
- entreprise et nouveaux outils ;

ainsi qu'un 4$^{e}$ domaine « fonction actuelle et position par rapport à ADELI ».

Les fonctions des personnes ayant répondu se répartissent comme suit :

- consultants (y compris juridiques) : 60% environ,
- autres fonctions (management, projet) : 40%

Ces adhérents s'intéressent, au sein d'ADELI, pour environ moitié d'entre eux : à la qualité, à la sécurité des SI, au management, aux aspects juridiques. Certains ont participé à des Groupes de Travail, par exemple : HCSI, LEAN 6 SIGMA, Positionnement et Notoriété, Juridique et Internet du Futur.

## 3.2. Déroulement de l'enquête

L'ensemble des questions posées et des réponses apportées figure dans un tableau, au chapitre 4.2 de ce document.

Début juillet 2010, l'envoi du questionnaire à une centaine d'adhérents, donnait lieu à 11 réponses en retour ; en novembre, on dénombrait au total 61 réponses. C'est à partir de ces dernières que ce document a été rédigé.

## 3.3. Analyse des réponses

### 3.3.1. Socle législatif et juridique

Les aspects législatifs et juridiques, ne sont sérieusement pris en compte par les correspondants interrogés, que dans environ 15% des réponses.

Lorsqu'ils le sont, leur connaissance repose sur un « spécialiste » : directeur juridique, juriste, avocat spécialisé. En particulier, les règles générales des contrats échappent aux préoccupations des opérationnels, dans la moitié des cas ; on lit dans certaines réponses : « ce n'est pas mon métier » ou « le service informatique fait appel au département des achats ». Bien que non explicite, on perçoit dans diverses réponses, une hésitation à transmettre des données spécifiques à l'entreprise, avec d'éventuelles fâcheuses conséquences relationnelles.

À noter que les peines judiciaires découlant d'intrusions dans les systèmes informatiques ne sont jamais évoquées (alors que l'existence de malveillances est évoquée dans le domaine sécuritaire, cf. § 3.3.2).

La moitié des entreprises disent s'intéresser à une « durée de conservation des données ». Rappelons, à cet égard, que plus de la moitié des sociétés ont nommé un CIL. Dans les hôpitaux publics, outre la nomination de CIL dans 40% des cas, des chartes de sécurité informatique ont été adoptées, essentiellement en raison de la confidentialité des dossiers médicaux.

Concernant la présence des CIL (fonction décrite au § 2.2), les réponses restent assez ambiguës, car, malgré son caractère obligatoire, la moitié des entreprises n'ont pas de CIL; pour les autres, il est en général, interne à l'entreprise.

Trois sociétés disent avoir effectué plus de 20 déclarations à la CNIL dans les 2 dernières années (dont une plus de 100).

### 3.3.2. Qualité et sécurité des systèmes d'information

#### 3.3.2.1. Qualité

Même si le terme « sécurité » n'est jamais employé dans le texte de la norme ISO 9001, la sécurité fait partie des exigences auxquelles un système qualité doit se conformer. Il nous paraissait donc essentiel de savoir sur quel terrain qualité la démarche sécurité venait se développer. Il est effectivement peu probable que des bonnes pratiques sécuritaires s'installent sur un terrain vierge de toute préoccupation de conformité.

Le résultat est assez surprenant et nous remercions nos adhérents de leur franchise : sur l'ensemble des réponses fournies, la moitié seulement indique qu'une démarche qualité serait appliquée dans leur entité. Ceci s'explique en partie par la proportion de consultants indépendants dans notre échantillon : ceux-ci indiquent qu'ils n'ont pas eux-mêmes de démarche qualité fondée sur un référentiel particulier mais appliquent celles de leur client.

Les référentiels cités sont divers. Certains, tels ISO 9001, EFQM ou 6 Sigma correspondent bien à la mise en œuvre d'une démarche qualité. D'autres, comme ISO 20000, ITIL, CMMI, SOX ou ISO 14000 sont plus ciblés sur des domaines particuliers. Nous pouvons noter qu'il y a une assimilation entre démarche qualité et mise en œuvre de bonnes pratiques, quel qu'en soit le domaine. « ADELI » est même cité au titre des référentiels qualité, ce qui est un hommage indéniable à notre association.

Les référentiels sont quelquefois utilisés comme cadre général, sans viser la certification, ce qui est le cas pour ISO 9001 dans deux réponses. En résumé, nos adhérents semblent appliquer les démarches qualité avec circonspection et esprit critique.

#### 3.3.2.2. Sécurité

Souvent lié à la Qualité, l'aspect Sécurité des systèmes d'information, antérieur à la prise en compte de l'aspect juridique, ne cesse de prendre de l'importance dans les entreprises et les administrations, avec le développement d'Internet, des Intranets et plus récemment, des systèmes « réseaux sociaux », « Cloud computing » et « mobilité ».

La Sécurité consiste à identifier les risques et les menaces sur la sécurité physique et logique, et à mettre en œuvre les parades (y compris humaines) associées. La Sécurité revêt diverses formes, la démarche étant le plus souvent rattachée, soit aux métiers de l'informatique et des télécommunications, soit au management en général.

40% seulement des réponses font état de l'existence d'un RSSI « Responsable Sécurité du Système d'Information », chargé de l'organisation générale de la sécurité. Dans la plupart des cas, elle relève, soit de la Direction générale, soit des DSI, soit de l'équipe « réseau ».

Les normes (ISO27001) et les méthodes d'audit ou d'analyse (Mehari, Marion..) sont assez exceptionnellement mises en œuvre. Les « chartes sécurité des systèmes d'information », autre outil très classique, ne sont mentionnées que dans 40% des réponses, et dans l'affirmative, les domaines couverts sont assez méconnus (à noter que la sécurité d'accès aux locaux – risques d'intrusion - est néanmoins citée dans les objectifs des chartes).

Les séances de sensibilisation à la sécurité du système d'information, concernent à la fois les métiers de l'informatique et les managers, mais paradoxalement, pas les personnels des sociétés extérieures (qui sont nombreux dans la profession).Enfin, des malveillances informatiques sont citées dans 20% des réponses.

Au final, la prise en compte semble un peu meilleure que celle des aspects législatif et juridique développés au chapitre 2 (historiquement, le thème de la sécurité est apparu plus tôt dans les domaines technique et économique).

### 3.3.3. Position de l'entreprise par rapport aux nouveaux outils

Les réponses font état d'une faible utilisation (ou intention d'utilisation) de ces outils :

- 50% pour les « logiciels libres » (logiciels dont l'utilisation et la modification, peuvent s'effectuer dans le cadre de licences générales sans droits) ;
- 20% pour les « réseaux sociaux ». Ce nouvel outil, avec sa structure et ses risques propres d'atteinte aux données personnelles, est analysé dans divers articles des Lettres d'ADELI (article détaillé au § 4.3.2.3) ;
- et 20% pour les systèmes de « Cloud computing » (article détaillé au § 4.3.2.2).

### 3.3.4. Analyse de certains commentaires

- À la question « Q1-1 « qui assure la veille juridique dans votre entreprise ? » la plupart des consultants indépendants, précisent qu'une autre fonction que celles citées (Directeur, Directeur juridique, juriste), assure la veille juridique : avocat, Département des Achats, consultant juridique.
- À certains commentaires à Q1-1 « si j'ai une question, j'appelle mon avocat qui est spécialisé en informatique » sont associés, de façon contradictoire, des observations telles que « la connaissance [des contrats informatiques] est indispensable.
- à la question « Q2-2 « si l'entreprise applique une démarche qualité, quel(s) référentiel(s) utilise-t-elle », 5 référentiels sont cités, dont seul le référentiel ADELI appelle le commentaire suivant : « l'adhérent [est] au centre de l'Association ».

# 4. Annexes

## 4.1. Glossaire

- **CIL :** Correspondant Informatique et Libertés, fonction créée en 2003 dans les entreprises, permettant de mieux assurer la protection juridique et l'utilisation ad hoc des données personnelles traitées.

- **Cloud computing** (« informatique dans les nuages ») : déportation du système informatique d'une entreprise sur des serveurs informatiques distants (« informatique dématérialisée »).
  L'utilisateur n'a plus à gérer l'infrastructure sous-jacente des réseaux, mais le système n'est intéressant que si les données de l'entreprise demeurent protégées là où elles se trouvent.

- **Éthique :** sorte de « comportement moral » consistant dans le respect de normes visant à respecter les autres membres de la société, leurs expressions, le plus souvent en se conformant à un ensemble de règles, soit implicites, soit réglementées ou légalisées.
  L'éthique en informatique visera à utiliser les données personnelles d'autrui dans des conditions de protection, de non-divulgation, de non-utilisation commerciale.

- **Réseau social** : site interactif dans le cadre du « Web 2.0 », regroupant des internautes liées par une tendance ou des goûts communs, une activité, ou appartenant à une organisation (associative, politique, confessionnelle).
  Chaque internaute définit un profil personnel, plus ou moins « protégé ».
  Les réseaux sociaux se développent, les principaux utilisateurs actuels à titre le plus souvent personnel, étant les 15-40 ans.

## 4.2. Les réponses au questionnaire

**Q1-1 Qui assure la veille juridique dans votre entreprise ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 7 | 11,48% |
| Un(e) juriste | 15 | 24,59% |
| Le Directeur juridique | 8 | 13,11% |
| Personne | 15 | 24,59% |
| Autre | 16 | 26,23% |
| Non complété | 0 | 0 |

**Q1-2 – comment êtes-vous informé des obligations légales incombant à votre métier ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 7 | 11,48% |
| par le « bouche à oreille » | 12 | 19,67% |
| par des formations | 5 | 8,20% |

**Q1-3 En particulier, connaissez-vous les règles générales en termes de contrats informatiques ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 7 | 11,48% |
| Oui | 14 | 22,95% |
| Non | 8 | 13,11% |
| Partiellement | 32 | 52,46% |
| Non complété | 0 | 0 |

**Q1-4 Estimez-vous que cette connaissance est indispensable à l'exercice de votre métier ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 10 | 16,39% |
| Oui - Absolument indispensable | 22 | 36,07% |
| Non - Ce n'est pas mon métier | 7 | 11,48% |
| Partiellement - C'est un plus | 22 | 36,07% |
| Non complété | 0 | 0 |

**Q2-1 L'entreprise applique-t-elle une démarche qualité ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 0 | 0 |
| Oui | 26 | 42,62% |
| Non | 27 | 44,26% |
| Non complété | 8 | 13,11% |

**Q2-2 Si oui, quels référentiels utilise-t-elle ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| ISO 9001 | 14 | 22,95% |
| EFQM | 2 | 3,28% |
| ISO 20000 | 1 | 1,64% |
| ITIL | 14 | 22,95% |
| 6 SIGMA | 3 | 4,92% |
| Autre :<br>• ADELI<br>• CMMI<br>• Q QualiServ<br>• SOX<br>• ISO14000 | 7 | 11,48% |

**Q3-1 L'entreprise dispose-t-elle d'un Correspondant Informatique et Libertés ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 0 | 0 |
| Oui | 13 | 21,31% |
| Non | 35 | 57,38% |
| Non complété | 13 | 21,31% |

**Q3-2 Si oui, connaissez-vous son nom ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 36 | 59,02% |
| Oui | 8 | 13,11% |
| Non | 5 | 8,20% |
| Non complété | 12 | 19,67% |

**Q3-3 Si oui est-il externe ou interne à l'entreprise ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 37 | 60,66% |
| Interne à l'entreprise | 12 | 19,67% |
| Externe à l'entreprise | 0 | 0 |
| Non complété | 12 | 19,67% |

**Q3-4 Connaissez-vous ses fonctions dans l'entreprise ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 39 | 63,93% |
| Oui | 10 | 16,39% |
| Non | 0 | 0 |
| Non complété | 12 | 19,67% |

**Q3-5 Si oui a-t-il en charge le recensement de « failles de sécurité » ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 43 | 70,49% |
| Oui | 4 | 6,56% |
| Non | 2 | 3,28% |

**Q3-6 À votre connaissance, combien de déclarations à la CNIL l'entreprise a-t-elle effectuées ces deux dernières années ?**

| Calcul | Résultat |
|---|---|
| Décompte | 31 |
| Somme | 298 |
| Écart type | 28,90 |
| Moyenne | 9,61 |
| Minimum | 0 |
| 1er quartile (Q1) | 0 |
| 2ème quartile (Médiane) | 0 |
| 3ème quartile (Q3) | 2 |
| Maximum | 150 |

*Les valeurs nulles sont ignorées dans les calculs.*
*Q1 et Q3 sont calculés en utilisant la Méthode « minitab »*

**Q3-7 En particulier, un (ou plusieurs) dispositif(s) informatisé(s) de contrôle d'accès aux locaux (badges, code,..) ont-ils fait l'objet d'une déclaration?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 22 | 36,07% |
| Oui | 6 | 9,84% |
| Non | 21 | 34,43% |
| Non complété | 12 | 19,67% |

**Q3-8 Pour certains traitements à caractère personnel dans l'entreprise, une « durée de conservation des données » a-t-elle été définie ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 17 | 27,87% |
| Oui | 12 | 19,67% |
| Non | 20 | 32,79% |
| Non complété | 12 | 19,67% |

**Q3-9 L'entreprise est-elle soumise à la « Loi Sarbanes-Oxley » sur l'audit et le contrôle interne ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 15 | 24,59% |
| Oui | 4 | 6,56% |
| Non | 30 | 49,18% |
| Non complété | 12 | 19,67% |

**Q4-1 Y-a-t-il un responsable de la Sécurité des Systèmes d'Information ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 0 | 0 |
| Oui | 24 | 39,34% |
| Non | 20 | 32,79% |
| Non complété | 17 | 27,87% |

**Q4-2 Si oui, le connaissez-vous ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 21 | 34,43% |
| Oui | 24 | 39,34% |
| Non | 0 | 0 |
| Non complété | 16 | 26.23% |

**Q4-3 Si oui, à quel service (département, division, etc.) le responsable sécurité est-il rattaché ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| • au Service Sécurité des SI, rattaché au Directeur du Pôle Support (qui a rang de Directeur général adjoint)<br>• Centre de ressources informatiques<br>• Département Infrastructure & Production<br>• Direction<br>• Direction Administrative et Financière<br>• Direction générale<br>• Direction Générale ou Direction de l'Informatique<br>• DOSI<br>• DSI<br>• IT<br>• Rattaché opérationnellement à la DG, hiérarchiquement à la production Informatique<br>• Réseaux<br>• Sécurité<br>• Service technique<br>• Système et réseaux | 22 | 36,07% |
| Sans réponse | 39 | 63.93% |
| Non complété | 0 | 0 |

**Q4-4 L'entreprise applique-t-elle un référentiel sécurité ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 39 | 63,93% |
| ISO 27001 | 5 | 8,20% |
| Autre | 1 | 1,64% |
| Non complété | 16 | 26,23% |

**Q4-5 L'entreprise a-t-elle obtenu une certification sécurité ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 43 | 70,49% |
| ISO 27001 | 1 | 1,64% |
| Autre | 1 | 1,64% |
| Non complété | 16 | 26,23% |

**Q4-6 Existe-t-il une charte des bonnes pratiques de la sécurité des systèmes d'information ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 0 | 0 |
| Oui | 23 | 37,70% |
| Non | 21 | 34,43% |
| Non complété | 17 | 27,87% |

**Q4-7 Si oui, quels domaines cette charte couvre-t-elle ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Messagerie interpersonnelle | 21 | 34,43% |
| Intranet | 17 | 27,87% |
| Échange de données informatisées | 16 | 26,23% |
| Intelligence économique | 5 | 8,20% |
| Autres domaines | 5 | 8,20% |

**Q4-8 Y-a-t-il des séances de sensibilisation à la sécurité des systèmes d'information ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 0 | 0 |
| Oui | 15 | 24,59% |
| Non | 29 | 47,54% |
| Non complété | 17 | 27,87% |

**Q4-9 Si oui, quelles sont les populations concernées ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| • Chefs de projet<br>• Équipes informatiques, MOA<br>• la DSI et le personnel au travers de campagne d'affichage de recommandations<br>• Utilisateurs des bases de données<br>• Management et chefs de projet<br>• Managements général, 1e et 2e ligne Métiers Informaticiens, télécommunicants<br>• L'ensemble des collaborateurs.<br>• Personnels DSI et métier<br>• Tous salariés | 14 | 22,95% |
| Sans réponse | 47 | 77,05% |
| Non complété | 0 | 0 |

**Q4-10 Avez-vous vous-même suivi une telle sensibilisation ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 4 | 6,56% |
| Oui | 18 | 29,51% |
| Non | 23 | 37,70% |
| Non complété | 16 | 26,23% |

**Q4-11 Ces formations impliquent-elles le management ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 22 | 36,07% |
| Oui | 16 | 26,23% |
| Non | 7 | 11,48% |
| Non complété | 16 | 26,23% |

**Q4-12 Ces formations impliquent-elles les personnes extérieures sous contrat ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 25 | 40,98% |
| Oui | 8 | 13,11% |
| Non | 12 | 19,67% |
| Non complété | 16 | 26,23% |

**Q4-13 A votre connaissance l'entreprise a-t-elle connu des malveillances notoires ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 10 | 16,39% |
| Oui | 13 | 21,31% |
| Non | 22 | 36,07% |
| Non complété | 16 | 26,23% |

**Q4-14 A votre connaissance l'entreprise a-t-elle connu des pertes de données ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 11 | 18,03% |
| Oui | 10 | 16,39% |
| Non | 24 | 39,34% |
| Non complété | 16 | 26,23% |

**Q4-15 A votre connaissance l'entreprise a-t-elle connu des contentieux liés à la sécurité informatique ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 7 | 11,48% |
| Oui | 6 | 9,84% |
| Non | 32 | 52,46% |
| Non complété | 16 | 26,23% |

| **Q4-16 L'entreprise utilise-t-elle des logiciels de chiffrement ?** | | |
|---|---|---|
| Réponse | Décompte | Pourcentage |
| Sans réponse | 6 | 9,84% |
| Oui | 19 | 31,15% |
| Non | 20 | 32,79% |
| Non complété | 16 | 26,23% |
| **Q5-1 L'entreprise utilise-t-elle, ou a-t-elle l'intention d'utiliser, des « logiciels libres » ?** | | |
| Réponse | Décompte | Pourcentage |
| Sans réponse | 8 | 13,11% |
| Oui | 31 | 50,82% |
| Non | 5 | 8,20% |
| Non complété | 17 | 27,87% |
| **Q5-2 L'entreprise utilise-t-elle, ou a-t-elle l'intention d'utiliser, un réseau social d'entreprise ?** | | |
| Réponse | Décompte | Pourcentage |
| Sans réponse | 16 | 26,23% |
| Oui | 11 | 18,03% |
| Non | 17 | 27,87% |
| Non complété | 17 | 27,87% |
| **Q5-3 L'entreprise a-t-elle l'intention d'externaliser tout ou partie de ses traitements, dans une configuration de « Cloud computing » ?** | | |
| Réponse | Décompte | Pourcentage |
| Sans réponse | 14 | 22,95% |
| Oui | 12 | 19,67% |
| Non | 18 | 29,51% |
| Non complété | 17 | 27,87% |
| **Q6-1 Quelle est votre situation professionnelle actuelle ?** | | |
| Réponse | Décompte | Pourcentage |
| Sans réponse | 0 | 0 |
| Actif | 40 | 65,57% |
| Inactif | 3 | 4,92% |
| Non complété | 18 | 29,51% |

| **Q6-2 Quelle est votre fonction actuelle ?** | | |
|---|---|---|
| Réponse | Décompte | Pourcentage |
| Adjoint de direction<br>Chef de service logistique<br>Consultant (5)<br>Consultant Associé Gérant<br>Consultant fonctionnel éditorial<br>Consultant gestion de projet<br>Consultant indépendant<br>Consultant senior (développt logiciel)<br>Consultant SSII<br>Consultant-Associé<br>Consultante<br>Chef de projet<br>Customer Relationship Manager<br>DG<br>Directeur associé<br>Directeur de Projets (2)<br>Directeur de projets informatiques<br>DSI<br>DSI – Auditeur<br>Enseignant-chercheur<br>Expert de justice en informatique<br>Gérant (2)<br>Gérant de ma société<br>Ingénieur conseil<br>Inspecteur bancaire aspects liés aux SI)<br>Professeur d'université<br>Propre patron<br>Responsable Études – Finance<br>Responsable Processus<br>Responsable Qualité et méthodes<br>Responsable Qualité Informatique<br>Responsable virtuel d'une association<br>Retraité<br>Sans (retraité) président de club sportif<br>Secrétaire (général)<br>Vice-Président Université | 43 | 70,49% |
| Sans réponse | 18 | 29,51% |
| Non complété | 0 | 0 |

| **Q6-3 Êtes-vous adhérent à ADELI ?** | | |
|---|---|---|
| Réponse | Décompte | Pourcentage |
| Sans réponse | 0 | 0 |
| Oui | 41 | 67,21% |
| Non | 2 | 3,28% |
| Non complété | 18 | 29,51% |

**Q6-4 Quels sont vos domaines d'intérêt au sein d'ADELI ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| • Veille - référentiels - participation à la diffusion des savoirs et au brassage d'idées d'une discipline « jeune » en perpétuelle évolution donc soumis au phénomène de « mode » au-delà du discours marketing des éditeurs et de certains professionnels<br>• AMOA, ERP<br>• appropriation des outils juridique, éthique problèmes sociétaux<br>• Architecture SI, qualité, processus<br>• cf. « Fonction actuelle » sur la base des pôles d'intérêt d'ADELI<br>• Gestion des adhérents Logistique de la revue trimestrielle Gestion des fournisseurs<br>• Gestion projet, Qualité des SI, Sécurité des données<br>• Ingénierie et qualité du logiciel<br>• la modélisation, l'analyse de la valeur, l'économie du S.I.<br>• Veille normative, le partage d'information et de bonnes pratiques<br>• Lean Six Sigma<br>• Les Systèmes d'Informations et leurs modélisations<br>• Maîtrise d\'ouvrage<br>• Management du SI<br>• Méthodes<br>• Méthodes de développement<br>• Modélisation, Réseaux sociaux<br>• Organisation, sécurité, management<br>• Qualité et respect de l'expression de besoin en SI et organisation<br>• Référentiels de SI<br>• SI / points de vue fonctionnels, organisationnels et humains - Conduite de projet.<br>• Systèmes d\'information<br>• Tous, Tout ;-)<br>• Tous, gestion, réalisation de projet et sécurité des SI en particulier<br>• Veille technologique, regard critique sur la nébuleuse des SI ++ | 29 | 47,54% |
| Sans réponse | 32 | 52,46% |
| Non complété | 0 | 0 |

**Q6-5 Avez-vous participé en 2009 ou 2010 à un Groupe de Travail ADELI ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| Sans réponse | 0 | 0 |
| Oui | 11 | 18,03% |
| Non | 32 | 52,46% |
| Non complété | 18 | 29,51% |

**Q6-6 Si oui, lequel ?**

| Réponse | Décompte | Pourcentage |
|---|---|---|
| • Guide des certifications.<br>• HCSI<br>• Juridique et Internet du Futur (3)<br>• Lean Six Sigma (5)<br>• Positionnement et Notoriété (2) | 11 | 18,03% |
| Sans réponse | 50 | 81,97% |

## 4.3. Références adéliennes

De nombreux témoignages, réflexions, rubriques, articles de fond alimentent, outre le Groupe de Travail cité au § 1, les deux principaux organes de communication adéliens, la Lettre trimestrielle et le site ADELI, sur le thème « Juridique et Internet du Futur ».

### 4.3.1. La Lettre

Tout adhérent d'ADELI reçoit trimestriellement la « Lettre d'ADELI » qui contient des articles de fonds, dont ceux remontant à plus de deux ans sont librement téléchargeables par le public.

Voici un tableau de récentes Lettres contenant des articles sur le thème juridique et législatif :

| Référence | Date parution | Articles |
|---|---|---|
| Lettre n°75 | Printemps 2009 | Réseautage social |
| Lettre n°76 | Été 2009 | Facebook : les pièges à éviter |
| Lettre n°79 | Printemps 2010 | • Les principales lois informatiques françaises<br>• Des nouvelles d'HADOPI<br>• L'entreprise face aux réseaux sociaux |
| Lettre n°80 | Été 2010 | Le rôle du CIL dans l'entrepri se |
| Lettre n°82 | Hiver 2011 | Cloud computing, juste du bu zz ? |

### 4.3.2. Le site ADELI : extraits d'articles

Le paragraphe ci-après présente une sélection de diverses communications parues sur le site ADELI depuis le début de l'année 2010 sur le thème étudié.

Celles-ci consistent en extraits d'articles, billets de forums ou de blogs, qui résultent :

- soit de rédactions de la part des membres d'ADELI ;
- soit de reproductions totales ou partielles, de contenus de sites choisis. Ces dernières respectent les droits d'auteur et licences d'utilisation pour la reproduction et la diffusion (suivant l'article L122-4 du Code de la Propriété Intellectuelle).

#### 4.3.2.1. Nouveau statut du CIL (billet de blog, 09/05/2010)

La Loi Informatique et Libertés (LIL) du 6 janvier 1978, modifiée le 6 août 2004, a introduit une fonction permettant de mieux assurer le respect de ces droits fondamentaux : le Correspondant à la protection des données à caractère personnel ou « Correspondant informatique et libertés » (CIL).

La LIL permet à l'organisme de désigner un CIL : il s'agit d'une faculté et non d'une obligation légale. On assiste à l'esquisse d'une nouvelle fonction. Dans le texte de 2004 et son décret d'application d'octobre 2005, la fonction du CIL est à peine mentionnée.

L'Article 22-III de la loi du 6 janvier 1978 modifiée stipule : « La désignation d'un correspondant informatique et libertés, ou « CIL », permet au responsable du traitement d'alléger ses obligations déclaratives auprès de la CNIL.

Il désigne, au sein de sa structure (ou en externe pour les petites structures), une personne qui sera chargée : de tenir un registre des traitements mis en œuvre au sein de l'organisme, d'établir un bilan annuel et de veiller au respect des dispositions de la LIL au sein de l'organisme. »

La réforme de la LIL du 23 mars 2010 consacre la fonction du « CIL ». Les amendements relatifs à la nomination obligatoire du CIL, qui composent la proposition de loi, reflètent cette volonté du législateur d'asseoir cette fonction au sein des entreprises aussi bien publiques que privées. Le seuil initial pour la nomination obligatoire d'un CIL était fixé à 50 salariés. Il a été voté un amendement modificatif fixant ce seuil à 100 salariés.

Cette nouvelle obligation légale constitue une reconnaissance d'un dispositif qui a déjà permis la diffusion de la culture informatique et libertés au sein de nombreux organismes publics et privés.

La mission essentielle du CIL est de veiller à l'application de la loi : le Correspondant est « chargé d'assurer d'une manière indépendante, le respect des obligations prévues dans la présente loi » ; il veille au respect des obligations pour les traitements pour lesquels il a été désigné ; il est consulté avant la mise en œuvre des traitements « listés » Cette mission le conduira à endosser plusieurs rôles auprès du responsable de traitement :

- gérer les « livrables » obligatoires : registre des traitements, bilan annuel, registre failles de sécurité…
- responsabilité vis-à-vis du responsable de traitement ;
- responsabilité vis-à-vis de la CNIL ;
- obligation de conseil ;
- obligation de contrôle de conformité.

Grâce à la réforme du 23 mars 2010, il est reconnu comme un personnage incontournable, à la fois chargé de la bonne application de la LIL et garant de la protection des données à caractère personnel au sein de son entreprise. C'est une fonction qui concentre à elle seule plusieurs compétences : juridiques, informatiques et techniques. Dès lors, une question se pose depuis sa création en 2004 : dispose-t-il en pratique des moyens nécessaires pour répondre à ses missions et ses obligations ?

*(© CNIL - droits réservés, avec autorisation de diffusion associative)*

### 4.3.2.2. Cloud computing : définitions générales, types d'infrastructures concernées... (billet de blog, 17/01/2011)

- Cloud computing - notions générales, implantation

Le concept de « Cloud computing » (« informatique dans les nuages ») est comparable à celui de la distribution de l'énergie électrique. La puissance de calcul et de stockage de l'information est proposée comme produit aux services informatiques par des compagnies spécialisées ; les entreprises n'ont plus besoin de serveurs propres, mais externalisent en ligne leurs ressources à un « fournisseur » qui leur garantit une puissance de calcul et de stockage à la demande plus importante qu'en traitement local.

Ce qui, début 2010, apparaissait encore comme un simple « buzz » - appuyé sur des néologismes autour de la virtualisation - semble se dessiner comme une tendance lourde de l'organisation et des contrats de gestion dans les infrastructures informatiques actuelles.

NB- Des articles détaillés sur ce thème ont été publiés dans la Lettre n°82 de l'hiver 2011.

- Catégories de « Cloud » :

On parle de « Clouds publics » et « Clouds privés (d'entreprise) », mais aussi parmi ces derniers, de « Clouds externes » ou « internes » à l'entreprise. Il y a 3 types de Cloud suivant la « couche » sous-traitée collectivement par le fournisseur :

- IaaS « Infrastructure As A Service » : l'entreprise maintient : les applications, les runtimes, les bases de données, le logiciel serveur ; le fournisseur maintient la virtualisation, le matériel serveur, le stockage, les réseaux ;
- PaaS « Platform As A Service »: l'entreprise maintient uniquement les applications ; le fournisseur maintient : les runtimes, l'intégration ;
- SaaS « Software As A Service » : le fournisseur maintient l'ensemble : applications, runtimes, bases de données, logiciel serveur, virtualisation, serveur, stockage, réseaux. Le Saas est un modèle économique original, où les applications sont consommées et payées à la demande (par utilisateur et par minute d'utilisation par exemple) et non plus acquises par l'achat de licences.

En rajoutant une couche « Bureau » (desktop) et une couche « Mémoire » (storage), on peut symboliser un réseau complet de « Cloud » classiquement en plusieurs couches : soft/bureau/plateforme, réseau, utilisateur, stockage (Datacenter).

- Entreprises fournissant des systèmes de « Cloud »

Amazon, Google, IBM, Intel, Microsoft, Yahoo sont les principaux fournisseurs de Cloud. Certaines de ces sociétés ont noué des partenariats. Citons également Oracle et VMware pour les applications.

- Rentabilité d'un Cloud

L'investissement dans un tel système s'élève en général, à plusieurs dizaines, voire centaines de k€. Le calcul de retour sur investissement tenant compte des simplifications (forces humaines) est donc un passage obligé dans tous les cas.

- Problèmes de protection des données

Ils sont nombreux :

- sécurisation de l'accès à l'application entre le client et le serveur distant (risques d'attaques réseau ;
- perte de la maîtrise de l'implantation des données ;
- statut juridique de la délocalisation des données : en Espagne, des poursuites ont été engagées contre Google pour avoir détourné et stocké des données Wifi personnelles ; en Angleterre, des internautes ont identifié une photo ambiguë concernant une fillette gisant à même le sol, d'où une réaction des autorités de police. On ne peut que se réjouir d'initiatives pour défendre les libertés individuelles (par exemple le droit à l'image).

#### 4.3.2.3. Maîtriser les informations publiées sur les réseaux sociaux (publié le 10/1/2011)

Les paragraphes qui suivent détaillent la réponse à diverses questions de protection des données sur les réseaux sociaux actuels.

- Est-il possible de se faire licencier pour des propos tenus sur un réseau social ?

Oui. Le conseil des prud'hommes de Boulogne s'est prononcé sur une affaire concernant trois salariés qui se sont fait licencier pour avoir dénigré leur hiérarchie sur Facebook.

Le tribunal a considéré que les propos publiés sur le mur d'un des salariés étaient publics car accessibles aux « amis d'amis ». Ces propos ont perdu leur caractère privé du fait qu'ils étaient accessibles à des personnes non concernées par la discussion.

- Quelles précautions un salarié doit-il prendre quand il diffuse des informations sur un réseau social comme Facebook ?

La CNIL a toujours appelé les utilisateurs de Facebook à la plus grande vigilance vis-à-vis des contenus qu'ils diffusent sur leurs pages, et des personnes qui peuvent y accéder.

C'est d'autant plus important que les informations qui figurent sur les profils Facebook sont de plus en plus souvent utilisées pour justifier des mesures disciplinaires, dans un cadre professionnel ou scolaire.

De manière générale, on ne dit pas, la même chose à sa famille, à son ami d'enfance, à son collègue de bureau ou à son patron. Sur Facebook, il faut adopter les mêmes réflexes.

- Peut-on différencier des catégories de contacts sur Facebook ?

Facebook permet de répartir ses contacts dans des listes. Vous pouvez ainsi créer différentes listes correspondant aux membres de votre famille, à vos amis proches, à vos collègues, etc., puis adapter les paramètres de confidentialité en fonction des informations que vous souhaitez partager avec chaque catégorie de personnes.

- Comment peut-on créer des listes d'amis et quels sont les avantages pour les utilisateurs ?

L'avantage principal des listes d'amis est de classer les contacts que nous avons sur Facebook. Il faut savoir que sur Facebook, les gens ont en moyenne 120 amis.

De nombreux utilisateurs aujourd'hui ont, parmi leurs contacts, des personnes qu'ils n'ont rencontrées qu'une fois. Ils ne souhaitent pas forcément que ces personnes, qu'ils connaissent peu dans la vie réelle, aient accès à leurs dernières photos de vacances ou aux discussions publiées sur leur « mur ». Ils peuvent en revanche vouloir partager ces informations avec d'autres personnes plus intimes. L'intérêt de répartir ces personnes dans différentes listes est de faciliter le paramétrage des accès aux différents contenus de leur profil.

La CNIL milite depuis plusieurs années pour que les utilisateurs prennent conscience de l'importance de bien gérer leurs données personnelles sur les réseaux sociaux. Elle s'est aussi rapprochée des différents réseaux sociaux pour que leurs paramètres de confidentialité deviennent plus clairs, plus accessibles et plus complets.

D'ailleurs, une étude récente de l'agence Iligo montre que 74% des membres français de Facebook ont déjà utilisé les paramètres de confidentialité pour restreindre l'accès à leurs données, et que 45% le font régulièrement.

Mais cette étude montre aussi que 60% des internautes pensent qu'il n'est pas facile de modifier ou de supprimer des données personnelles sur Internet. Ceux qui n'y parviennent pas peuvent adresser une plainte en ligne à la CNIL, car notre Commission est là pour les aider.

### 4.3.2.4. La publicité ciblée en questions (site CNIL, publié le 13/4/2011)

- En quoi consiste précisément la publicité ciblée ?

Après avoir réservé un billet d'avion pour Berlin sur Internet, si vous lisez dans votre quotidien en ligne, une publicité qui vous propose des locations de voitures ou de logements pour cette ville, ce n'est évidemment pas une coïncidence. C'est ce qu'on appelle de la publicité ciblée. Il s'agit en fait de personnaliser la publicité en fonction des données qu'un internaute a communiquées à un site ou en fonction du comportement de navigation. La personnalisation peut dépendre des actions effectuées sur le site visité mais aussi sur d'autres sites ayant recours à la même régie publicitaire.

Comment peut-on connaître les centres d'intérêt ou les caractéristiques d'un internaute ? Il existe différentes techniques :

- 1er cas : l'internaute a fourni des informations sur sa personne : son âge, son sexe, sa localisation, mais aussi ses centres d'intérêt. On pourra alors le classer dans une catégorie marketing : par exemple « jeune urbain » ou « senior ».
- 2e cas : l'analyse de la manière dont l'internaute navigue sur Internet, les liens sur lesquels il clique, les recherches qu'il effectue, permettent d'obtenir des indices sur ses centres d'intérêt supposés et ainsi de déterminer la publicité qui sera affichée sur son écran.
- Techniquement, comment sont enregistrés les parcours des internautes ?

Les techniques de profilage des internautes passent souvent par l'utilisation de « cookies ». Les cookies sont des petits fichiers que les serveurs des sites visités installent sur l'ordinateur de l'internaute, afin, entre autres, d'enregistrer des informations sur l'internaute, ses préférences ou encore son parcours sur le site web.

Certains cookies peuvent être lus par plusieurs sites différents, ce qui permet de suivre la navigation de l'internaute sur la toile d'un site à un autre. Cela peut s'avérer très intrusif.

- Existe-t-il d'autres méthodes pour mettre en place de la publicité ciblée ?

Oui, par exemple, sur le réseau social Facebook qui surveille votre activité sur son site et même au-delà, grâce aux boutons « J'aime » ou « Like ». Ainsi, quand un utilisateur se rend sur une page Internet où se trouve un bouton « J'aime », Facebook peut associer cette visualisation à son profil. Et cela sans même que l'utilisateur ne clique sur le bouton. Facebook a ainsi la possibilité d'adapter sa publicité en fonction des sites visités par l'internaute.

- La publicité ciblée est-elle légale ?

Oui, à condition que les internautes soient informés de ces mécanismes de profilage et de l'utilisation qui sera faite de leurs données personnelles. Ils doivent également connaître les moyens mis à leur disposition pour s'y opposer.Certains acteurs proposent d'ailleurs des techniques permettant aux internautes de connaître et de modifier le profilage dont ils font l'objet ?

Enfin, pour ce qui est des boutons « J'aime », on peut regretter que Facebook ne communique pas davantage sur ces fonctionnalités et notamment sur la possibilité d'utilisation de l'historique de navigation des utilisateurs.

- Peut-on s'opposer à la publicité ciblée ?

Il est possible de paramétrer son navigateur pour bloquer ce qu'on appelle les « cookies tiers ». Mais la méthode la plus efficace consiste à effacer régulièrement l'ensemble des « cookies » de son navigateur.

Il existe également des outils, comme « Ghostery », permettant de bloquer l'affichage des publicités ainsi que des boutons Facebook sur les pages web. De cette manière, aucune information sur la visite du site par l'internaute n'est transmise à la régie publicitaire ou à Facebook.

- Existe-t-il d'autres méthodes pour refuser la publicité ciblée ?

Normalement, si un site Internet utilise un cookie pour analyser le profil de ses visiteurs, il doit alors les informer de la mise en place de ce cookie, de son objet et de leur droit de le refuser. Dans la pratique, les cookies sont massivement utilisés sans que l'internaute en soit toujours informé correctement. Les règles applicables aux cookies et utilisées pour encadrer leur utilisation sont d'ailleurs sur le point d'être réexaminées, dans la cadre de la transposition d'une directive européenne. Cette directive crée de nouvelles obligations pour les professionnels d'Internet qui devront notamment obtenir l'accord préalable de l'internaute avant toute installation de cookie.

- Quels moyens sont mis en œuvre par la CNIL ? auprès des régies publicitaires ne respectant pas la loi ?

Tout citoyen peut saisir la CNIL lorsqu'il constate des abus ou des pratiques irrégulières. La CNIL interviendra auprès de l'auteur de la publicité ou du responsable du site Internet sur lequel cette publicité s'affiche. La CNIL pourra aussi procéder à un contrôle sur place pour vérifier que l'entreprise concernée respecte bien la loi.



### 4.3.2.5. Puissance et risques des réseaux sociaux et politiques publiques

Les « réseaux sociaux » ne cessent de défrayer l'actualité depuis leur début de montée en puissance. Il y a quelques mois, l'« apéro géant » (7 000 participants) organisé à Nantes après une annonce sur Facebook avait indirectement engendré un accident mortel dû à une alcoolémie excessive chez un jeune homme ; ce qui a, une fois de plus, posé la question de l'anonymat sur ces réseaux, et donc soit la responsabilité du rédacteur, soit celle de l'éditeur.

À cette question de l'anonymat sont associées d'autres particularités d'« auberge espagnole » constatées dans l'extension actuelle de ces systèmes : toutes les instances s'accordent à le reconnaître, mais les solutions si elles existent, tardent à se mettre en place :

- si l'adhérent à un réseau social n'adopte pas des règles minimales de confidentialité, la banalisation des échanges entraîne une perméabilité des types personnel, juridique ou commercial. Souvent, les réseaux sont reliés à d'autres sites : ainsi, un système (…) permet à partir de certains sites, de publier gratuitement les nouveautés du site sur un compte Facebook donné et vice-versa, d'ouvrir ce site aux « amis » du titulaire du compte ;
- beaucoup d'adhérents à des réseaux n'affichent pas de finalité affirmée pour leur utilisation du réseau, et la plupart des serveurs ne sont pas adossés à des structures économiques stables ;
- progressivement, les réseaux entrent en concurrence avec des systèmes informatiques (Éducation Nationale, Culture..) ou des medias plus anciens (sites d'actualité, moteurs de recherche, forums et blogs) (…)
- Il apparaît qu'aussi bien les pouvoirs publics que le monde économique ne semblent pas pressés de « réglementer » ce nouveau type de média, comptant avec le temps sur une auto-adaptation sociétale des usagers (qui peut prendre quelques décennies). En revanche, des accords ou partages de territoires semblent se faire au coup par coup dans le monde des multinationales informatiques (…)
  *(librement rédigé et réactualisé à partir d'un article de 01net.com)*

# LES AUTEURS


**Patrick KINEIDER**

ingénieur diplômé, retraité depuis 2008 de l'entreprise publique EDF où il a exercé des fonctions d'analyste, de chef de projet, de gestion de parc, dans divers paliers techniques, puis d'expert en sécurité des systèmes d'information, dans le domaine de l'informatique de gestion.
Adhérent à ADELI depuis 2007, il anime, depuis 2010, le Groupe de Travail « Juridique et Internet du futur », domaine qui recoupe en partie ses dernières fonctions dans l'entreprise.

**Dominique BERGEROT**

après quelques années d'enseignement, s'est orientée vers la gestion de projets en informatique industrielle et temps réel et vers les aspects méthodes et qualité des projets, puis vers le conseil, l'organisation et l'urbanisation de projets.
Adhérente à ADELI depuis 2006, membre du Comité, elle anime le Groupe de Travail « Métiers » et est membre du Groupe « Juridique et Internet du futur » ; et considère que l'aspect juridique des SI est à présent incontournable.

**Martine OTTER**

a rempli successivement les fonctions de directeur de projet, Directeur « qualité, audit interne et sécurité », au sein de diverses sociétés de service en informatique.
Expert de justice auprès de la Cour d'Appel de Paris, elle exerce aujourd'hui en tant que conseil indépendant.
Depuis 1999, elle préside ADELI, Association pour la Maîtrise des Systèmes d'Information.

**Thêt SOK**

juriste de formation, a fondé un Cabinet de conseil en droit des NTIC et des Systèmes d'Information.
Elle est membre de plusieurs associations juridiques, et exerce tout particulièrement la fonction de correspondant CNIL (appelé « CIL ») externe, au sein de différents groupes et entreprises.
Elle est également auteur de publications dans ces domaines.
Elle a adhéré début 2010 à l'Association ADELI, et a apporté sa contribution aux productions du groupe de travail « Juridique et Internet du Futur ».


# RÉSUMÉ


Le présent document, produit par le Groupe de Travail ADELI « Juridique et Internet du Futur », concerne le socle juridique, les risques sécuritaires et éthiques des Systèmes d'Information et leur perception dans les métiers correspondants.
Il exploite une enquête ADELI du 2e semestre 2010 sur la connaissance de ce thème auprès de nos adhérents. L'ouvrage comprend un premier chapitre sur le contexte juridique, un deuxième sur les réponses globales à l'enquête, un troisième sur les réponses détaillées, suivi de diverses références adéliennes sur le sujet (« Lettres » publiées entre 2009 et 2011, reproduction de textes ou d'articles figurant sur le site adeli.org).



Adeli
www.adeli.org

**Adresse**
87 rue Bobillot
75013 PARIS
**Téléphone :**
01 45 89 02 01

N° ISBN : 2-9517899-3-9