Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

JURIDENDANCES INFORMATIQUE ET LIBERTES

n° 61 – Janv-Févr. 2015

LE NOUVEAU LABEL CNIL « GOUVERNANCE INFORMATIQUE ET LIBERTES »

Un nouveau référentiel « gouvernance Informatique et libertés »

Les enjeux

- Le **11 décembre 2014**, la Cnil a adopté son **quatrième référentiel** lui permettant de délivrer des labels concernant les procédures de gouvernance Informatique et Libertés (1).
- Ce nouveau label fait suite aux labels « formation », « procédure d'audit » et « coffre-fort numérique » pour lesquels la Cnil a délivré au total 37 labels aux organismes candidats.
- La **gouvernance « Informatique et Libertés »**, désigne l'ensemble des mesures, des règles et des bonnes pratiques qui permettent l'application des lois et règlements pour la gestion de ces données, et de préciser les responsabilités qui interviennent dans cette gestion.
- Le label est un **outil de responsabilisation** et un véritable **indicateur de confiance** pour leurs clients ou usagers.
- Ce nouveau référentiel définit les critères d'**évaluation** et les moyens permettant à la Cnil de déterminer si les procédures de gouvernance présentées sont conformes aux exigences fixées.

Ce nouveau label permet de préparer les organismes aux règles du futur règlement européen en intégrant notamment le principe d'accountability.

(1) Délib. n°2014-500 du 11-12-2014

Les exigences requises pour bénéficier du label

Les conseils

- Ce nouveau référentiel prévoit **25 exigences cumulatives** afin de bénéficier du label « Gouvernance Informatique et libertés ».
- Ces exigences sont réparties selon les **trois thématiques** suivantes :
  - l'**organisation interne** liée à la protection des données, comprenant des exigences relatives à l'adoption d'une politique de protection des données et au statut, à la formation, aux ressources et aux activités du correspondant Informatique et libertés (Cil) ;
  - la **méthode de vérification** de la conformité des traitements à la loi Informatique et libertés avec des exigences sur l'analyse et le contrôle de la conformité ;
  - la **gestion des réclamations** et incidents, intégrant des exigences sur la gestion des réclamations et droits des personnes, sur la journalisation des événements de sécurité et sur la gestion des violations de données.
- Il convient de préciser que ce référentiel s'adresse uniquement aux organismes disposant d'un correspondant Informatique et libertés (Cil).

Réaliser un audit de conformité du dispositif aux exigences du référentiel avant de déposer un dossier de candidature.

CELINE AVIGNON
RAOUF SAADA

LA NORME ISO 27018 : UN RENFORCEMENT DE LA SECURITE DES DONNEES PERSONNELLES CLOUD

La normalisation : une réponse efficace à la question de sécurité

▪ L'organisme **ISO** a répondu à la question de sécurité des informations personnelles identifiables (IPI) traitées dans le cloud en adoptant **la première norme internationale de sécurité 27018**.

▪ La norme 27018 applique des **standards préexistants** qui fournissent un socle commun des contrôles de sécurité (1) et facilitent la sélection, la mise en œuvre et la gestion de mesures de sécurité en prenant en compte les spécificités de chaque environnement (2).

▪ Pour parvenir à atteindre ces objectifs, elle applique ces normes en se focalisant dans la protection des données personnelles dans un environnement cloud public.

▪ Les **objectifs principaux** de la nouvelle norme de sécurité sont les suivants :

- assister les **responsables de traitement** des données personnelles migrées dans un environnement Cloud de se **conformer à la réglementation** en vigueur ;
- renforcer la **transparence des offres cloud public** disponibles dans le marché informatique et du **niveau de protection des données personnelles migrées,** accordé par les différents prestataires ;
- faciliter la phase la négociation commerciale des acteurs qui envisagent de **s'engager dans un contrat cloud public** ;

▪ élaborer un **mécanisme d'exercice du droit d'audit** qui vise à assurer la bonne exécution de l'obligation de sécurité mise en place à l'égard des prestataires informatiques

L'apport de la norme ISO 27018 pour les entreprises

▪ La volonté profonde des auteurs de cette norme est de **restaurer la confiance des utilisateurs** dont les données sont « cloudisées » dans un système informatique externe. Cela devient possible en respectant ce **nouveau code de bonnes pratiques** assurant un niveau de protection élevé aux données personnelles migrées dans un environnement cloud public.

▪ La nouvelle norme s'inscrit dans un **mouvement de responsabilisation** des entreprises informatiques. Elle vise à satisfaire le principe d'*accountability* d'origine anglo-saxonne qui consiste à répondre efficacement aux exigences de sécurité et de conformité à la réglementation en vigueur.

▪ L'adoption de la norme n'a **pas de caractère réglementaire obligatoire**. Or, les prestataires qui font le choix de l'appliquer fournissent une preuve incontestable aux utilisateurs du fait qu'ils disposent un **très haut niveau** de protection des données personnelles traitées sur le cloud.

▪ Le caractère certifiable de la norme renforce l'**exercice d'un droit d'audit**. La norme 27018 constitue alors une **référence incontournable** pour les acteurs du cloud.

▪ Nul doute que cette norme est appelée à fonder l'état de l'art des mesures de sécurité nécessaires pour **rétablir la confiance** au niveau du traitement des données personnelles. Elle doit être d'ores et déjà utilisée comme référentiel pour la négociation ou la renégociation des contrats cloud.

Les enjeux

La norme 27018 permet d'identifier les risques particuliers à l'environnement Cloud public menaçant l'intégrité des données personnelles.

(1) ISO/IEC 27001 :2013 Management de la sécurité de l'information.

(2) ISO/IEC 27002:2013 Technologies de l'information, Techniques de sécurité, Code de bonne pratique pour le management de la sécurité de l'information.

Les conseils

Non obligatoire, cette norme permet de garantir un niveau de sécurité satisfaisant tout en étant vecteur de confiance.

Appliquer cette norme doit permettre de lever les dernières réserves à un projet de migration vers le cloud.

ERIC LE QUELLENEC
VASILIKI ALEVIZOPOULOU

Prochains petits-déjeuners

High Tech et Culture Chinoise : élaborer une stratégie marketing : 4 février 2015

▪ Denis Niedringhaus formateur interculturel animera un Petit-déjeuner débat pour mieux comprendre la culture chinoise et élaborer des stratégies de marketing efficaces.
▪ Avec plus de 618 millions d'internautes, des services et des innovations apparaissent constamment sur le marché chinois. Les entreprises qui souhaitent s'attaquer à ce marché lucratif mais complexe doivent être à la pointe des dernières tendances technologiques mais aussi connaitre les fondements de la culture chinoise.
- Quelles leçons tirer du succès que connait la société Starbucks depuis 5 ans en Chine ?
- Quels sont les principaux obstacles et défis au plan légal ? (relations, violations de copyright, censure et VPN, etc.).
- Quels sont les équivalents chinois de Twitter, Youtube, Facebook et Ebay ?

▪ Ce petit-déjeuner sera l'occasion de mieux comprendre la culture chinoise, un préalable indispensable à l'élaboration de stratégies de marketing efficaces.
▪ **Lieu :** de 9h30 à 12h00 (accueil à partir de 9h00) dans nos locaux, 58 bd Gouvion-Saint-Cyr, 75017 Paris.
▪ **Inscription gratuite** (sous réserve des places disponibles).

Objets connectés en matière de santé : 11 février 2015

▪ Marguerite Brac de La Perrière et Uwe Diegel, Président de iHealth Labs Europe animeront un Petit-déjeuner débat sur les produits et services liés aux objets connectés dans le domaine du bien-être et de la santé.
▪ Multiplier les liens entre patients, proches, professionnels de santé et auxiliaires médicaux est, en la matière, tout l'enjeu des objets connectés et ce, à des fins de prévention, de bien-être, d'amélioration de la prise en charge et de coordination entre ces acteurs.
▪ Ces dispositifs connectés de données à caractère personnel afférentes placent le patient connecté, les fabricants, les éditeurs, les professionnels de santé au cœur de nouvelles problématiques :
- Quelle est la frontière entre les données de « bien-être » et de « santé » ?
- Comment déterminer le régime juridique applicable aux objets connectés ?
- Quelles sont les obligations relatives aux traitements de données collectées, produites et stockées ?

▪ Ce petit-déjeuner consistera en un bref état des lieux à destination des acteurs du secteur afin de guider leurs choix stratégiques liés à la conception, la commercialisation et l'utilisation de ces objets.
▪ **Lieu :** de 9h30 à 12h00 (accueil à partir de 9h00) dans nos locaux, 58 bd Gouvion-Saint-Cyr, 75017 Paris.
▪ **Inscription gratuite** (sous réserve des places disponibles). L'enregistrement en ligne est obligatoire pour y assister : formulaire en ligne.

Les applications mobiles dans tous leurs états : 11 mars 2015

▪ Céline Avignon animera un Petit-déjeuner débat sur les applications mobiles et les risques pour l'entreprise au regard de la Cnil.
▪ Les applications mobiles représentent un champ d'investigation pour la Cnil qui vient de publier les résultats de son étude menée avec l'Inria dans le cadre de son projet Mobilitics dénonçant les caractères limités et insuffisants des informations et outils mis à disposition des utilisateurs par rapport à la quantité de données collectées.
- Quels sont les principes qui doivent être respectés au regard de la loi Informatique et libertés ?
- Comment concevoir dans une démarche " privacy by design " efficace ?
- Quelle politique de confidentialité mettre en œuvre ?
- Comment assurer la gestion des données personnelles et l'information des personnes concernées ?
- Comment utiliser des cookies et autres traceurs en toute légalité ?

▪ Ce petit-déjeuner sera l'occasion de faire le point sur les risques juridiques et les moyens de garantir la protection du consommateur et de ses données personnelles dans les applications mobiles.
▪ **Lieu :** de 9h30 à 12h00 (accueil à partir de 9h00) dans nos locaux, 58 bd Gouvion-Saint-Cyr, 75017 Paris.
▪ **Inscription gratuite** (sous réserve des places disponibles). L'enregistrement en ligne est obligatoire pour y assister : formulaire en ligne.

NOTRE RESEAU DE CORRESPONDANTS ORGANIQUES LEXING VOUS INFORME

Le traitement du cyberharcèlement en Italie

Lexing Italie

Studio Legale Zallone

▪ En septembre 2014, la **Cour de cassation** italienne a eu à connaitre d'une affaire où un journaliste avait publié sur **Facebook** des commentaires insultants à caractère sexuel à propos d'une collègue de travail.

▪ Les juges devaient décider si ces commentaires pouvaient être qualifiés de harcèlement, cette infraction nécessitant, aux termes du Code pénal italien (1), que les faits litigieux aient eu lieu en public. Ce faisant, la haute juridiction italienne devait donc se prononcer sur le caractère « public » d'une page Facebook.

▪ La conclusion des magistrats de la Corte Suprema di Cassazione fut très pragmatique : si la page où les commentaires litigieux sont affichés peut être consultée sans restriction (c'est-à-dire pas seulement par des « amis », mais également par d'autres internautes, selon le mécanisme habituel de partage des réseaux sociaux), la page doit être considérée comme étant publique. Ce qui était bien le cas en l'espèce : l'**infraction de harcèlement** était dès lors **caractérisée** (2).

(1) Article 660 du code pénal italien
(2) Décision n°37596 du 12 septembre 2014

▪ Le Code pénal italien a été conçu et adopté pour un monde non numérique. Or, à l'heure du tout numérique, les juges sont aujourd'hui appelés à se prononcer dans des situations que le législateur italien n'a pas anticipées. Les magistrats doivent donc répondre à une série de questions inédites, en s'efforçant de transposer les règles établies hier dans le monde d'aujourd'hui.

▪ Pour l'instant, les tribunaux italiens ont réussi à résoudre ces nouvelles problématiques au moyen des outils traditionnels à leur disposition, mais il n'est pas exclu que cela ne puisse plus être le cas dans le futur.

Le traitement du cyberharcèlement en Allemagne

Lexing Allemagne

Schulte Riesenkampff

▪ Les plates-formes communautaires, telles que les forums et les réseaux sociaux, sont des lieux où se pratique, bien souvent de manière anonyme, le « cyberharcèlement ».

▪ Le cyberharcèlement est très fréquent dans le monde scolaire : en 2013, un élève sur trois en a été victime en Allemagne (3). Il est également présent dans le monde des affaires, notamment sous la forme de diffamation sur les réseaux sociaux. Ces actes peuvent avoir des graves répercussions commerciales pour les professionnels et les entreprises concernées.

▪ En droit allemand, la **liberté d'expression** atteint ses limites lorsque les propos tenus sont utilisés uniquement en vue de dénigrer autrui. A ce jour, **aucun texte pénal spécifique** n'incrimine le cyberharcèlement en Allemagne.

▪ Néanmoins, d'autres infractions visées dans le code pénal peuvent permettre de réprimer les actes de cyberharcèlement, telles que les insultes (art. 185) (4), la diffamation (art. 186) (5), la diffamation intentionnelle (art. 187) (6), le harcèlement (art. 238) (7), ou l'atteinte à la vie privée (art. 201 et suiv.) (8). En outre, en cas d'atteinte au droit à l'image, il est possible d'intenter une action civile en réparation. A cet égard, il convient de noter que les montants accordés en réparation du préjudice moral subi sont généralement négligeables.

(3) Rache im Netz, 26-07_2013.
(4) "Beleidigung"
(5) "Üble Nachrede"
(6) "Verleumdung"
(7) "Nachstellung"
(8) "Verletzung des persönlichen Lebens- und Geheimbereichs"

Première rencontre de l'ensemble de l'écosystème français du véhicule connecté

▪ Pour la première fois, les acteurs de la mobilité de demain se sont retrouvés début janvier à l'initiative de la CNIL pour échanger et identifier les nouveaux enjeux de ce secteur (1).

(1) Communiqué Cnil du 19-01-2015.

Signature d'une convention de partenariat entre la Cnil et le Défenseur des droits

▪ Dans le cadre d'une mission commune de protection et de promotion des droits, la Cnil signa une convention avec le Défenseur des droits en matière de traitement des plaintes (2).

(2) Communiqué Cnil du 16-01-2015.

Communiqué du G29 à la suite des attaques perpétrées à Paris

▪ Les autorités de protection des données européennes réunies au sein du G29 expriment leur profonde indignation après les attaques perpétrées à Paris et réaffirment leur attachement au respect de l'équilibre entre libertés individuelles et protection des données personnelles (3).

(3) Communiqué du 13-01-2015 (en anglais).

Autorisation unique pour les ATU et les RTU (AU-041)

▪ La Cnil simplifie les formalités pour les dispositifs d'**autorisation temporaire d'utilisation** (ATU) et de recommandation temporaire d'utilisation (RTU) mis en œuvre par les laboratoires (4). Les ATU ont pour objet de permettre l'accès précoce aux médicaments qui sont en phase finale d'évaluation avant l'obtention de leur autorisation de mise sur le marché (AMM) en France.

(4) AU-041 ATU-RTU, Délib. 2014-501 du 11-12-2014.

Enregistrement des écoutes sur le lieu de travail : nouvelle norme simplifiée

▪ La CNIL a adopté une nouvelle norme simplifiée encadrant les fichiers mis en œuvre lors de l'écoute et de l'enregistrement des conversations téléphoniques sur le lieu de travail à des fins de formation, d'évaluation ou d'amélioration de la qualité du service rendu (5).

(5) Norme simplifiée n°57, Délib. 2014-474 du 27-11-2014.

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan.

Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier

Diffusée uniquement par voie électronique – gratuit –

ISSN 1634-0701

Abonnement à partir du site : http://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-juristendance

Formations intra-entreprise : 1e semestre 2015

LE CABINET A LA QUALITE D'ORGANISME DE FORMATION PROFESSIONNELLE DEPUIS 30 ANS.

Informatique et libertés	Dates
Informatique et libertés (niveau 1) : Identifier et qualifier les intervenants et les responsabilités, prévenir les risques et cerner les formalités obligatoires.	24-07 et 13-11-2015
Cil (niveau 1) : Permettre au Cil de maîtriser les obligations et responsabilités qui lui incombent et de savoir les mettre en œuvre.	14-01 et 02-04-2015
Informatique et libertés secteur bancaire : Sensibiliser les opérationnels sur les risques Informatique et libertés liés aux traitements du secteur bancaire.	20-01 et 04-03-2015
Informatique et libertés collectivités territoriales : Informer les collectivités territoriales sur les modalités d'application de la réglementation Informatique et libertés.	15-04 et 24-06-2015
Sécurité informatique et libertés : Connaître les exigences issues de la réglementation Informatique et libertés en matière de sécurité des données personnelles et sensibiliser aux risques liés à une faille de sécurité.	20-01 et 26-03-2015
Devenir Cil : Mettre en œuvre une politique de protection des données efficace (accountability, etc.) et résoudre les questions complexes (réseaux sociaux, etc.).	06-03 et 03-06-2015
Cil (niveau 2 expert) : Perfectionnement et résolution de questions complexes ; acquisition de méthodologie pour exercer l'activité selon l'approche Privacy by Design.	05-02 et 17-06-2015
Informatique et libertés gestion des ressources humaines : Donner aux membres de la direction des ressources humaines les clés pour utiliser les outils et les traitements de données personnelles mis en œuvre en matière de gestion des ressources humaines.	15-01 et 18-03-2015
Flux transfrontières de données : Présenter les dispositions qui régissent ces flux et élaborer une stratégie de gestion des flux conformément à la loi.	11-02 et 19-03-2015
Contrôles de la Cnil : Connaître l'étendue des pouvoirs de la Cnil et ses moyens de contrôle, apprendre à dialoguer avec la Cnil (notamment par le biais d'un jeu de rôle).	13-02 et 10-04-2015
Informatique et libertés secteur santé : Sensibiliser aux risques Informatique et libertés liés aux traitements du secteur santé et assurances et apporter des éléments de benchmark permettant de positionner son niveau de conformité.	27-01 et 25-03-2015
Informatique et libertés à l'attention du comité exécutif : Sensibiliser les membres du comité exécutif aux risques Informatique et libertés liés à leur activité.	Selon demande