Cyrille Boulogne

www.inovo-consulting.fr

DEP 2011-12-09

La protection des données personnelles

Une dimension incontournable

de la gouvernance des données

Pourquoi l'intégrer ?

Ne pas considérer la protection des données personnelles…

… expose les organisations à des risques économiques directs et indirects

Les risques sont-ils réels ?

Les sanctions financières de la CNIL

Peu fréquentes

- ✓ 5 sanctions en 2010
- ✓ 5 sanctions en 2009

Peu élevées

- ✓ CNIL *(Art.47 loi Informatique et Libertés)*
  - ✓ jusqu'à 150 000 euros
  - ✓ et 300 000 en cas de récidive
- ✓ En pénal *(Art. 226-16 à 226-24 du Code Pénal)*
  - ✓ jusqu'à 300 000 euros d'amende
  - ✓ et 5 ans de prison

Moyenne des condamnations :

- 15 000 euros

Condamnation maximale appliquée :

- 100 000 euros

Mais attention à l'impact des autres sanctions !

La mise en demeure

- ✓ Coût de mise en conformité
- ✓ Arrêt d'un traitement en exploitation
- ✓ Désorganisation opérationnelle
- ✓ Investissement à perte

La communication publique

- ✓ Reprise et amplification par les journalistes
- ✓ Dégradation de l'image
- ✓ Perte potentielle de clients

Avertissement public

- Pour enregistrement de données abusives
- Publication d'informations privées sans l'accord des personnes

Mise en demeure

- Contrôle d'accès biométrique non conforme
- Système de vidéosurveillance abusif

Les entreprises peuvent faire face à une perte de compétitivité

Difficulté à pénétrer un marché ou à capter des clients

- ✓ Mauvaise réputation lié au non respect de la vie privée
- ✓ Barrières règlementaires

Barrières règlementaires

- Agrément
- Niveau de sécurité requis pour le traitement des données sensibles

Les évolutions juridiques présentent aussi des risques

Pour l'exploitation

- ✓ de technologies
- ✓ de finalités

Elles peuvent avoir un impact

- ✓ Opérationnel
- ✓ Stratégique

Paquet télécoms

- Utilisation des cookies

Loi Kouchner

- Hébergement de données de santé

Adoption de normes

- Contrôles d'accès biométriques
- Géolocalisation

Jurisprudence sur le webcrawling

Qui est concerné ?

Toutes les organisations !

Au niveau opérationnel

- ✓ Gestion administrative et organisation du travail
- ✓ Outils de contrôle d'activité

Et au niveau stratégique

- ✓ Hébergeurs, télécoms
- ✓ Fournisseurs de données
- ✓ Services grand public sur internet
- ✓ Services de marketing direct
- ✓ Conseils TIC
- ✓ …


Les contrôles et sanctions …
… en croissance
avec les pouvoirs de la CNIL

L'évolution en quelque chiffres

(Source : Rapport 2010 et 2009 de la CNIL)

Plaintes

- ✓ 4821 en 2010 **(+13%** par rapport à 2009)
- ✓ 4265 en 2009 (+0,5% par rapport à 2008)
- ✓ 20% faites en ligne

Contrôles

- ✓ 308 en 2010 **(+14%)**
- ✓ 270 en 2009 (+23%)
- ✓ 19% suite à des plaintes

Mises en demeure

- ✓ 111 en 2010 **(+20,6%)**
- ✓ 92 en 2009 (-27%)
- ✓ 60% sont clôturées sans sanction

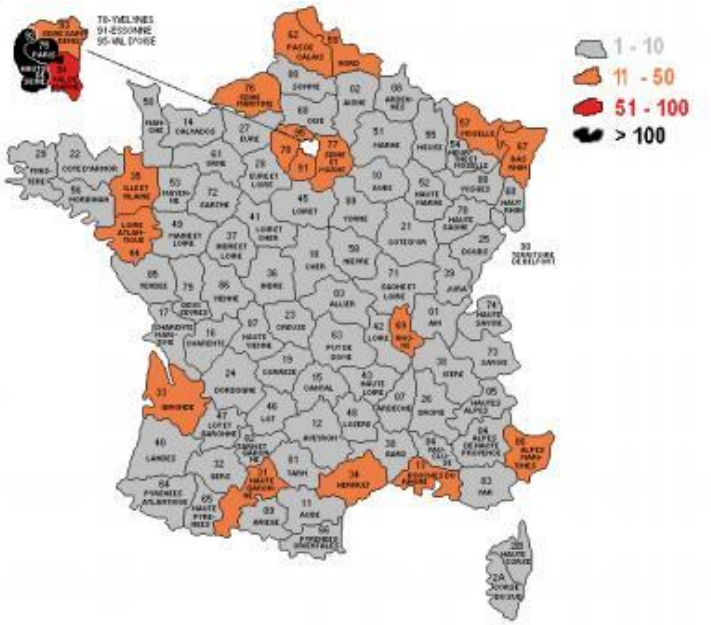
Sanctions

- ✓ 5 en 2010 (=)

Avertissements

- ✓ 4 en 2010 (=)

Répartition géographique des contrôles



Source : rapport CNIL 2010

➲ **Augmentation du nombre de plaintes, de contrôles et de mises en demeure**

Les secteurs contrôlés en 2010

Commerce
- ✓ 45%

Immobilier
- ✓ 11%

Education
- ✓ 8%

Santé
- ✓ 8%

Transports
- ✓ 6%

Industrie
- ✓ 5%

Police – justice
- ✓ 5%

Banques-assurances
- ✓ 4 %

Collectivités locales
- ✓ 3%

NTIC
- ✓ 3%

Associations
- ✓ <2%

Sport
- ✓ <2%

Le palmarès 2010 des traitements !

Ont fait l'objet du nombre de plaintes les plus fréquentes :

- ✓ Fichiers de crédit (FCIP)
- ✓ Outils de contrôle des salariés
- ✓ CRM, fichiers clients et prospection

Plaintes clients

- Données abusives
- Mise en place de listes noires
- Prospection non sollicités ou sans possibilité de désabonnement

Plaintes salariés

- Vidéosurveillance
- Contrôle des connexions Internet
- Contrôle du temps de travail
- Géolocalisation des véhicules

Quelles pratiques sont sanctionnés ?

Collecte déloyale

- ✓ Webcrawling
- ✓ Communication forcée pour accéder à un service

Traitement de données abusives

Non respect des droits

- ✓ Prospection non sollicitée
- ✓ Désabonnement non pris en compte
- ✓ Non respect des procédures d'information


Que dit la Loi I&L ?
Quelles données ?
Quelles obligations ?

Quels traitements sont concernés ?

L'Art.2 de la loi I&L dit :

« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, **directement ou indirectement**, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. »

Identification d'une personne

- Numéro de matricule,
- Numéro client,
- Adresse IP,
- Numéro de Tel,
- Adresse email,
- Numéro de sécurité sociale
- Gabarit de la main, empreinte digitale,
- Images ou photos
- Toute donnée dont il est le seul à en posséder les caractéristiques

Les obligations de la Loi I&L

Elles sont au nombre de 6

- ✓ Formalités
- ✓ Finalités
- ✓ Proportionnalité
- ✓ Durée de conservation
- ✓ Sécurité et confidentialité
- ✓ Respect des droits des personnes

Finalités :

Usage déterminé , explicite et légitime

Proportionnalité :

Seules les données pertinentes et nécessaires peuvent être enregistrées

Droits des personnes :

Information préalable, accès, modification ou opposition pour motif légitime (hors promotion)

Et les normes publiées par la CNIL

Normes simplifiées :

- ✓ Elles servent principalement à faciliter les formalités pour les traitements les plus courants

Autorisations uniques :

- ✓ Elles permettent l'exploitation d'un traitement sensible dans un cadre strict d'utilisation

Ex. de normes simplifiées :

- NS048 : Fichier clients / Prospects
- NS046 : Gestion administrative et organisation du travail
- NS047 : Gestion de la téléphonie
- NS042 : Gestion du temps de travail
- NS051 : géolocalisation des véhicules

Ex. d'autorisations uniques :

- AU013 : Pharmacovigilance
- AU014 : Prévention des impayés par chèque
- AU017 : Fichier des infractions
- AU007 / 008 / 019 / 027 : contrôle d'accès biométrique

Les traitements soumis à autorisation

En raison des données traitées

- ✓ Santé
- ✓ Infraction
- ✓ Opinion politique, religieuse, vie sexuelle …

En raison du traitement effectué

- ✓ Retrait d'un droit
- ✓ Transfert hors UE ou pays protégé

Mais la Loi I&L n'est pas la seule …

D'autres lois sont à considérer :

- ✓ Droit du travail
- ✓ Code de la santé : « Loi Kouchner »
- ✓ LCEN
- ✓ Code des postes et communications électroniques
- ✓ Loppsi 2

…

- Données de santé
- Données comptables
- Images de vidéosurveillance
- Système informatique et messagerie
- Données RH

Quelles sont les conséquences …

… pour la gouvernance des données ?

Le détournement de finalité par ignorance … ou intentionnellement

Lors de :

- ✓ Evolution d'un traitement ou création d'un service
- ✓ Projet de centralisation des données (MDM, datawarehouse)
- ✓ Transfert à un autre service, un partenaire ou sous-traitant

MDM ou datawarehouse
centralisent les données et les mettent à disposition pour des traitements pouvant ne pas répondre aux finalités pour lesquelles elles ont été collectées.

Enrichissement des bases de prospection
Téléphones ou emails collectés aux SAV / Service Réclamation utilisés à des fins de prospection

Extraction
Créées en marge, transférées puis réutilisées, les données n'ont plus leur finalité originelle

Une gourmandise d'informations « disproportionnées »

Informations obligatoires abusives en e-commerce

- ✓ Pour obtenir un service

Relation clients

- ✓ Commentaires abusifs ou listes noires

Recrutement

- ✓ Information non pertinente à l'évaluation des capacités d'un candidat
- ✓ Collecte d'information sur les réseaux sociaux

Utilisation du numéro de sécu abusif

Comme numéro de compte d'épargne salarial

Achat en ligne

Renseignement personnel sur le dirigeant obligatoire pour obtenir une facture.

Relation client

Commentaire en e-commerce « Client à surveiller ».

Le casse-tête de la conservation des données.

La tendance à tout conserver

- ✓ Web, moteurs de recherche, réseaux sociaux, base de connaissance, …

Le labyrinthe législatif

- ✓ Evolution des durées légales de conservation
- ✓ Différentes lois impliquées

Les sauvegardes et archivages

- ✓ Nettoyage des archives et sauvegardes par type de données selon leur durée

RH

- Problématique de conservation des données des salariés après leur départ
- Messagerie et données privées des salariés

Sécurité

- Suppression des images de vidéosurveillance en fonction de l'autorisation de la préfecture
- Suppression des données relatives aux accès après 3 mois

La sécurité et confidentialité presque parfaite … sauf que …

Elles s'arrêtent aux marges du système maitrisé par la DSI

- ✓ Transfert à des partenaires ou sous-traitants

Extractions ou bases annexes

- ✓ Budget, temps de développement non disponibles

Les procédures ne sont pas toujours respectées

- ✓ Urgence sur un projet marketing et transfert de fichier sans garantie

RH

Sauvegarde pdf des feuilles de paye

ERP ou CRM

Ne remplissent pas toutes les fonctionnalités et ne permettent pas de traiter certaines données, extraction par les utilisateurs

Art de la collecte déloyale et entrave à l'exercice du droit

Données collectées à l'insu des personnes

- ✓ Webcrawling ou aspirateur Internet
- ✓ Formulaire de collecte et utilisation des données à des fins non indiquées
- ✓ Intégration d'un fichier externe sans accord des personnes

Droit d'accès pas toujours évident à appliquer

Webcrawling :
Collecte de données sur des sites tiers (ex. annuaires, réseaux sociaux), sans l'accord de l'utilisateur

Formulaire :
Test d'un service en ligne et réutilisation à des fins de prospections sans information ou accord du clients

Fichier prospects :
Commercial qui récupère le fichier d'un ancien « collègue ou ami».

Sans formalité, pas d'utilisation, pas de transfert

Formalités obligatoires pour

- ✓ Tout traitement sauf dispense

Transfert sans autorisation pour

- ✓ Pays de l'UE,
- ✓ Pays protégés
- ✓ Société américaine adhérente au Safe Harbor

Sinon autorisation avec

- ✓ Clauses contractuelles garantissant la sécurité, la confidentialité, le droit à l'oubli et les droits des personnes
- ✓ Binding Corporate Rules pour les filiales

Dispenses : Comptabilité, paie, fichiers fournisseurs

Pays protégés :

Islande, Lichtenstein, Norvège, Suisse, Argentine, Canada, Guernesey, Isle de Man, Jersey

Safe Harbor : Programme d'auto-certification pour assurer la protection des données personnelles, défini en collaboration entre le Département du Commerce Américain et la Commission Européenne

Le respect de ces obligations n'est pas une problématique ponctuelle

Il doit s'inscrire dans le temps à cause :

- ✓ Des évolutions règlementaires
- ✓ De l'intégration de nouveaux traitements et technologies
- ✓ De la durée de conservation des données
- ✓ Des dérives organisationnelles

La protection des données personnelles est un sujet transversal

Qui impacte

- ✓ La nature et les conditions d'exploitation des données, les traitements ou services
- ✓ Les moyens de mise en œuvre de la sécurité et de la confidentialité
- ✓ Les procédures de conservation, stockage, sauvegarde, archivage, et nettoyage des données

Et implique

- ✓ La direction
- ✓ La DSI
- ✓ Le service juridique
- ✓ Les opérationnels (RH, marketing …)

La solution ne peut être ni locale, ni ponctuelle

Elle doit s'intégrer

- ✓ Dans tout lancement de projet traitant des données personnelles
- ✓ Dans un programme ou une politique de respect des obligations légales et de la vie privée

Une place naturelle dans la gouvernance des données

Aussi bien au niveau stratégique qu'au niveau opérationnel

Comment l'intégrer ?

Quels sont les moyens ?

Le Correspondant Informatique et Libertés (CIL) comme vecteur principal

Création de la fonction

- ✓ En 2004

Ses objectifs

- ✓ Veiller au respect de la loi Informatique et Libertés
- ✓ Sensibiliser les responsables de traitements et les utilisateurs quant à la protection des données personnelles

Les missions officielles du CIL

Définies par la CNIL

- ✓ Veiller au respect de la loi I&L
- ✓ Informer les responsables de traitements en cas de manquement
- ✓ Tenir à jour un registre des traitements
- ✓ Réaliser un bilan annuel pour la direction
- ✓ Répondre aux réclamations et aux demandes des clients ou salariés

Registre des traitements :

Document recensant les traitements actifs au sein de l'entreprise, leur finalité, le type de données traitées, leurs destinataires, les modalités de droit d'accès

Bilan annuel :

Rapport rappelant l'ensemble des actions menées sur les traitements des données personnelles, les manquements constatés et les solutions apportées, ainsi que les projets prévus pour l'année suivante

Le CIL, un gage de qualité

Les principaux avantages

- ✓ Désignation officielle d'une personne chargée de la mise en conformité réglementaire des traitements
- ✓ Centralisation de l'information sur les données personnelles
- ✓ Garantie de la conformité des déploiements des nouveaux traitements
- ✓ Prise en compte des évolutions juridiques sur le long terme

Et surtout

- ✓ Amélioration de l'image grâce à la démonstration d'une réelle volonté à respecter les données personnelles

Mais contrairement aux idées reçues

- ✓ Pas d'allègement des formalités

La participation CIL dans la gouvernance

Son apport est essentiel pour :

- ✓ Valider la conformité des projets
- ✓ Valider les transferts ou flux de données
- ✓ Définir les durées de conservation
- ✓ Cartographier, cataloguer les données et leur sensibilité
- ✓ Participer à la définition des politiques de confidentialité, stockage, transfert
- ✓ S'assurer de la signature de clauses de confidentialité avec les partenaires, prestataires, fournisseurs
- ✓ Participer à l'élaboration de la charte informatique
- ✓ Assurer une veille règlementaire

Le CIL est aussi opérationnel

Son action comprend

- ✓ Gestion de l'application des droits des personnes
- ✓ Validation des conditions de transferts ponctuels de données
- ✓ Contrôle des « zones commentaires »
- ✓ Contrôle du nettoyage des données
- ✓ Contrôle de la gestion des droits d'accès et de la confidentialité

Le CIL, un mouton à 5 pattes

Pour couvrir l'ensemble de sa mission, il doit avoir une culture

- ✓ Juridique
- ✓ TIC
- ✓ Audit/Qualité/Organisation

Quelque soit son profil d'origine, il devra travailler avec un partenaire complémentaire.

Rester neutre s'impose !

Il ne doit pas faire partie d'un service impliqué dans les traitements

Il est de préférence rattaché à :

- ✓ Cellule de gouvernance
- ✓ Service juridique
- ✓ Service qualité

Un spectre d'intervention adapté au fonctionnement

Son champ d'action dépend de la taille et de la structure de l'organisation

- ✓ Un CIL pour chaque société d'un groupe
- ✓ Mutualisé au sein d'un groupe (nécessite des relais)
- ✓ Un CIL par Business Unit
- ✓ Un CIL par domaine d'activité

Les outils et moyens mis à disposition du CIL

Moyens techniques pour mener à bien sa mission de CIL

- ✓ Une cartographie des flux de données
- ✓ Un outil pour créer et alimenter le registre des traitements

Implémentation dans les systèmes

- ✓ La traçabilité des données personnelles dans les MDM et datawarehouses
- ✓ Outils d'analyses de données avec alertes sur les champs commentaire

Cartographie

Avoir une vision globale de tous les traitements, des échanges de données, de leur réutilisation

Traçabilité / registre

Origine, Finalités, Accord, Destinataire

Communication

Sensibiliser et former les salariés à la protection des données personnelles

Quelles perspectives ?

Evolutions juridiques et technologiques

Les orientations de l'Assemblée Nationale sur les droits de l'individu

Une mission d'information a proposé en juin 2011 :

- ✓ de soumettre les systèmes de géolocalisation à l'autorisation de la CNIL,
- ✓ de clarifier le statut juridique de l'adresse IP,
- ✓ d'instaurer un droit à l'oubli sur les réseaux sociaux,
- ✓ d'exclure du cloud computing réalisé hors de l'Union européenne les données personnelles dites "sensibles"…

Les autres sujets d'actualité

L'opt-in pour tous les canaux de prospection ?

Le CIL obligatoire pour les entreprises de plus de 50 salariés ?

La traçabilité exigée des données personnelles ?

La création d'un label de respect de la vie privée pour les entreprises ?

La règlementation des technologies en croissance ou développement ?

- ✓ Biométrique
- ✓ Nano
- ✓ RFID, NFC

Pour résumer …

Risques sont réels

- ✓ Coût financier indirect potentiellement élevé
- ✓ Plaintes et contrôles sont en croissance
- ✓ A prendre particulièrement en considération dans les secteurs où elle est stratégique
- ✓ La veille règlementaire y est essentielle

Le points sensibles

- ✓ Détournements de finalité
- ✓ La collecte déloyale
- ✓ Les données abusives
- ✓ Les durées de conservation

Les moyens pour y répondre

- ✓ Désignation d'un CIL intégré dans la cellule de gouvernance des données
- ✓ Traçabilité des données personnelles
- ✓ Contrôle des données « abusives » potentielles
- ✓ Contractualisation de tout transfert de données


Merci pour votre attention …
C’est à vous …