Données de santé : Gestion des risques juridico-technologiques ?

Yaël COHEN-HADRIA
Avocate – Cabinet HAAS
Directrice du Pôle Données personnelles et vie privée

PLAN

Introduction : MESURE DU RISQUE

Le référentiel légal et technologique

Partie 1 : RISQUE TECHNOLOGIQUE

La dématérialisation des données de santé

Partie 2 : RISQUE JURIDIQUE

Les responsabilités et enjeux associés aux données de santé

Partie 3 : DISCUSSION DES ENJEUX DE L'OPEN DATA

Les enjeux associés à l'ouverture de l'accès aux données de santé

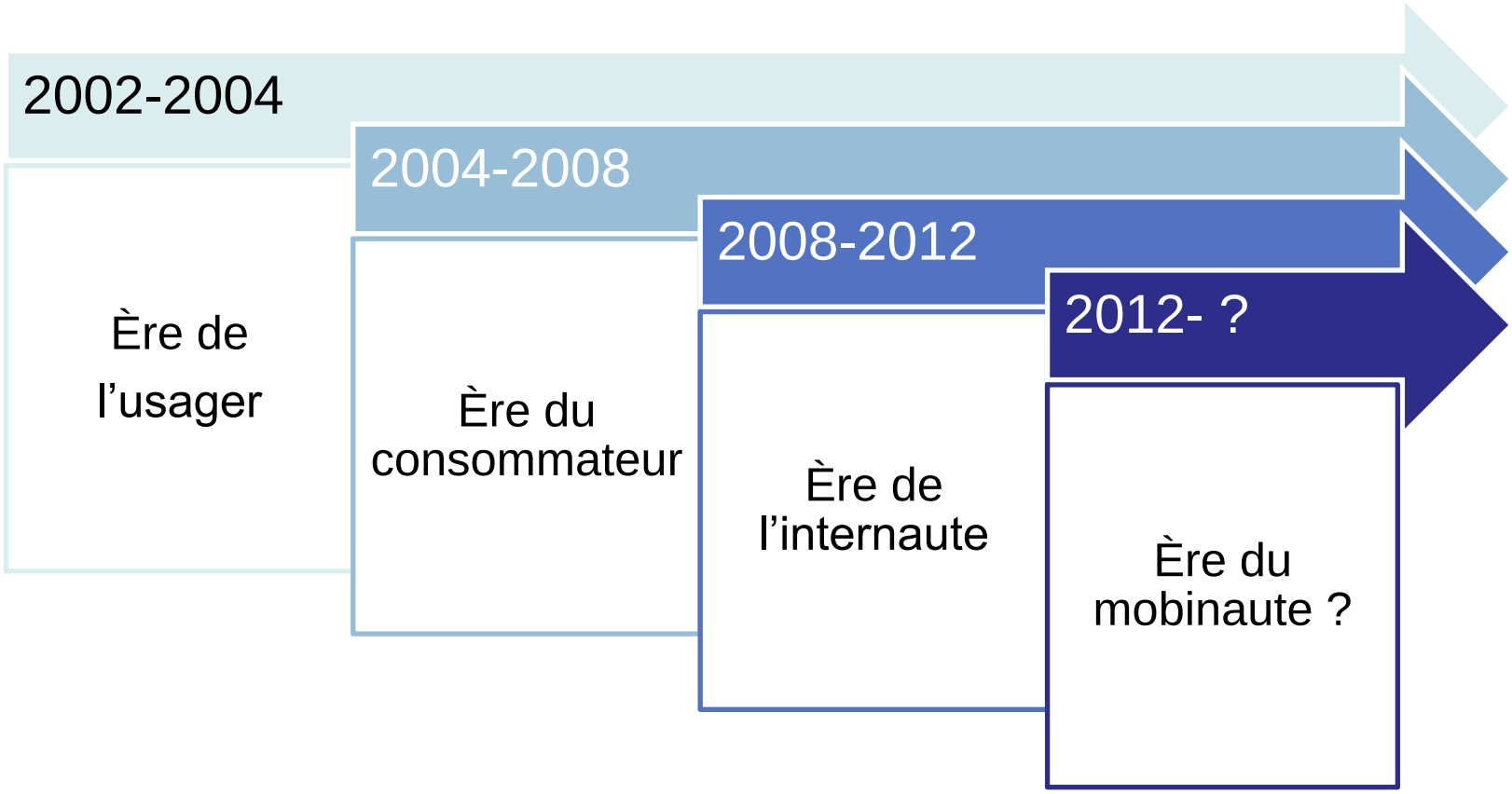
Introduction : MESURE DU RISQUE

Le référentiel légal des données de santé

- Loi n°78-17 du 6 janvier 1978 (article 8 et chapitres IX et X) dite loi « Informatique et libertés »
- Code pénal (articles 226-19 et 226-19-1)
- Code de la recherche (articles 225-1 et 225-2)
- Code de la santé publique (notamment le chapitre Ier du titre 1 de la première partie sur l'information des usagers du système de santé et expression de leur volonté)
- Code plus spécifiques tels que le Code de l'éducation, du sport ou le Code rural et de la pêche maritime

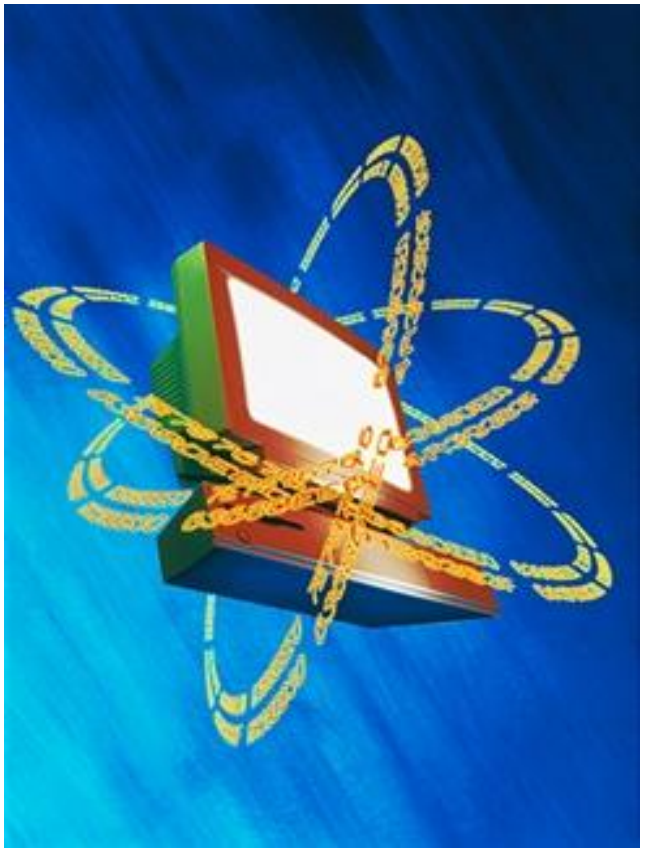
Introduction : MESURE DU RISQUE

Le référentiel technologique



PARTIE 1 : RISQUE TECHNOLOGIQUE

I. CONTEXTE
II. ANALYSE DU RISQUE
III. MESURE DU RISQUE
IV. MOYENS DE LIMITER LE RISQUE



Partie 1 : RISQUE TECHNOLOGIQUE
Contexte

- **Modernisation du système de santé**
  - développement des technologies et à la dématérialisation des données dans un objectif certain : facteur de progrès, de qualité et d'efficacité !
- **Collaboration entre professionnels de la santé**
  - interopérabilité accrue entre les divers systèmes d'informations des centres de santé, des professionnels libéraux dits de ville et l'équipe de soin…mais également avec des professions non médicales dans l'intérêt du patient

Partie 1 : RISQUE TECHNOLOGIQUE

Analyse des risques liés à la techno

Vidéosurveillance / géolocalisation dans les établissements hospitaliers

Les bracelets électroniques d'alarme

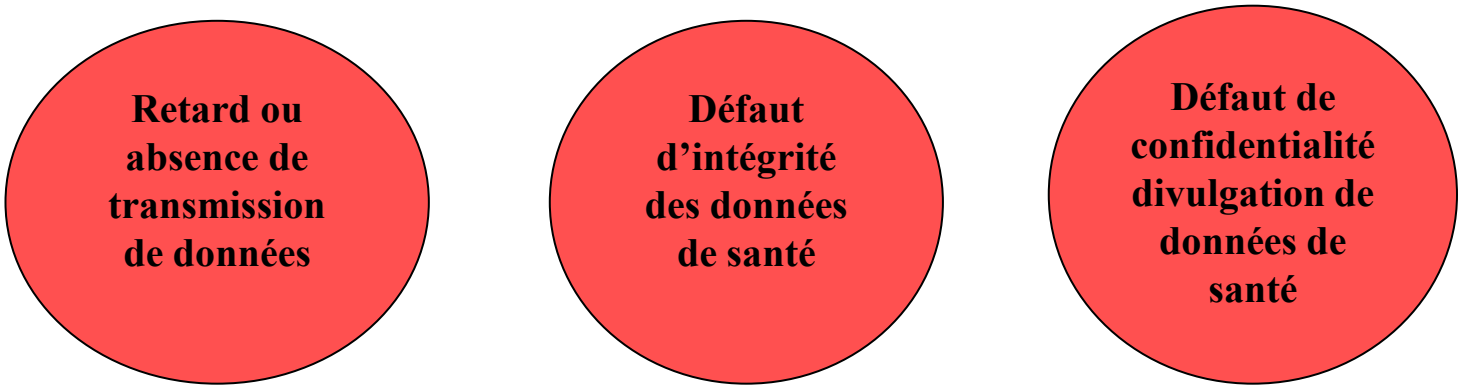
Les systèmes de monitoring à distance par Internet

Télémédecine

Partie 1 : RISQUE TECHNOLOGIQUE

Analyse des risques liés à la transmission

Risques pouvant entrainer des erreurs de diagnostics, des retards d'interventions chirurgicales ou des erreurs médicales :



MENACES : « *l'attaque logique de l'équipement, notamment par exploitation de vulnérabilités de ses logiciels ; l'introduction ou l'activation de codes malveillants dans l'équipement ; la perturbation de fonctionnement de l'équipement à partir du SIS ou de son réseau ; la capture ou la modification de données sur la liaison entre l'équipement et le SIS ; l'accès illicite à l'équipement, et l'introduction ou l'extraction de ses données ; le mésusage de l'équipement par une personne autorisée ; la modification non autorisée des logiciels de l'équipement*. » (ASIP SANTE)

contact@haas-avocats.com

Partie 1 : RISQUE TECHNOLOGIQUE
Mesure du risque

- Selon un article publié par la Mutualité française le 20 Mars 2013, la CNIL a reçu **51 plaintes de la part de patients et d'établissements de santé**, victimes de divulgation d'informations médicales sur Internet.

- Selon le même article, à Marseille, les données d'une étude de médecins travaillant sur des bébés prématurés ont été rendues accessibles à la population car elles avaient été stockées chez un **hébergeur non agréé par le Ministère de la Santé**

Partie 1 : RISQUE TECHNOLOGIQUE
Mesure du risque

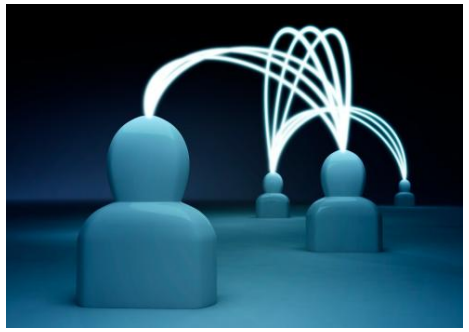
Taper son nom sur Google et voir apparaître son dossier médical ? C'est possible !

- des données issues de l'hôpital Foch de Suresnes ou encore du Pôle de santé du Plateau, qui regroupe les cliniques des Hauts-de-Seine, se sont retrouvées sur Internet, à cause d'une erreur d'un hébergeur non agréé
- déjà en Juin 2012, 375 dossiers d'une clinique de Troyes avaient été indexés sur Google.

Partie 1 : RISQUE TECHNOLOGIQUE
Solutions pour limiter les risques

Un plan de progrès doit être mis en place pour AGIR SUR:

- la structure et l'organisation du responsable de traitement des données
- les données de santé collectées et leur support de collecte et de conservation
- les modalités de transmission et d'accès aux données
- les sources extérieures de risques
- Les impactes et conséquences de la prise de risque



Partie 1 : RISQUE TECHNOLOGIQUE
Solutions pour limiter les risques

Des **règles strictes de communication** sont nécessaires au niveau :

- des structures de soins (dossiers informatisés, hospitalisation à domicile) ;
- des relations entre les structures et les acteurs de la santé (télémédecine, concertation pluridisciplinaire) ;
- de la coordination des soins (DMP, RPPS) ;
- de la recherche et de la santé publique (essais cliniques, pharmacovigilance…etc.).

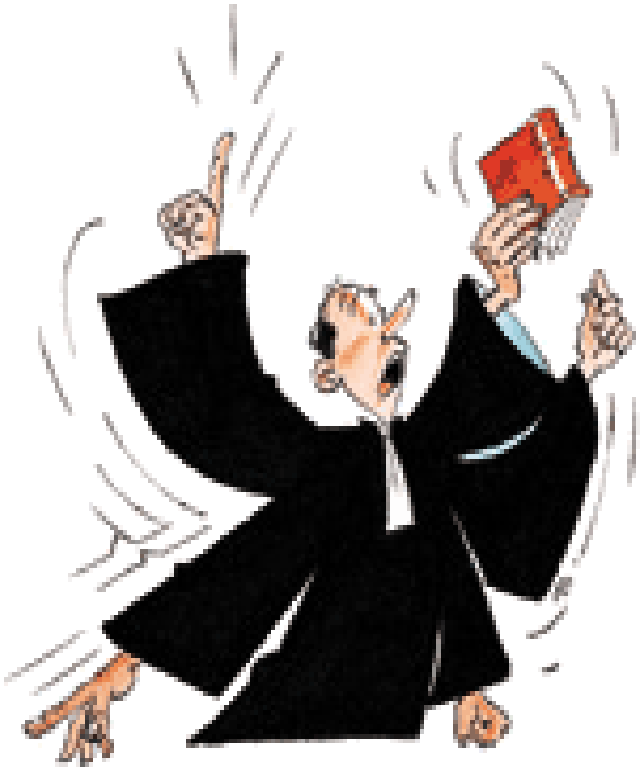
Partie 1 : RISQUE TECHNOLOGIQUE
Solutions pour limiter les risques

Définir des règles d'accès aux données dans le SIS:

- Règles d'or pour la gestion des habilitations
- Modèle d'habilitation
- Organisation et processus de gestion des habilitations
- Processus de contrôle

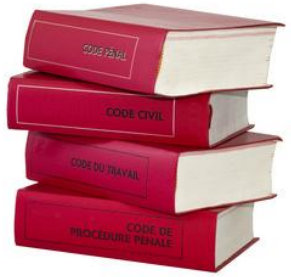
PARTIE 2 : RISQUE JURIDIQUE

I. CONTEXTE
II. ANALYSE DU RISQUE
III. MESURE DU RISQUE
IV. MOYENS DE LIMITER LE RISQUE



Partie 2 : RISQUE JURIDIQUE
Contexte

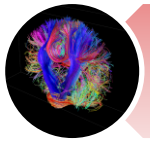
Accès à des données de santé par les professionnels de ce secteur ou non = régime de responsabilité spécifique à sa situation (responsable de traitement, personne habilitée à accéder au traitement, sous-traitant…etc.)



Bloc d'obligations légales et règlementaires en rapide évolution (Loi Informatique et Libertés de 1978, Code de la santé publique, référentiels techniques de la PGSSI-S…etc.).

Partie 2 : RISQUE JURIDIQUE
Contexte - Les données sensibles

Les données biométriques



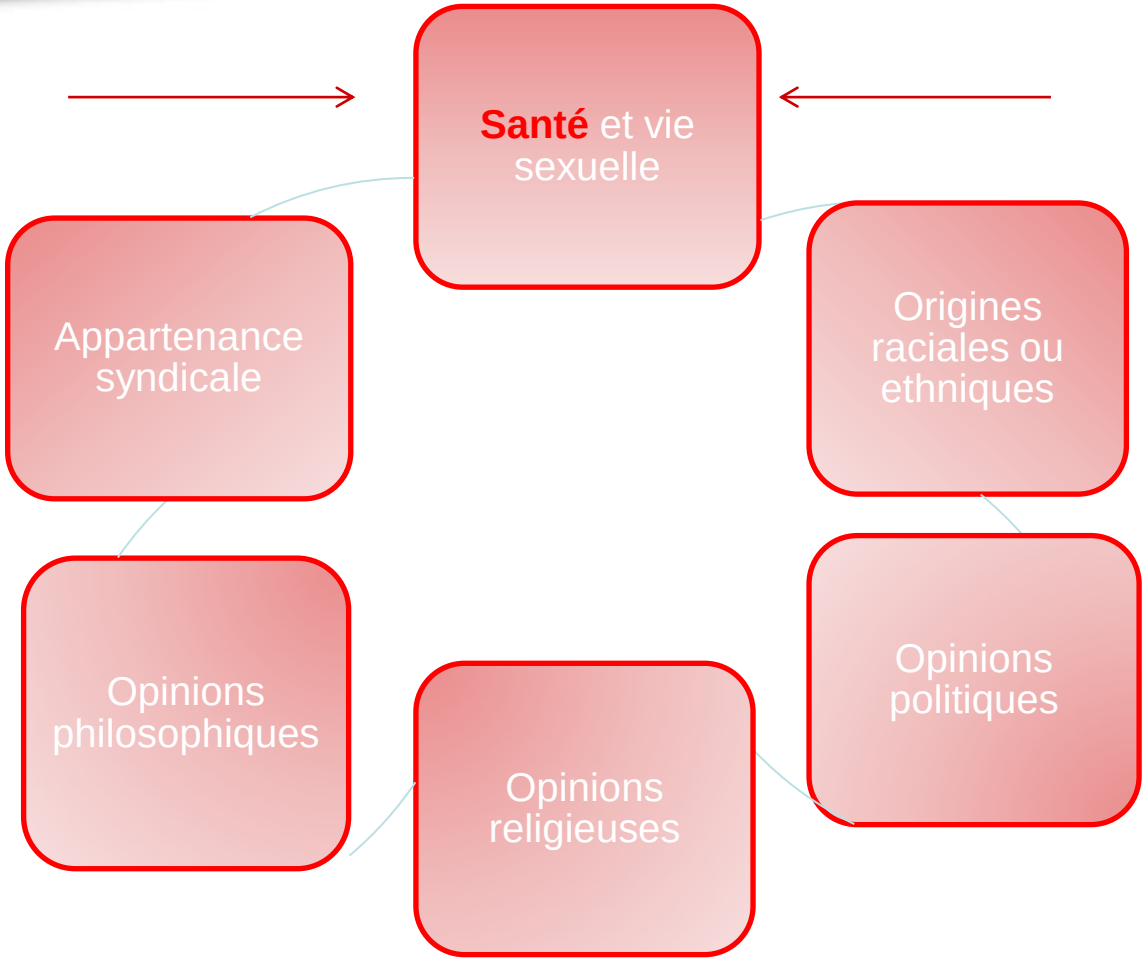
Les données génétiques

Les infractions, condamnations et mesures de sureté

Le numéro de sécurité sociale

Les difficultés sociales

Partie 2 : RISQUE JURIDIQUE
Contexte - Les données interdites



Partie 2 : RISQUE JURIDIQUE
Contexte - Les données interdites

Principe : Article 8-I de la loi I&L

Interdiction de collecter les données

Conditions strictes de licéité de leur traitement

Exception: Article 8-II de la loi I&L

Partie 2 : RISQUE JURIDIQUE

Analyse du risque : principales autorités de contrôle

La CNIL

- a augmenté son nombre de contrôle dans le domaine de la santé ;

- Exemple : mise en demeure d'un centre hospitalier de St Malo fin 2013 pour remédier à des failles de sécurité et confidentialité.

La HAS

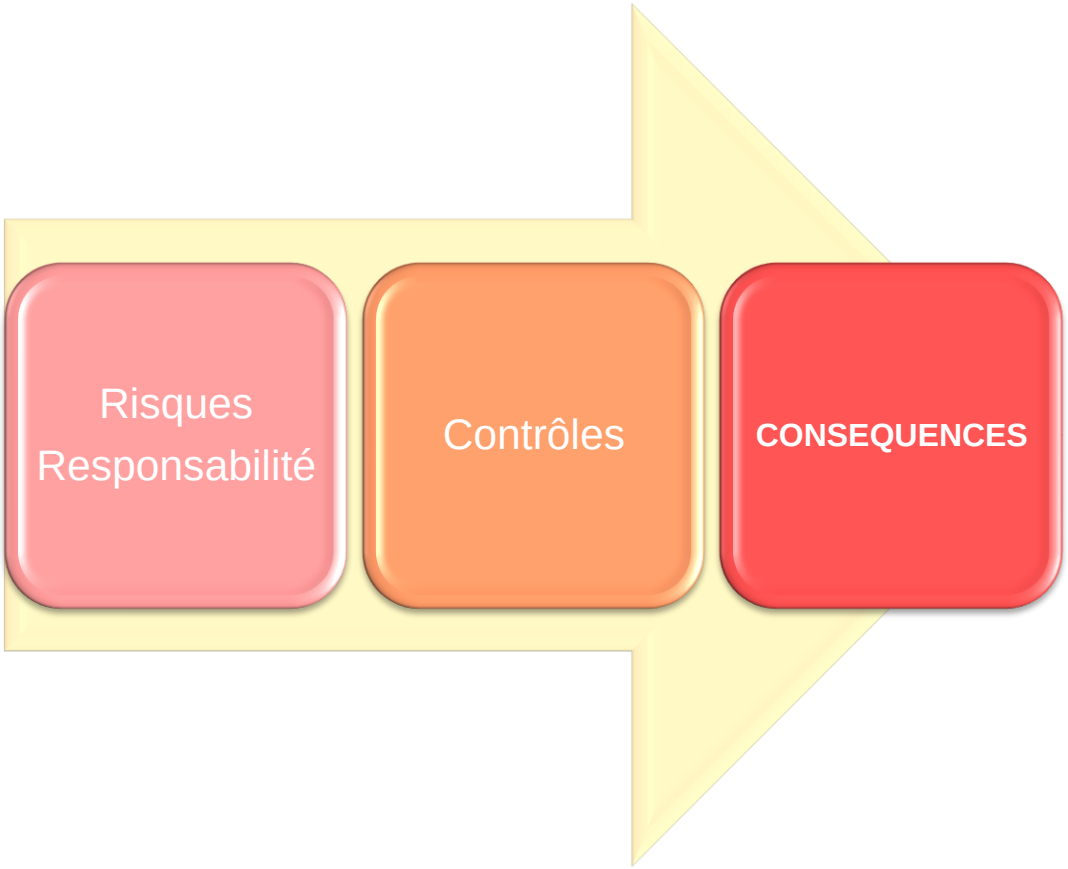
- délivre des accréditations aux établissements de santé;

- délivre des certifications aux établissements de santé.

- contrôle et peut retirer ces accréditations et certifications.

Partie 2 : RISQUE JURIDIQUE

Mesure du risque



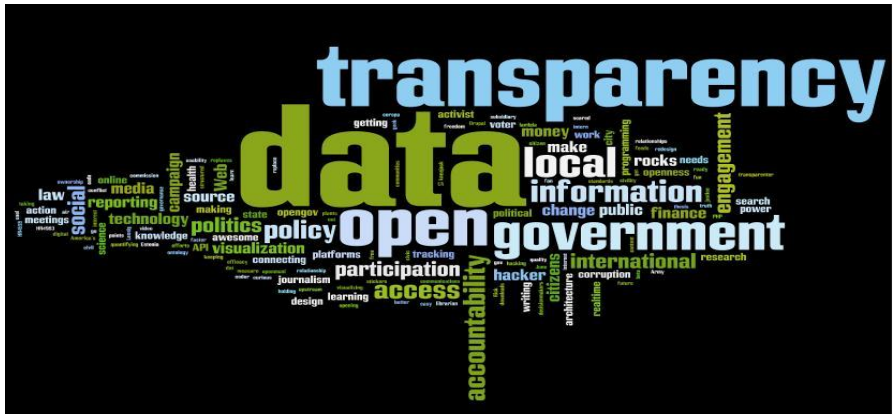
- **responsabilité pénale** (article 226-16 du Code pénal punit de 1.5 millions d'euros et 5 ans d'emprisonnement pour non respect de la loi Informatique et Libertés) ;
- **impact médiatique néfaste** pour l'établissement contrôlé et sanctionné ;
- **Création de nouveaux enjeux économiques** (intensification des négociations pour les contrats de sous-traitance, d'hébergement…etc.).

Partie 2 : RISQUE JURIDIQUE
Solutions pour limiter les risques

- Auditer son SI pour relever les failles et estimer le niveau de manquement
- Mettre en place un plan d'actions adapté, en fonction du degrés de risque acceptable et souhaité par la direction
- Adopter une charte Informatique ou la mettre à jour
- Constituer un Comité de Gestion du risque afin d'étudier l'opportunité de mettre en place les outils juridiques tels que le Guide des opérations de contrôles ou la PSSI. Le cas échéant préparer et adopter ces documents
- Prévoir des contrôles de maintien en conformité

PARTIE 3 : OUVERTURE SUR L'OPEN DATA

I. CONTEXTE
II. DISCUSSION



PARTIE 3 : OPEN DATA
Référentiel légal

- L'ouverture des données publiques est fondée sur la loi n° 78-753 du 17 juillet 1978 relative au droit d'accès aux documents administratifs, ainsi définis :
- « quels que soient leur date, leur lieu de conservation, leur forme et leur support, les documents produits ou reçus, dans le cadre de leur mission de service public, par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission.

  Constituent de tels documents notamment les dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, directives, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions et décisions. (…) » (*article 1er*).

PARTIE 3 : OPEN DATA
Définition

- OPEN DATA concerne les « données publiques »
- OPEN DATA = C'est la mise à disposition des internautes d'informations détenues par le secteur public
- Article 1 de la loi CADA du 17 juillet 1978 :
  - Une donnée recueillie « dans le cadre de leur mission de service public, par l'État, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission »
- Exemple : statistiques, cartographiques, horaires, données économiques, sociales, touristiques ou encore financières sur le territoire

PARTIE 3 : DISCUSSION

Possibilité d'anticiper les épidémies, de créer des remèdes, de séquencer l'ADN….

Nouvelles technologies et partage des informations de santé apportent des bienfaits

A VOUS DE JOUER

Avez-vous des observations/ des questions ?

HAAS SOCIETE D'AVOCATS

Tel : 01 56 43 68 80

Fax : 01.40.75.01.96

Email : contact@haas-avocats.com

87 BD DE COURCELLES
75008 PARIS

Métro Ternes