Privacy Impact Assessment

Etude d'Impact de Vie Privée

La méthode CNIL

Benjamin NGUYEN

D'après D. Le Métayer (Inria) & CNIL

Objectif du cours

- Pourquoi un PIA ?
- Présentation de la méthode CNIL
- Exemples
- Exercices

POURQUOI UN PIA ?

Une contrainte légale …

- Le PIA est défini dans le RGPD, article 35.
- L'article 24 définit la notion de responsabilité du responsable de traitement, en intégrant la question du risque à l'analyse :

  Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement.

La question du risque dans le RGPD

- Article 32 – Sécurité du traitement
- Article 33 – Notification à l'autorité de contrôle d'une violation de données à caractère personnel
- Article 34 – Notification à la personne concernée d'une violation de données à caractère personnel
- Article 36 – Consultation préalable

Article 35 du RGPD

« Analyse d'impact relative à la protection des données »

1- Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, **est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques**, le responsable du traitement effectue, avant le traitement, une **analyse de l'impact des opérations de traitement envisagées** sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

Analyse de risque vs. règle de droit

- Régulation par la règle de droit (« right-based regulation »):
  - Prescriptive: mesure obligatoires
  - Déterministe: conformité facile à vérifier
- Régulation par la gestion de risques (« risk-based regulation ») :
  - Non prescriptive: des objectifs plus que des mesures (niveau de risque toléré, etc.)
  - Probabiliste: objectif de réduction plus que d'élimination des risques

La gestion des risques

Avantages

- **Grande variété de situations** ⇒besoin de flexibilité :

  la régulation par la règle est souvent trop rigide et ne conduit pas forcément à la meilleure protection
- **Les risques ne peuvent pas être complètement éliminés** ⇒besoin d'une démarche rationnelle pour les analyser et prendre les décisions appropriées

  priorités d'actions, calibration des mesures, allocation optimale des ressources en fonction des risques identifiés

Critiques

- Risque de réduire un droit fondamental en un simple paramètre dans un processus d'optimisation des coûts

  ⇒ *démarche pouvant se réduire à un outil de gestion dépourvu de toute substance*
- Démarche pouvant conduire à un exercice d'auto-justification

Position du groupe Article 29

- L'analyse de risque ne doit jamais conduire à un affaiblissement du droit des personnes: les droits du sujet doivent être respectés quel que soit le niveau de risque (information, consentement, droit d'accès, de rectification, d'effacement, etc.)
- On doit considérer non seulement les risques pour les individus mais aussi les impacts sur la société

Historique des PIA

- Précurseurs: organismes d'évaluation des technologies (technologyassessment, OTA) et études d'impact environnemental (EIS) dans les années 70
- Dans le domaine de la protection de la vie privée: Canada (1999), Nouvelle Zélande (2002), Australie (2006), Royaume-Uni (2007), Union Européenne (2011: RFID, 2014: smart grids)
- Guides: ICO (2011), BSI (2011), NIST (2015), **CNIL (2015)**

Quelques conseils …

- Initier le PIA le plus tôt possible
- Ne pas réduire l'objectif à la production d'un rapport : le PIA doit faire partie d'un processus global de gestion des risques
- Impliquer toutes les parties prenantes
- Eviter les conflits d'intérêt ou les soupçons de green washing : un PIA doit être réalisé et/ou audité par un tiers indépendant, publié et approuvé par un responsable de haut niveau

Principaux défis de l'analyse de risques

- Complétude: ne pas oublier de facteurs de risques majeurs

  Définition de typologies
- Validité des hypothèses: ne pas sous-estimer certains risques

  Définition d'attributs et d'échelles de valeurs
- Combinaison d'aspects techniques et non techniques (juridiques, sociaux)

  Séparation claire. Origine des sources pour la partie non technique, mode de calcul rigoureux pour la partie technique, traçabilité du processus
- Evolution du contexte (techniques, usages, etc.)

L’approche CNIL

Composée de 3 documents et d’un logiciel (PIA)

1. La méthode
2. Les modèles
3. Les bases de connaissances

La méthode

1. Délimiter et décrire le **contexte** du(des) traitement(s) considéré(s)

   traitement, périmètre, finalités, données personnelles, durée de conservation, supports, etc.

2. Analyser les **mesures** garantissant le respect des principes fondamentaux : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées

   juridiques, organisationnelles, sécurité logique, sécurité physique

3. Apprécier les **risques** sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités

   sources de risques, événements redoutés, menaces, risques (gravité et vraisemblance)

4. Formaliser la **validation** du PIA au regard des éléments précédents ou bien décider de réviser les étapes précédentes.

   PIA acceptable → plan d'action et validation formelle

   PIA non acceptable → objectifs et itération ou rejet.

Principaux composants

- Définition du contexte
  - Système
  - Données personnelles en jeu
  - Parties prenantes
- Définition des risques
  - Sources de risque
    - Peut être le responsable de traitement lui-même
  - Faiblesses du système
    - Peut être la fonctionnalité elle-même
  - Evénements redoutés
  - Impacts sur la vie privée

Distinction entre les évènements techniques et les impacts sur la personne

Principaux composants

- Définition du contexte
  - Système
  - Données personnelles en jeu
  - Parties prenantes
- Définition des risques
  - Sources de risque
  - Faiblesses du système
  - Evénements redoutés
  - Impacts sur la vie privée

Analyse :

- Vraisemblance des impacts
- Gravité des impacts

Attributs des données personnelles

- Sensibilité (statut juridique)
- Niveau de précision (granularité)
- Volume (nombre de données)
- Format (chiffrement, bruitage, etc.)
- Finalité
- Durée de conservation
- Contrôle (qui peut accéder aux données)

Catégories de sources de risque

- Sources de risques liées au responsable de traitement :
  - responsable de traitement, sous-traitants, employés, clients, etc.
- Sources de risques liées au sujet :
  - famille, amis, collègues, fournisseurs de service, etc.
- Sources de risques liées aux états :
  - police, justice, agences de renseignement, etc.
- Sources de risques génériques :
  - hackers, escrocs, publicitaires, etc.

Attributs des sources de risque

- Capacités:
  - Droits d'accès
  - Informations auxiliaires
  - Ressources techniques (matériel, outils, expertise, etc.)
- Déterminants (par événement redouté):
  - Positifs: motivation, facteurs d'incitation (atteintes délibérées), manque de sensibilisation (atteintes accidentelles)
  - Négatifs: facteurs de dissuasion, sensibilisation aux exigences de protection de la vie privée

Catégories d’évènements redoutés

1. Collecte excessive de données (violation de principe de minimisation)
2. Usage excessif de données (violation de principe de finalité)
3. Divulgation de données à un tiers (violation des engagements affichés ou de la finalité)
4. Non-respect des obligations du responsable de traitement (effacement, droits d’accès, droit de correction, etc.)
5. Modification ou destruction intempestive de données (atteinte à l’intégrité ou à la disponibilité des données)

Attributs des évènements redoutés

Ensemble des scenarios conduisant à l'événement redouté avec leurs:

- **Faisabilité :** dérivée des capacités des sources de risques et des faiblesses du système
- **Vraisemblance :** dérivée de la faisabilité de l'événement redouté et des déterminants des sources de risques
- **Impacts sur la vie privée**

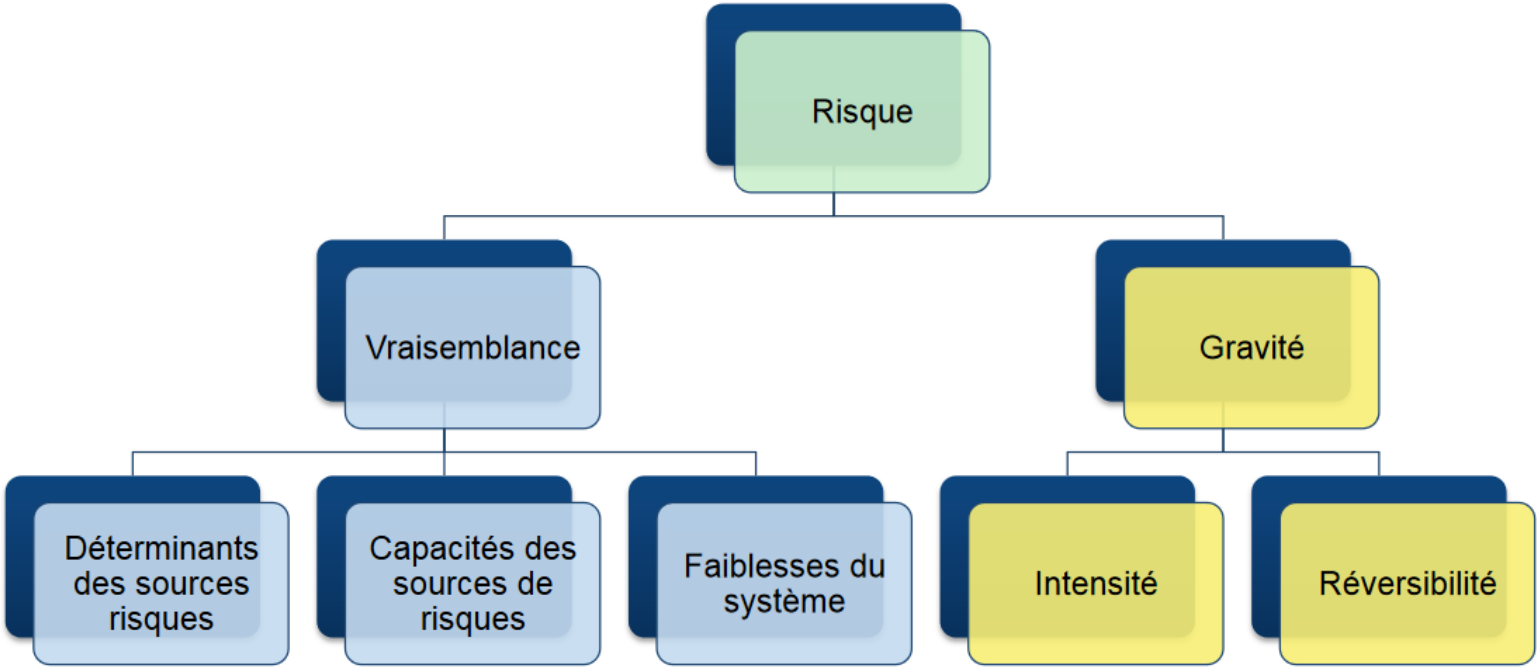
Catégories d'impact sur la vie privée

1. Impacts physiques : des désagréments mineurs jusqu'aux maladies ou la mort
2. Impacts psychologiques : impression d'intrusion, de perte d'intimité, difficultés relationnelles, dépression, maladie de long terme, etc.
3. Impacts matériels : perte de temps, d'argent, d'opportunités, de travail, de logement, etc.

Attributs sur les impacts sur la vie privée

1. **Vraisemblance:** fonction de la vraisemblance des événements redoutés produisant l'impact
2. **Gravité:** fonction de l'intensité des conséquences et de la capacité des personnes à les surmonter

Risques d’impact sur la vie privée



Evaluation des attributs

- Gravité :
  - utilisation de modèles existants (par exemple échelle de gravités proposée par la CNIL)
  - Idéalement: après consultation des parties prenantes
- Vraisemblance:
  - Evaluation quantitative (rigueur) et/ou qualitative (compréhension): tables de correspondance
  - Arbres d'impact (privacy harm trees) (cf Le Métayer)

LES BASES DE CONNAISSANCES CNIL

Bases de connaissances : Organisation

- Organisation (avoir un DPO)
- Politique (gestion des règles)
- Sous-traitance : identifiée et contractualisée
- Transferts hors UE
- Relations avec les tiers

Bases de connaissances : Préalables

- Formalités préalables
- Finalités : déterminées, explicites et légitimes
- Fondement : licéité du traitement, interdiction du détournement de finalité

Bases de connaissances : Droits des utilisateurs

- Recueil du consentement
- Droit de limitation du traitement et opposition
- Droit de rectification et d'effacement
- Droit d'accès et portabilité
- Gestion des incidents et des violations de données
- Information des personnes concernées (traitement loyal et transparent)

Bases de connaissances : Sûreté et qualité des données

- Sauvegardes
- Archivage
- Contrôle d’intégrité
- Qualité des données : exactes et tenues à jour

Bases de connaissances : Sécurité des données

- Anonymisation
- Chiffrement
- Cloisonnement des données
- Contrôle d’accès physique
- Contrôle d’accès logique
- Durées de conservation limitées
- Minimisation des données : adéquates, pertinentes et limitées

Bases de connaissances : Sécurité des systèmes

- Gestion des postes de travail
- Lutte contre les logiciels malveillants
- Maintenance
- Sécurité de l'exploitation (PRA)
- Sécurité des canaux informatiques (réseaux)
- Sécurité des matériels
- Sécurité des sites web

Bases de connaissances : Audits

- Supervision (audits)
- Surveillance (journalisation)
- Sécurité des documents papier
- Traçabilité

Bases de connaissances : Risques physiques

- Eloignement des sources de risque
- Protection contre les sources de risques non-humaines

En conclusion

- Importance fondamentale de l'obligation de rendre des comptes et de la validation par un tiers indépendant(par exemple accrédité par l'autorité de protection).
- Sinon, loin de représenter un progrès, le nouveau règlement risque de se traduire par une régression des droits des personnes
- L'*accountability* joue un rôle central dans le règlement: si elle n'est pas mise en œuvre de manière rigoureuse, c'est tout l'édifice des protections qui est menacé