Institut Mines-Télécom

Informations personnelles et cybersécurité : le risque par essence indissociable

Claire Levallois-Barth

Coordinatrice de la Chaire Valeurs et Politiques des Informations Personnelles

Colloque IMT

Gestion de crise et numérique : nouvelles menaces et nouvelles solutions

Jeudi 31 mars 2022

UNE CHAIRE DE L'IMT DEPUIS 2013

L'ÉQUIPE PLURI-DISCIPLINAIRE

Claire Levallois-Barth

Maître de conférences
en Droit
Coordinatrice et
co-fondatrice de la Chaire

Ivan Meseguer

EU Affairs, Head of Brussels Office,
représentant de l'IMT à Bruxelles –
DG IMT
Co-fondateur de la Chaire

Mark Hunyadi

Professeur de Philosophie morale et politique

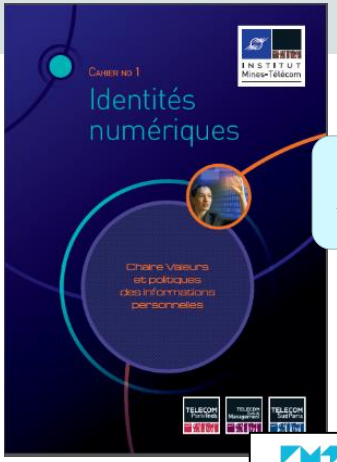
Patrick Waelbroeck

Professeur d'Economie
Co-fondateur de la
Chaire

Maryline Laurent

Professeure en Sciences
Informatiques
Co-fondatrice de la
Chaire

LES 5 AXES DE RECHERCHE



Axe 1. Identités numériques

Axe 2. Gestion des informations personnelles

Axe 3. Contributions et traces

Axe 4. Informations personnelles dans l'Internet des objets

Axe 5 . Politiques des informations personnelles

Institut Mines-Télécom

Institut Mines-Télécom

Informations personnelles et cybersécurité : le risque par essence indissociable

Nombreuses violations/fuites de données personnelles

- Piratage de comptes AMELI PRO concernant de plus de 500 000 citoyens en France
- Diffusion de données de vaccination en Belgique
- « Perte » de données par Facebook
- Nombreuses cyberattaques, rythme croissant, fichiers sensibles …

Usurpation d'identité, hameçonnage, faux sites web, reconnaissance faciale illégale …

Atteinte à nos droits fondamentaux, à notre liberté, à notre souveraineté

Sujet qui ne peut être laissé à l'entière discrétion seule des organisations

2016 : adoption du RGPD

- Mise en œuvre du droit à la protection des données personnelles tel que reconnu par l'article 8 de la Charte des droits fondamentaux de l'Union européenne
- Protéger les utilisateurs ET assurer les activités des entreprises et des organismes du secteur public

Passage du contrôle *a priori* au contrôle *a posteriori*

- Gestion en fonction des risques identifiés

Un marché numérique européen en construction et en connexions

Libre circulation des données

- *Data Gouvernance Act* : « Ouverture » des données personnelles via l'altruisme
- *IA Act* : régulation de la reconnaissance faciale notamment
- *Data Act* : ouverture des données liées à l'Internet des objet
- Révision du règlement eIDAS sur les identités numériques
- Révision du règlement *ePrivacy*
- …

1. L'APPROCHE PAR LES RISQUES

Institut Mines-Télécom

Une définition très large

- Toute information se rapportant à une **personne physique identifiée ou identifiable**
- À savoir une personne physique qui peut être identifiée directement ou indirectement,
- Notamment un identifiant : nom, n° d'identification, **données de localisation**, identifiant en ligne
- Ou à un ou plusieurs **éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale**
  - Données liées à l'utilisation du véhicule par le conducteur ou les occupants : style de conduite, vie à bord …

Pour le responsable de traitement et le sous-traitant

- Collecte, enregistrement, mise à disposition, interconnexion, effacement …

En adoptant des mesures techniques ou organisationnelles appropriées

- Compte tenu de l'état des connaissances
- Des coûts de mise en œuvre
- De la nature, de la portée, du contexte et des finalités du traitement
- Des risques pour les droits et libertés des personnes

En pratique, en fonction du contexte

- Pseudonymiser et chiffrer les données
- Garantir la confidentialité, l'intégrité, la disponibilité, la résilience des systèmes et services
- Rétablir la disponibilité des données et leur accès dans des délais appropriés
- Mettre en place des procédure de test, d'analyse et d'évaluation régulière des mesures …

Protection des données dès la conception

≃ Privacy by design

- **Au moment de la détermination des moyens du traitement et au moment du traitement**
- Mettre en œuvre des mesures techniques et organisationnelles appropriées

Protection des données par défaut

≃ Privacy by default

- **Traiter seulement les données nécessaires au regard de chaque finalité du traitement**
  - Quantité de données collectées
  - Durée de conservation
- **Les données ne sont pas accessibles à un nombre indéterminé de personnes** sans l'intervention de la personne concernée

≃ Cybersecurity by design → Cybersecurity by default

CNIL
Commission Nationale de l'Informatique et des Libertés

2020

2 825 notifications de violation de données

+ 24 % par rapport à 2019

A l'autorité de contrôle, si **risque** pour les droits et libertés des personnes

- Si possible 72 heures au plus tard après en avoir pris connaissance
- Le sous-traitant notifie au responsable du traitement toute violation

A la personne concernée, si **risque élevé** pour les droits et libertés des personnes

- Dans les meilleurs délais
- Conséquences probables et mesures prises, recommandations, coordonnées du délégué à la protection des données …

Prévoir des procédures pour détecter une violation (car risque critique pour la sécurité)

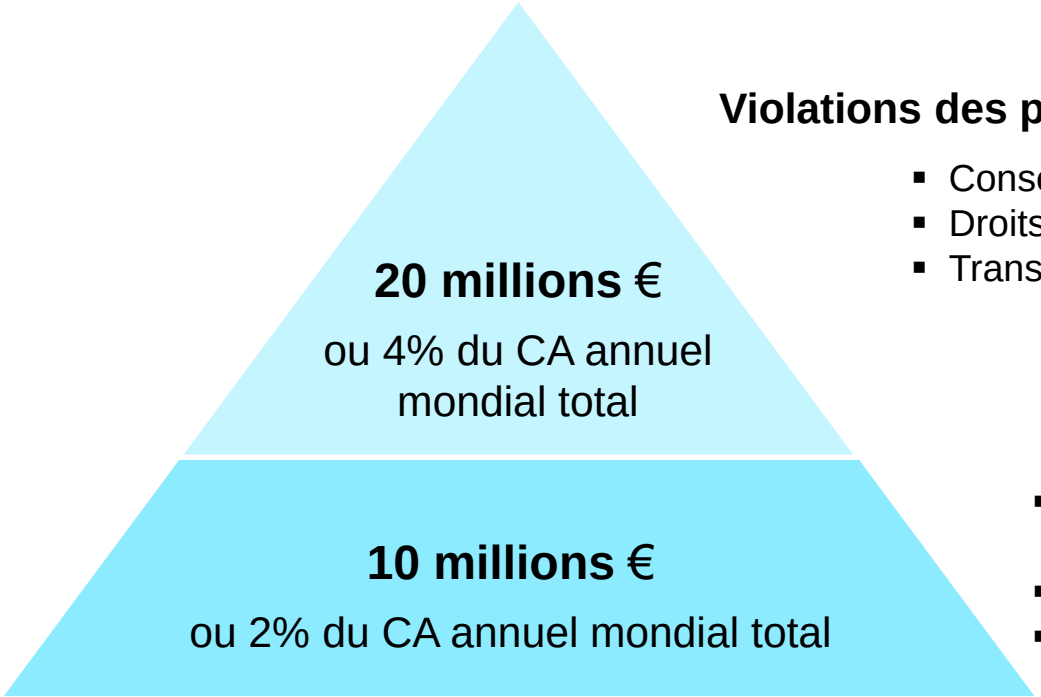
28 décembre 2021 : société SLIMPAY

- Solutions de gestion des abonnements et des paiements récurrents

- **Aucune mesure de sécurité**
  - Accès possible au serveur à partir d'Internet entre novembre 2015 et février 2020

- **Selon la CNIL, risque élevé**
  - Nature des données personnelles : notamment des informations bancaires
  - Volume de personnes concernées : plus de 12 millions
  - Possibilité d'identifier les personnes : risques d'hameçonnage ou d'usurpation d'identité

L'absence de préjudice avéré au moment de l'évaluation pour les personnes n'a pas d'incidence sur l'existence du défaut de sécurité



Violations des principes essentiels

- Consentement préalable
- Droits des personnes
- Transfert hors UE …

- Protection des données dès la conception ou par défaut
- Sécurité des données
- Notification des violation de données

Union européenne

- 30/07/2021 : Amazon : **746 millions** € par la Commission nationale luxembourgeoise
- 3/09/2021 : WhatsApp : **225 millions** € par l'autorité irlandaise pour partage illégal de données personnelles avec sa maison-mère, Meta (Facebook)

CNIL : vérifie systématiquement la sécurité du système lors d'un contrôle

- 14 000 plaintes
- 2021 : 214 millions € d'amende (+55%/2020)
- 135 mise en demeure et 6 mois pour se mettre en conformité

La moitié des sanctions concerne en partie une mauvaise sécurité

- Déc. 2021 : FREE MOBILE : transmet par courriel, en clair, les mots de passe des utilisateurs lors de leur souscription à son offre
  - 300 000 € d'amende car faible nombre de plaintes
  - **Publicité de la sanction** perçu pou FREE comme un « dommage irréversible à sa réputation »

2. LES MÉTHODOLOGIES D'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES

Institut Mines-Télécom

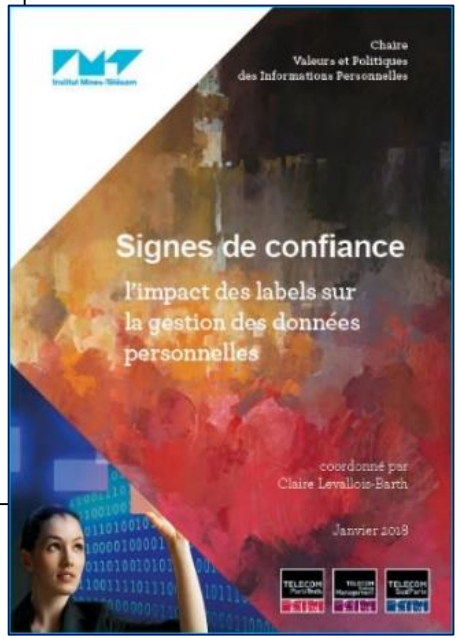
CLAIRE LEVALLOIS-BARTH

Gérer les risques

- **Repérer** les risques, notamment ceux liés à la sécurité des données
- **Qualifier** les risques
- **Diminuer** les risques

Démonter que les risques ont bien été gérés

- Obligation de responsabilité
- En mettant en œuvre les mesures appropriées et en les actualisant
  - Sous la forme de politiques appropriées
- Application d'un code de conduite
- Certification RGPD et Cyber



Pour les droits et libertés des personnes

- Respect de la vie privée, protection des données personnelles
- Non discrimination, liberté de déplacement, d'information …

Lignes directrices AIPD du Groupe de l'Article 29

- Le traitement figure dans la liste de traitements à risque élevé
  - Cybersurveillance par analyse de flux des courriels sortants afin de détecter des fuites d'information (*Data loss Prevention*)
- Ou remplit 2 des 9 critères cités
  - Un type de traitement : profilage pour personnaliser des publicité en ligne, décision automatique
  - Un type de données : données de santé

Aucune méthodologie préconisée

OBJECTIF : TESTER 4 MÉTHODOLOGIES D'ANALYSE D'IMPACT

Analyse d'Impact relative à la Protection des Données (AIPD)

CNIL (française)

- Mise à jour : 2018
- RGPD

BSI (allemande)

- *Bundesamt für Sicherheit in der Informationstechnik*
- Créée en 2011

Évaluation d'impact sur la Vie Privée (Privacy Impact Assessment)

PRIAM (française)

- *Privacy Risk Analysis Methodology*
- Conçue en 2016 par Sourya Joyee De et Daniel Le Metayer (Inria)
- RGPD

NIST (étasunienne)

- *National Institute of Standards and Technology*
- Créée en 2020

CNIL
Commission Nationale de l'Informatique et des Libertés

pia | Analyse d'impact sur la protection des données
privacy impact assessment

MES PIAS | MODÈLES DE PIA | BASE DE CONNAISSANCES | Paramètres | Aide

Mes PIAs > PIAs Actifs > x

X

Catégorie "s"

CONTEXTE
- Vue d'ensemble
- Données, processus et supports

PRINCIPES FONDAMENTAUX
- Proportionnalité et nécessité
- Mesures protectrices des droits

RISQUES
- Mesures existantes ou prévues
- Accès illégitime à des données
- Modification non désirées de do...
- Disparition de données
- Vue d'ensemble des risques

VALIDATION
- Cartographie des risques
- Plan d'action
- Avis du DPD et des personnes c...

Valider le PIA

PIÈCES JOINTES
+ Ajouter

VERSIONS DU PIA
● 29/03/2022 09:50 - Version actuelle
+ Créer une nouvelle version

Édition

Risques

Cette section vous permet d'apprécier les risques sur la vie privée, compte tenu des mesures existantes ou prévues.

MODIFICATION NON DÉSIRÉES DE DONNÉES

Analysez les causes et conséquences d'une modification non désirée de données, et estimez sa gravité et sa vraisemblance.

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Saisissez les impacts potentiels

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Saisissez les menaces

Quelles sources de risques pourraient-elles en être à l'origine ?

Saisissez les sources de risques

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Cliquez ici pour sélectionner les mesures contribuant à traiter ce risque.

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

(Non définie) | Négligeable | Limitée | Importante | Maximale

Justifiez ici la gravité estimée.

0 commentaire(s)

Base de connaissances

Sélectionnez votre base de connaissances

Base de connaissances CNIL

Définition
Mesure

Définition
Source de risque

Définition

Institut Mines-Télécom

PRINCIPALES CONCLUSIONS POUR UNE AIPD OPTIMALE

1. Description des flux de données personnelles

- ► Si traitement « simple » = CNIL
- ► Si flux de données complexes avec plusieurs acteurs = PRIAM qui détaille le cycle de vie des données

2. Évaluation juridique de la nécessité et de la proportionnalité au regard des principes de droits fondamentaux

- ► = CNIL qui permet de s'assurer de la conformité au RGPD

3. Étude technique des risques sur la sécurité des données

- ► État de l'art : ISO 27 000, méthode EBIOS et bonnes pratiques de l'ANSSI
- ► Complétée par PRIAM qui permet de préciser les risques de sécurité en fonction du cycle de vie des données personnelles (collecte, support, acteurs traitant les données …)
- ► Pour une prise en compte des risques financiers et réputationnels : BSI et NIST

4. Mesures d'atténuation des risques

- ► = CNIL pour s'assurer du respect des exigences posées par l'autorité de contrôle

Comment prendre en compte

- les traitements de données personnelles impliquant plusieurs acteurs ?
- Les systèmes déployés à grande échelle ?

En particulier, pour le futur portefeuille d'identité numérique européen

- Proposition de Règlement Identité numérique
- Ambition politique : avec son smartphone notamment, s'authentifier en ligne et hors ligne dans les 27 États membres et signer électroniquement
- Établir un lien entre l'identité légale nationale, les attributs et les justificatifs d'un utilisateur
  - Permis de conduire, diplômes, compte bancaire, paiement, pass sanitaire, santé, sécurité sociale, clés de voiture …
- Assurer la protection des données et leur sécurité de bout en bout
  - Double certification : Cyber (*Cyber Act* et dont le niveau reste à déterminer) et RGPD

Projets européens (de H2020 à Horizon Europe)

- Les nombreux appels à projets requièrent une bonne prise en compte du RGPD et des textes européens récents ou en cours d'écriture
- Il ne suffit pas de dire que l'on a un délégué à la protection des données (DPO) et qu'il va s'occuper de cette question

@CVPIP

YouTube

Valeurs et Politiques des Informations Personnelles