Institut Mines-Télécom

TELECOM Paris

IP PARIS

Conférence

Analyse d'impact relative à la Protection des Données : le cas des voitures connectées

En partenariat avec

TELECOM Paris

IP PARIS

François Pistre (Renault)

Président du Comité de pilotage de la Chaire C3S

NOKIA

THALES

Valeo
SMART TECHNOLOGY
FOR SMARTER CARS

WAVESTONE

ANSSI

SÉCURITÉ ROUTIÈRE
VIVRE, ENSEMBLE.

RÉPUBLIQUE FRANÇAISE
Le Gouvernement

Romain Galesne-Fontaine (IN Groupe)

Président du Comité de pilotage de la Chaire VP-IP

IN GROUPE

BNP PARIBAS

orange

DASSAULT SYSTEMES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

5 axes de recherche

Rida Khatoun

1. Analyse de risques et sûreté de fonctionnement
2. Protection des données et de leurs flux en temps réel, cryptographie et agilité
3. Authentification, identité et empreinte comportementale
4. Résilience « by design »
5. Protection des données personnelles impliquées dans le véhicule connecté (aspects juridiques et sociétaux)

Sur ce cinquième axe, la Chaire C3S travaille de façon rapprochée avec la Chaire « Valeurs et Politiques des Informations Personnelles » de l'Institut Mines-Télécom

CHAIRE VP-IP

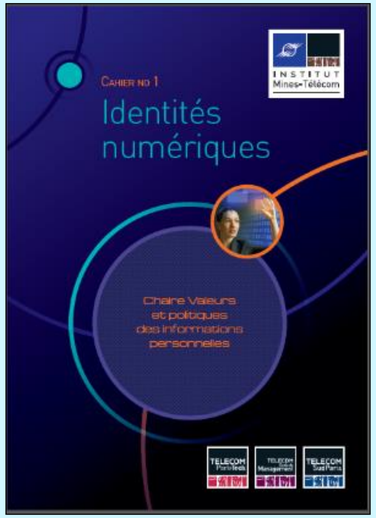
VALEURS ET POLITIQUES DES INFORMATIONS PERSONNELLES

DONNÉES, IDENTITÉS ET CONFIANCE À L'ÈRE NUMÉRIQUE

Institut Mines-Télécom

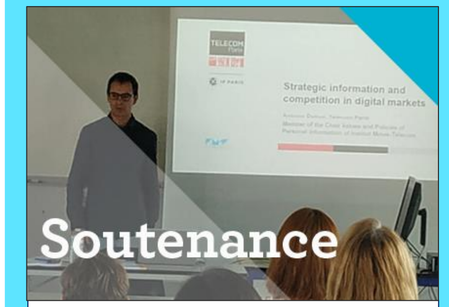
5 axes de recherche pluridisciplinaires

Axe 1. Identités numériques



Axe 2. Gestion des informations personnelles

Axe 3. Contributions et traces



Informations stratégiques et concurrence dans les marchés numériques

Antoine Dubus

Axe 4. Informations personnelles dans l'Internet des objets

13 novembre 2020
20e Rencontre
Identités numériques et reconnaissance faciale

Axe 5. Politiques des informations personnelles

11mars 2021
21e Rencontre

IN GROUPE · BNP PARIBAS · orange · DASSAULT SYSTEMES · CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Analyse d'Impact relative à la Protection des Données : le cas des voitures connectées

Claire Levallois-Barth
Jonathan Keller

Rapport de recherche
Novembre 2021

Renault Mégane E-Tech Electric.

L’analyse d’Impact Relative à la Protection des Données (AIPD)

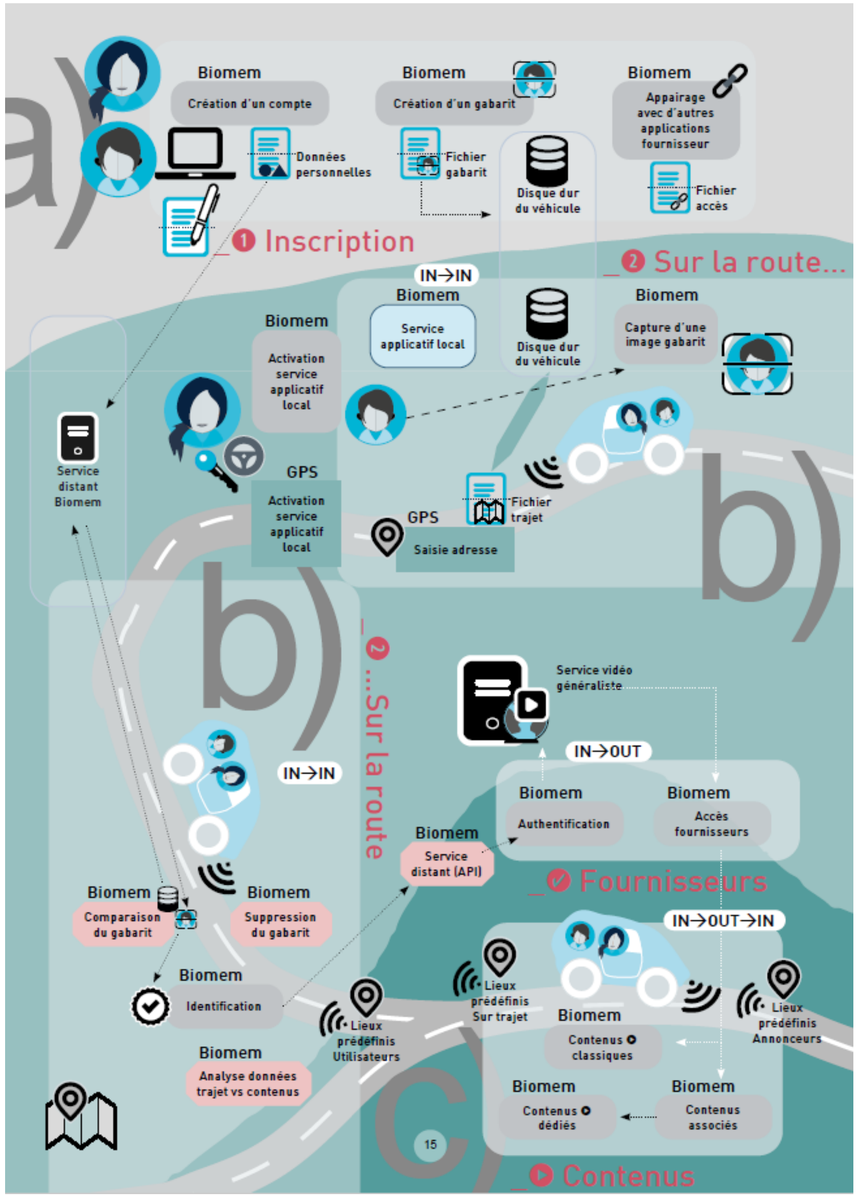
- Une obligation préalable au traitement de données personnelles
- Quand le traitement est « susceptible d’engendrer un **risque élevé pour les droits et libertés des personnes concernées »** (article 35 du RGPD)
  - Un type de traitement particulier (ex. le profilage)
  - Certains types de données (ex. données de santé)
- Un outil pour identifier et atténuer ces risques ET pour démontrer le respect du RGPD
  - Principe de responsabilité ou *accountability*
- Lignes directrices AIPD du Groupe de l’Article 29 de 2017
  - Pas de méthodologie type
  - Des critères à respecter mais loin de répondre à toutes les questions opérationnelles
  - Confusion sémantique entre les AIPD et les Évaluations d’Impact sur la Vie Privée (EIVP)

Partie I et II
Méthodologies d'AIPD

Définition d’un cas pratique

- Service Biomen dans un véhicule connecté
  - Reconnaissance faciale du passager enclenchée par le conducteur
  - Pour accéder à un service de Vidéo à la demande (VOD) auquel il est abonné
  - Avec une signalisation de points d’intérêts sur le trajet par l’utilisation de données de localisation
- Avec 3 sous-hypothèses
  - **Biomem-Indép** : Biomem est une application développée et fournie par une partie tierce du constructeur et du fournisseur de vidéo à la demande
    - Le service est installé par l’utilisateur sur le dispositif d’infodivertissement du véhicule.
  - **Biomem-Constructeur** : Biomem est un service ancillaire fourni par le constructeur par défaut dans le dispositif d’infodivertissement fourni par le constructeur
  - **Biomem-VOD** : Biomem est une application développée par le fournisseur de VOD fournie dans le véhicule connecté.
    - Le service est installé par l’utilisateur sur le dispositif d’infodivertissement du véhicule.
- Un traitement de données personnelles pluripartite
  - Déterminer les obligations qui incombent à chacun des acteurs impliqués

Illustration du flux de données du service Biomem



Textes applicables dans le contexte du véhicule connecté

- RDPD
- Directive ePrivacy

(en cours de révision)

Comité européen de protection des données

Lignes directrices 01/2020 sur le traitement des données à caractère personnel dans le contexte des véhicules connectés

- Notamment permet de déterminer dans quel cas le responsable de traitement doit recueillir le consentement de l'utilisateur (ou de l'abonné)

  ➢ Le responsable de traitement recueille le consentement

  - Lors de la localisation de l'utilisateur/abonné

    ✓ SAUF si la localisation est effectuée dans le cadre de la fourniture d'un service à la demande de l'utilisateur/abonné (art. 5 §3 ePrivacy)

  - S'il inscrit ou accède à des informations sur le support de l'utilisateur/abonné

Objectif : tester 4 méthodologies d'analyse d'impact

Analyse d'Impact relative à la Protection des Données

- **CNIL** (française)
  - Analyse d'Impact relative à la Protection des Données
  - Mise à jour : 2018
  - RGPD
- **BSI** (allemande)
  - *Bundesamt für Sicherheit in der Informationstechnik*
  - Analyse d'Impact relative à la Protection des Données
  - Créée en 2011

Evaluation d'Impact sur la Vie Privée

- **PRIAM** (française)
  - *Privacy Risk Analysis Methodology*
  - Conçue en 2016 par les chercheurs Sourya Joyee De et Daniel Le Metayer (Inria)
  - RGPD
- **NIST** (étasunienne)
  - *National Institute of Standards and Technology*
  - Créée en 2020

	CNIL (AIPD)	BSI (AIPD)	PRIAM (EIVP)	NIST (EIVP)
Axé	Données personnelles (RGPD mais surtout cybersécurité)	Données personnelles (directive 95/46/CE)	Données personnelles (RGDP)	*Personal information*
Conformité au RGPD	**+++**	**-**	**++**	**- -**
Définition des menaces	**+** **(uniquement cybersécurité)**	**-**	**+++**	**+++**
Type de risque pris en compte	Pour les personnes concernées	Pour les personnes concernées et le responsable du traitement	Pour les personnes concernées (groupe et société)	Pour le responsable de traitement
Vraisemblance	Appréciation subjective par le Responsable du traitement (**qualitative**)	Application rigoureuse de la méthode spécifique au RFID	Recours aux *harms trees* (**quantitative**)	Recours à des méthodes de calcul (**quantitative**)
Niveau d'appréciation de la gravité du risque	Individu (en fonction du dommage envisagé)	Individu / société	Individu / groupe / société (en fonction du type de dommage)	« *business impact* »
Facilité d'utilisation	**+++**	**+**	**- -**	**+++**
Application à un traitement complexe	**+**	**++** (si RFID)	**+++** (très coûteux et très chronophage)	**-**
Similarité des résultats obtenus	Répond aux critères de l'annexe 2 des lignes directrice AIPD du CEPD	Rigidité qui empêche l'adaptabilité	Répond aux critères de l'annexe 2 des lignes directrice AIPD du CEPD	Résultats hors sujet

Principales conclusions sur les AIPD

- L'article 35 du RGPD et les lignes directrices sur l'AIPD du CEPD ne préconisent aucune méthodologie
  - A la fois une opportunité et une incertitude quant à la conformité du traitement

- Pour une AIPD optimale
  1. **Description des flux de données personnelles**
     - Si traitement « simple » = méthodologie CNIL
     - Si traitement complexe (ex. multipartite) = méthodologie PRIAM qui détaille le cycle de vie des données
  2. **Appréciation de la nécessité et de la proportionnalité du traitement**
     - Méthodologie CNIL qui permet de s'assurer de la conformité au RGPD
  3. **Appréciation des risques**
     - S'inspirer de la méthodologie PRIAM
     - Pour une prise en compte les risques financiers et réputationnels : méthodologies BSI et le NIST
     - Pour une identification des risques pour la vie privée aussi complète que possible : méthodologie de modélisation des menaces pour la vie privée LINDDUN de KU Leuven
  4. **Mesures d'atténuation des risques**
     - Méthodologie CNIL = s'assurer du respect des exigences posées par l'autorité de contrôle

Partie III

Jurisprudences sur les notions de risque et de dommage

Qu’est-ce qu’un « risque » pour le juge ou une autorité de protection des données comme la CNIL ?

1. L’appréciation des risques par la CJUE et la CEDH

- Cour de justice de l’Union européenne (CJUE)
  - La gestion des risques pour les produits mis sur le marché
  - « État des connaissances » qui impose une veille continue
- Cour européenne des droits de l’homme (CEDH)
  - L’appréciation des risques aux regard des « droits et libertés »
  - Prise en compte du seul risque réel et immédiat
  - Non prise en compte du risque futur et improbable au moment de la demande

2. L’appréciation de la violation des données personnelles par le juge judiciaire

- Les actions de groupe
  - Origine : le juge étasunien et britannique : le dommage doit être identique
  - Repris dans le RGPD : pas de jurisprudence française (pour l’instant)
- Les sanctions et réparation
  - Critères définis par le CEPD (UE)
  - Critères définis par le juge étasunien, britannique et français
    - Prise en compte du dommage moral immédiat
    - Exclusion du dommage matériel et du dommage futur
    - Prospective : ? dommage d’anxiété

		Recevabilité en droit …				
Risque	Méthodologie	de l'Union européenne	de la Convention ESDH	Français	Étasunien	Britannique
Préjudice Individuel	CNIL, PRIAM, NIST, BSI	Oui				
Préjudice collectif	PRIAM, NIST	Oui (mais seulement par groupe de demandes de même catégorie)		Droit en cours d'élaboration	Si preuve d'un dommage provenant du même fait générateur	Si l'identité du dommage provenant du même fait générateur
Préjudice sociétal	PRIAM , NIST	Oui (indirectement pour qualifier une infraction)			Oui (l'importance de certaines bases de données personnelles a amené la FTC à reconnaître l'existence d'un dommage)	Non (la démonstration de la preuve d'un préjudice sociétal a été réfutée)

		Recevabilité en droit …				
Risque	Méthodologie	de l'Union européenne	de la Convention ESDH	Français	Étasunien	Britannique
Atteinte au droit à la vie privée	CNIL, PRIAM	Oui (indirectement pour des affaires relevant des données personnelles)	Oui (à titre principal)	Non (mais la CNIL le mentionne dans ses délibérations)	Oui (comme fondement spécifique)	
Violation des données personnelles	CNIL, PRIAM	Non (mais possible par le pouvoir normateur du juge européen)	Non (la CEDH n'a pas été interrogée sur cette question)	Oui (faiblement et uniquement en cas de mauvaise foi du responsable du traitement)	Un tel préjudice n'est pas encore retenu mais le droit des *torts* trouverait à s'appliquer	

Institut Mines-Télécom

CHAIRE CONNECTED CARS & CYBER SECURITY

CHAIRE VP-IP
VALEURS ET POLITIQUES DES INFORMATIONS PERSONNELLES
DONNÉES, IDENTITÉS ET CONFIANCE À L'ÈRE NUMÉRIQUE

TELECOM Paris

IP PARIS

Table ronde

Florian Damas
Responsable des affaires politiques et réglementaires
Nokia

Claire Levallois-Barth
Enseignant-chercheur en droit
IMT/Télécom Paris

Thomas Moreau
Juriste
CNIL

Cidalia Beleza
Déléguée à la protection des données
Renault

Antonio Kung
Président de Trialog

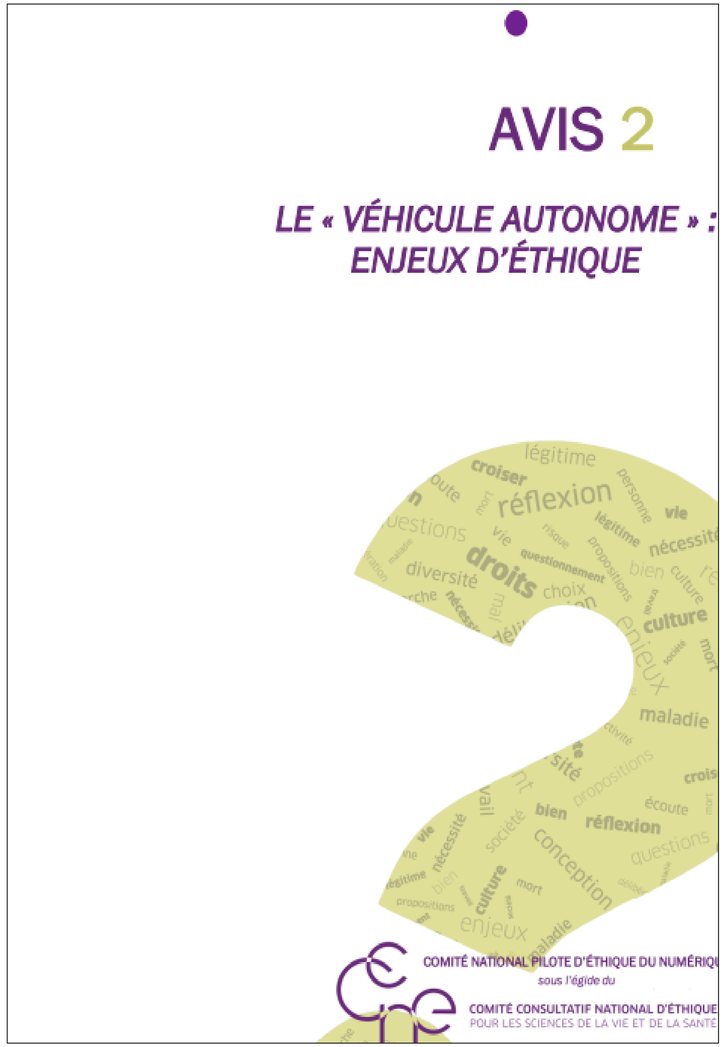
Jonathan Keller
Ingénieur d'études en droit
IMT/Télécom Paris

COMITE NATIONAL PILOTE D'ETHIQUE DU NUMERIQUE

Sous l'égide du
COMITE CONSULTATIF NATIONAL D'ETHIQUE
POUR LE SCIENCES DE LA VIE ET DE LA SANTE

Mardi 14 décembre 2021

Campus Pierre & Marie Curie
4, place Jussieu
75005 Paris



Institut Mines-Télécom

TELECOM Paris

IP PARIS