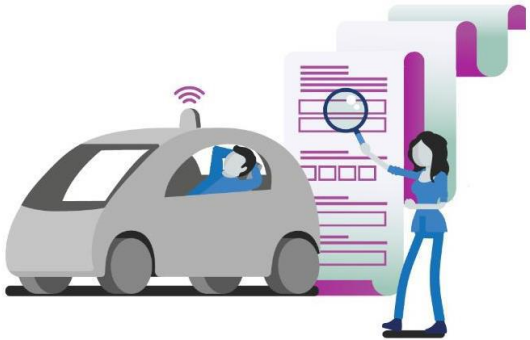
« L'assurance et la donnée »

AMU - Aix-en-Provence, 26 avril 2019



Quel traitement juridique pour la donnée personnelle ?

Illustration par la mobilité connectée et l'assurance

Michèle GUILBOT

Directrice de recherche

Laboratoire Mécanismes d'Accidents

Département TS2

IFSTTAR

Trystan LAURAIRE

Docteur en droit. Enseignant-Résident au Collège universitaire Français de Saint-Pétersbourg

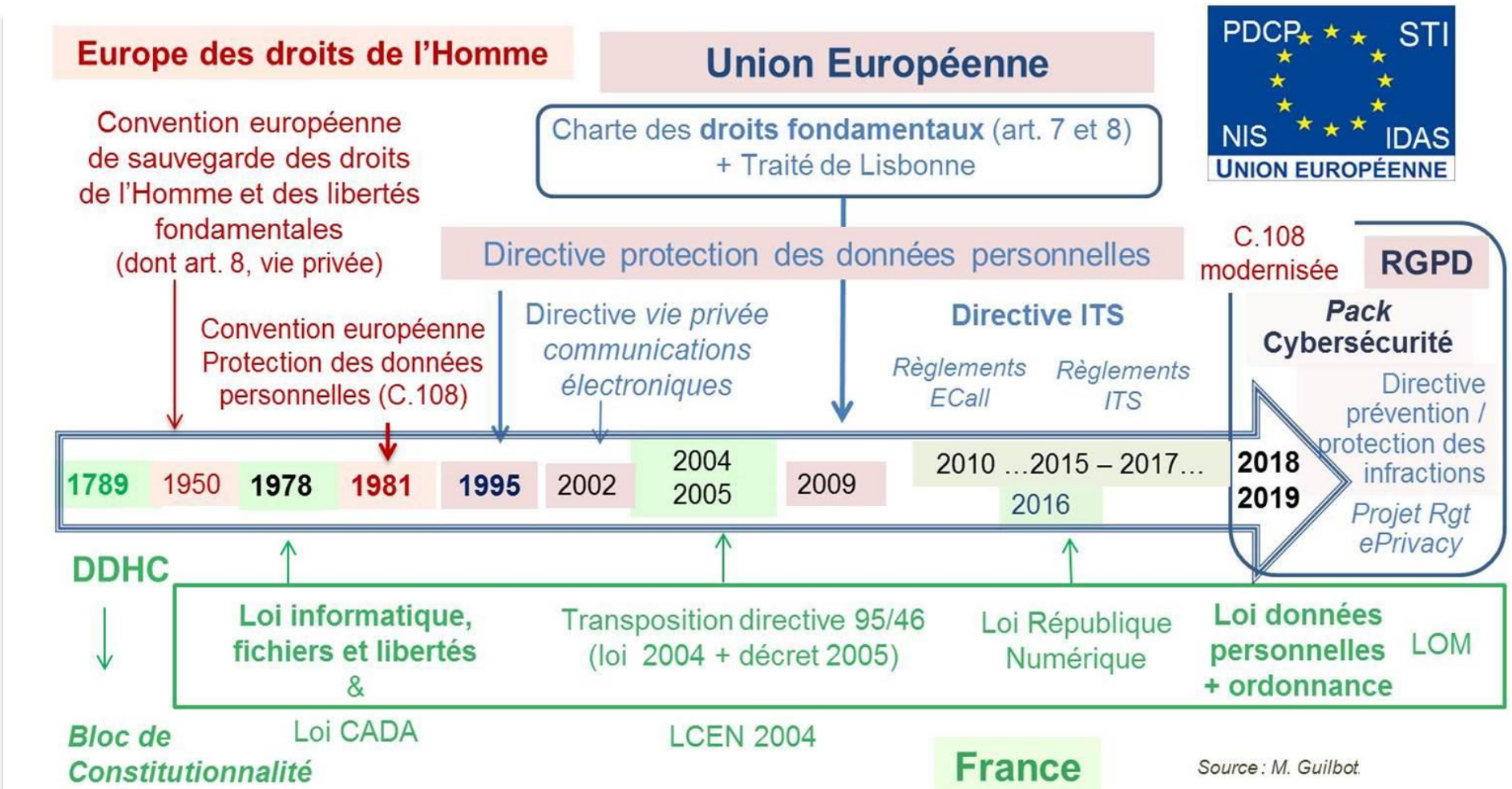
Laboratoire de droit privé et sciences criminelles

Sommaire

Introduction

Contexte juridique pour la protection des données personnelles

Un cadre juridique très complet en Europe et en France

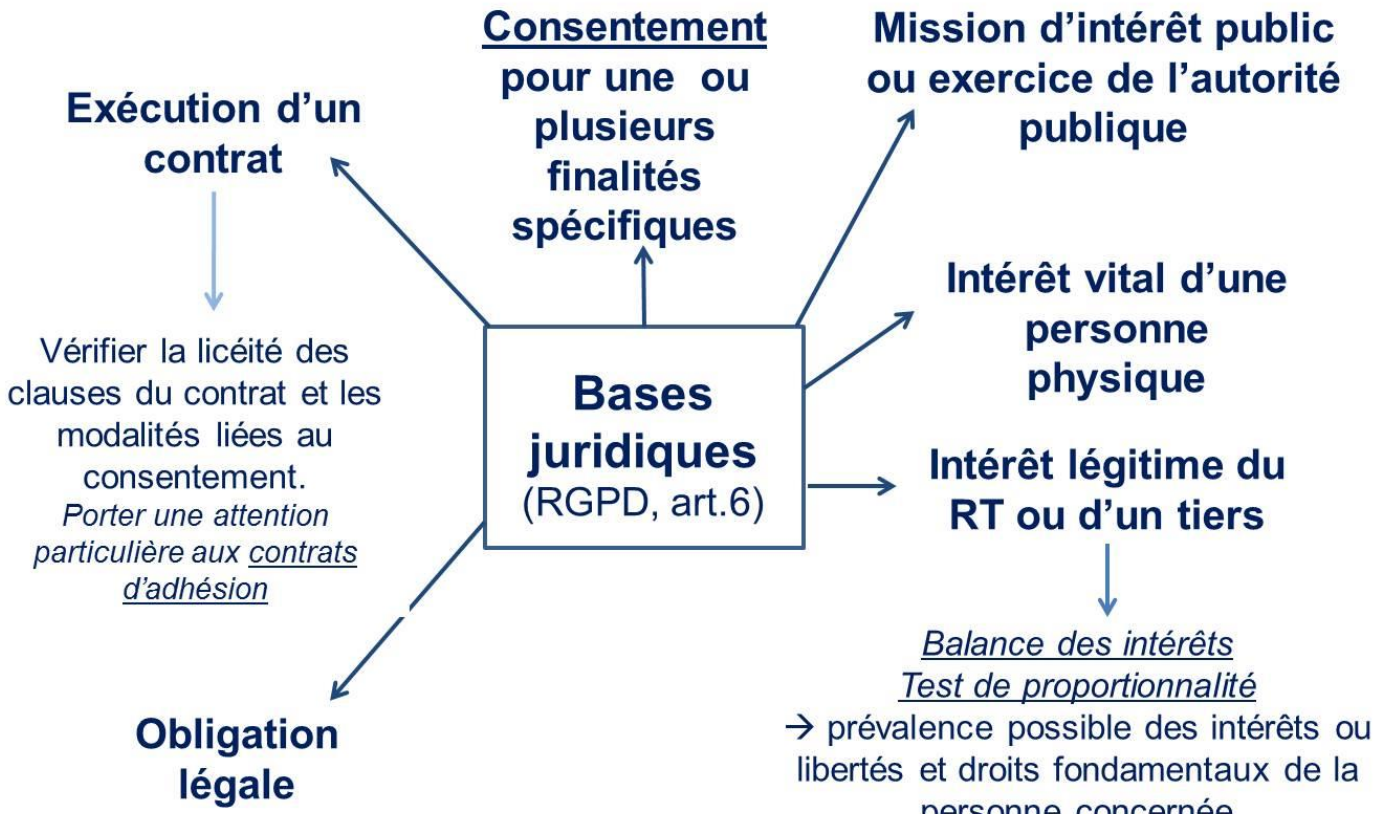


Quelle base juridique pour la collecte et le traitement ?

Quelle que soit la base juridique

↓

les règles de protection sont applicables



Source. M. Guilbot.

Quelles règles pour la protection des droits des personnes ?

1ère partie

Données personnelles et finalités des traitements

I.- La donnée personnelle

- *Notion, illustrations*
- *Focus sur la notion d'infraction pénale*

La donnée personnelle, notion, illustrations 1/2

La possibilité d'identifier une personne physique, un **critère central** de qualification des données personnelles

Toute information concernant une personne physique **identifiée ou identifiable** (personne concernée); est réputée identifiable une personne qui peut être identifiée **directement ou indirectement** (…), notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, **des données de localisation**, ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

(*RGPD, entré en application le 25 mai 2018*)

Une adresse IP, même dynamique (CJUE, 2016 ; C. Cass., 2016)
Une adresse MAC, même cryptée (CE, 2017)

pseudonyme, association de données …

Prendre en compte le **risque de ré-identification**

La pseudonymisation n'est pas l'anonymisation

La donnée personnelle, notion, illustrations 2/2

Des données **identifiantes** et/ou **sensibles**, …

… mais qui s'avèrent **nécessaires** pour la gestion des mobilités et de leurs conséquences, notamment dommageables

Exemples

– personnes physiques (auteurs présumés, victimes, témoins,...)
  - numéro d'identification (**NIR**),
  - données nominatives, adresse(s), n° tél., …
  - état physiologique du conducteur (*ex. alcoolémie, endormissement, malaise*)
  - défaut d'attention
  - infractions, condamnations, …

– véhicules
  - n° d'identification (***VIN***),
  - n° immatriculation,
  - état des équipements, données techniques (*qui peuvent révéler des données personnelles*), …

Focus sur la « donnée d'infraction » (1/3)

- Le concept retenu

Les données d'infraction : « *données personnelles relatives aux condamnations pénales, aux infractions ou aux mesures de sûretés connexes* ».

Critère déterminant le concept retenu : le régime commun et le recours à cette formule dans les principaux textes normatifs régissant la matière (ex : art. 9 Loi IL ; art. 10 RGPD).

Ex : fichiers judiciaires ; données de géolocalisation ; l'enregistrement des données de conduite par des boitiers EDR.

- Les concepts utilisés par la CNIL

Distinction entre la donnée *d'infraction par nature*, permettant à elle seule l'établissement d'une infraction et la donnée *d'infraction par destination* qui ne le permet pas mais qui entre toutefois dans le domaine de l'article 9 de la Loi IL.

Ex : une vitesse instantanée = donnée d'infraction par destination car il faut l'associer à une donnée de géolocalisation pour permettre le constat d'une infraction.

Focus sur la « donnée d'infraction » (2/3)

Les cadres relatifs au traitement des données d'infraction

- ### Les cadres européens

CEDH : Moule duquel les régimes de protection des droits sont issus.

Modèle bâti sur trois fondements : **légalité, légitimité et nécessité**.

La procéduralisation de la loi demeure catégorielle, c'est-à-dire en lien avec le degré d'atteinte au droit par le procédé utilisé.

UE : article 8 de la Charte des droits fondamentaux : « toute personne a droit à la protection des données à caractère personnel la concernant ».

Respect du droit européen des droits de l'homme et usage de la jurisprudence de la Cour européenne par la CJUE.

Prescriptions spécifiques au traitement des données d'infraction dans le droit dérivé :

art. 10 RGDP et Directive « Police-Justice ». Articulation entre ces outils organisée par les textes ce qui n'empêche pas certaines difficultés : Quid des fins entrant dans « la matière pénale » => utilisation de la jurisprudence européenne.

Focus sur la « donnée d'infraction » (3/3)

Les cadres relatifs au traitement des données d'infraction

- Le cadre national

Constitutionnel :

Mouvement d'extension puis, depuis 1999, de rétractation du domaine de la « liberté individuelle » dans la jurisprudence de l'article 66 de a Constitution.

De ce fait, fondement de la protection du droit au respect de la vie privée : article 2 de la DDHC qui s'étend, selon une jurisprudence bien établie, « *la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel* » (C.C. n° 2012-652 DC, cons. 8).

Légal :

Loi 78-17 du 6 janvier 1978 dite « Informatique et libertés » récemment modifiée par la loi du 20 juin 2018 pour mettre le droit national en conformité avec les prescriptions européennes.

Ordonnance 2018-1125 du 12 décembre 2018 modifiant la loi du 6 janvier 2018

- EV → 1er juin 2019 au plus tard
- loi de ratification a déposer le 13 juin 2019 au plus tard

1ère partie

Données personnelles et finalités des traitements

II.- L'assurance et la donnée : quelles données ? pour quelles finalités ?

- *L'indemnisation des victimes*
- *L'adaptation des primes à la situation de l'assuré*

Quelles données pour l'indemnisation des victimes d'accidents ?

Pour l'exécution de sa mission, l'assureur peut recevoir communication d'informations

- sur les véhicules
  - fichier des véhicules assurés … et des véhicules non assurés, établis à l'aide notamment du SIV → décret juillet 2018, *transmission par AGIRA / organisme d'information*
  - *des fichiers des véhicules (données techniques pour réparation, maintenance) sont-ils constitués ? → les données sont-elles communicables aux assureurs ? comment sont informées les personnes concernées ? quelle base juridique ?*
- sur les conducteurs
  - issues du SNPC (*fichier des permis de conduire*) → *c. route, R. 330-3, par min. intérieur*
  - concernant les pièces administratives relatives à la circulation du véhicule → *c. route, R.225-5.II, par préfet*
  - infractions et autres données (*par ex. transmission des PV par AGIRA-TransPV*)
- sur les circonstances d'un accident
  - géolocalisation, vitesse pratiquée, déroulement des faits, …

L'adaptation des primes à la situation de l'assuré : quelles bases juridiques ? Quels risques spécifiques ? (1/2)

Années 2000 : des offres basées sur l'utilisation de la géolocalisation pour vérifier certains éléments liés aux déplacements et à la conduite

- des conditions élaborées en concertation entre une mutuelle et la CNIL ont permis la mise œuvre d'une offre PAYD en 2008 après un refus en 2005
- 2010, recommandation CNIL sur la mise en œuvre des dispositifs de géolocalisation embarqués par les assureurs et les constructeurs
- 2018, constitution d'un groupe de travail sur la géolocalisation (CNIL)

Des offres diversifiées

Pay as you drive

L'assurance au kilomètre

- une cotisation calculée en fonction des kilomètres effectués
- une assurance éco responsable : « *moins vous roulez, moins vous payez !* »

Des services complémentaires

- suivi des kilomètres effectués et de la cotisation en cours
- contact automatique en cas d'accident : en cas de détection d'un accident potentiel, réception d'un SMS contenant les coordonnées de l'assistance
- service « *Où suis-je garé ?* »

La personnalisation de l'assurance auto

- adaptation de la tarification à la manière dont l'assuré conduit sa voiture.
  → prise en compte de certains paramètres comme l'accélération, le freinage ou encore la vitesse dans les virages, pour calculer la prime

Pay how you drive

L'adaptation des primes à la situation de l'assuré : quelles bases juridiques ? Quels risques spécifiques ? (2/2)

Demain, une prime déterminée à l'aide d'algorithmes prédictifs ?

– La décision individuelle automatisée et la loi

« *La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* » (RGPD, art. 22)

sauf

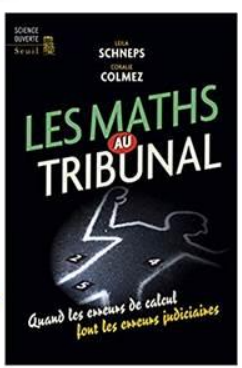
- exécution d'un contrat entre la personne et le RT
  (obs. le contrat n'exclut pas le consentement …)
- autorisation de la loi + mesures appropriées
- consentement explicite de la personne

« *Aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé* […] » (LIL, art. 10 al.2)

sauf

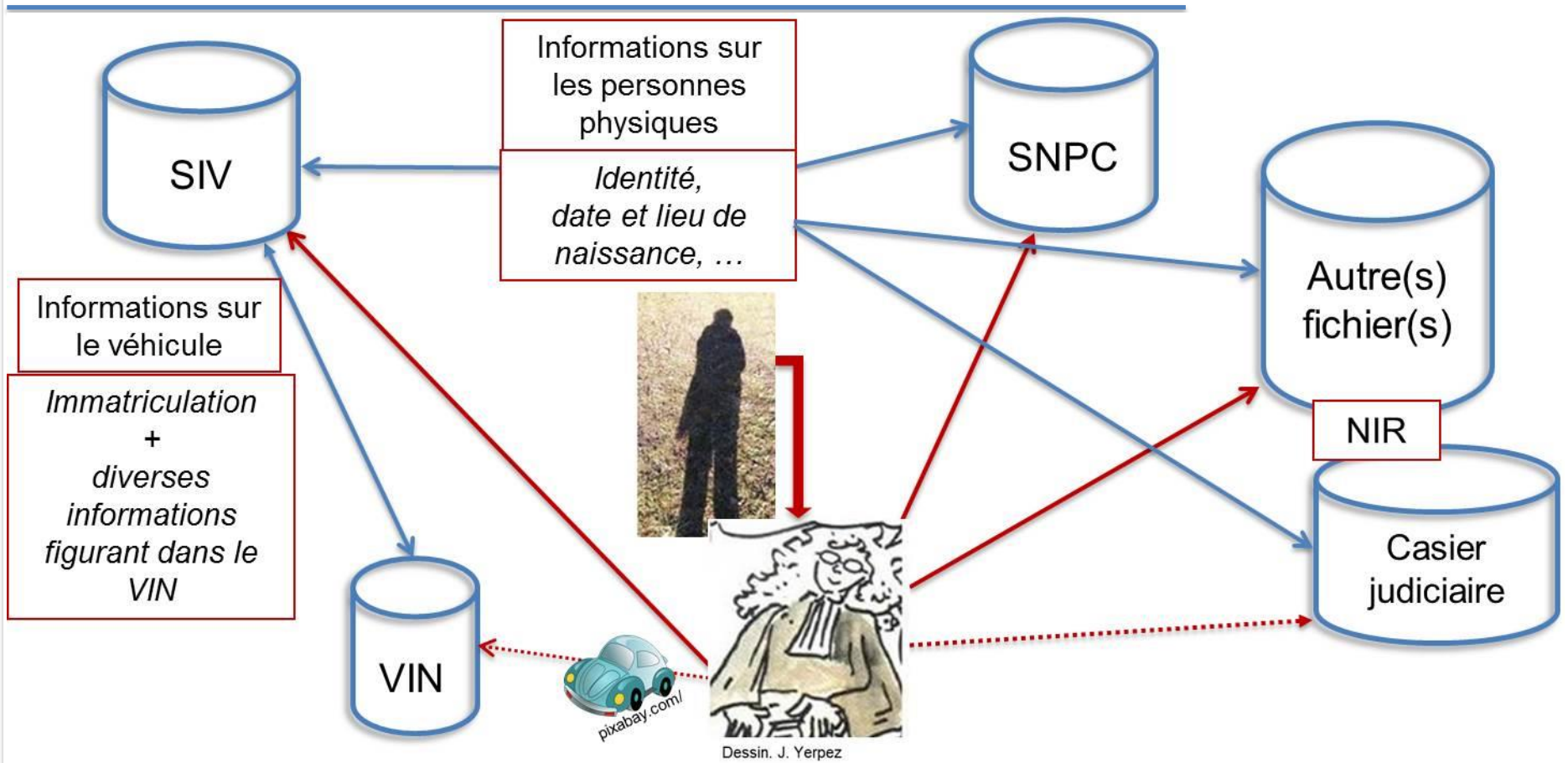
contrat, si la personne concernée a été mise à même de présenter ses observations

– La prédiction et les risques d'erreur dans les calculs de probabilité



– Le calcul des primes, le risque de discrimination et de modification du modèle
→ quid du caractère mutualiste de l'assurance ?

Le respect des finalités et des mesures de protection face aux risques d'interconnexions de fichiers et d'identification des personnes physiques



2ème partie

Un traitement protecteur des droits des personnes

I.- Droits des personnes concernées et conséquences des atteintes à ces droits

- *La personne : quels droits ? quels risques ?*
- *L'atteinte aux droits des personnes et les risques juridiques en cas de violation*

Préserver les risques d'atteintes aux droits des personnes

- Quels droits pour les personnes physiques ?
  - **Liberté individuelle**

> **DDHC, art. 4.** La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres membres de la société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la Loi.

→ DDHC intégrée au « bloc de constitutionnalité »

- **Liberté d'aller et venir** → Convention européenne des droits de l'Homme, protocole n°4, 1963 art 2 ; Pacte ONU, 1966, droits civils et politiques, art. 12
- **Vie privée**
  - protection du domicile, de l'image, de l'intimité, secret médical, …

→ protection des droits de la personnalité → code civil, art. 7 à 9 ; Charte des droits fondamentaux de l'UE

- **Protection des données personnelles** → RGPD, Convention européenne, droit interne
- **Droit de la consommation, droits des contrats, …**

Préserver les risques d'atteintes aux droits des personnes

- Quels droits pour les personnes physiques ?

Ne pas être connu, reconnu, tracé dans ses déplacements
(sauf nécessité pour la finalité)

Information claire et accessible
↓
Consentement éclairé

Droit d'accès aux données
et, selon les bases juridiques et les finalités
- **opposition**
- **rectification**
- **limitation**
- **effacement**
(droit à *l'oubli*)

Protection en cas de
traitement automatisé, algorithmique
↓
Décision individuelle produisant des effets juridiques

Décision de justice impliquant une appréciation du comportement d'une personne

Portabilité des données
fournies par la personne

Données personnelles
= attributs de la personnalité (UE) vs/ biens de consommation (EU)

Source : M. Guilbot

La faille de sécurité, un risque majeur à anticiper

Captation / utilisation illicites de données

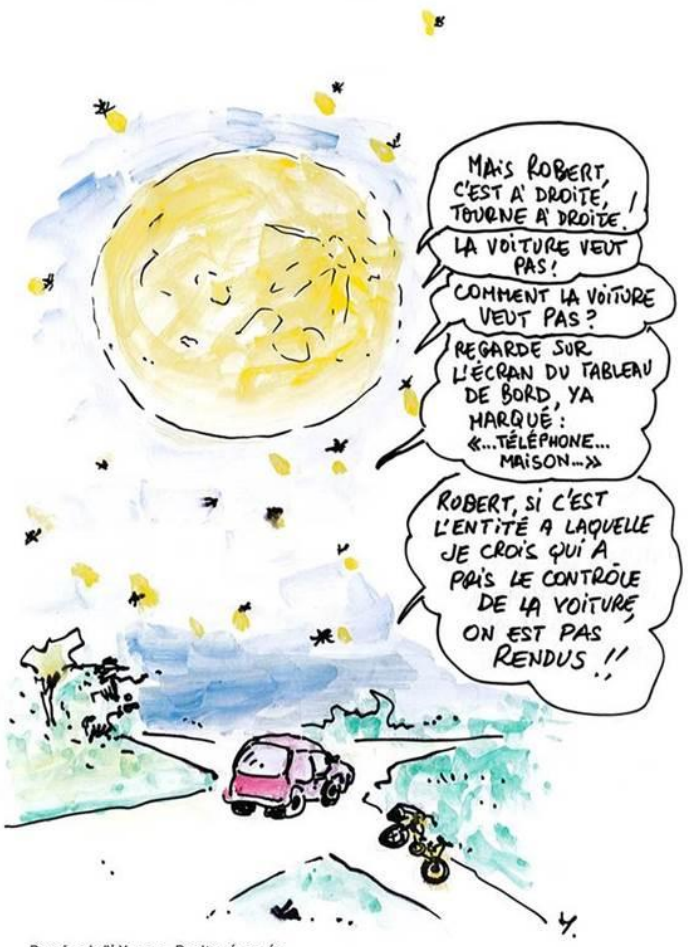
- injection de données erronées, modification des algorithmes, des messages délivrés…
  - impact sur les tâches confiées au système ou à l'humain
  - atteinte aux droits des usagers (*données personnelles, vie privée, …)*

Attaque par déni de service

- *ex.* communication véhicule ⟷ infra => déni de service sur le système de gestion du trafic

Prise en main du contrôle par un tiers

- d'un élément du système, d'une tâche, …
- d'une activité (*ex. ITS => gestion du trafic routier*)



Dessin : Joël Yerpez. Droits réservés

La faille de sécurité, un risque majeur à anticiper

Prendre des mesures de sécurité pour

Le fonctionnement des systèmes

Construction d'un **droit de la cybersécurité**

Des projets pour la sécurité des systèmes automatisés dans les véhicules

Réglementation communautaire / Réglementation technique du véhicule / droit interne / normalisation

La protection des données personnelles

RGPD, art. 32
Loi Informatique et Libertés, art. 34

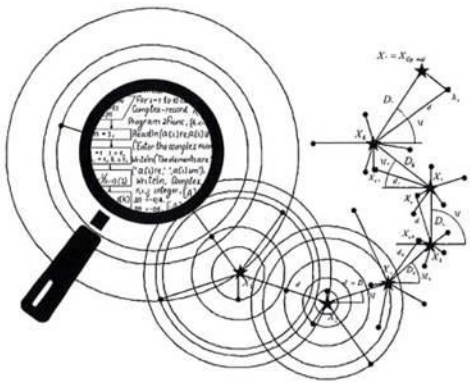
La sécurité des systèmes de communications

Quid du règlement ePrivacy ?

ECE-ONU → proposition d'un texte pour la protection des données et la cybersécurité dans le véhicule connecté, automatisé (mars 2017)

=> Réglementation technique internationale des véhicules

Comment garder la main ?



COMMENT PERMETTRE À L'HOMME DE GARDER LA MAIN ?

Les enjeux éthiques des algorithmes et de l'intelligence artificielle

SYNTHÈSE DU DÉBAT PUBLIC ANIMÉ PAR LA CNIL DANS LE CADRE DE LA MISSION DE RÉFLEXION ÉTHIQUE CONFIÉE PAR LA LOI POUR UNE RÉPUBLIQUE NUMÉRIQUE

DÉCEMBRE 2017

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

éthique numérique les algorithmes en débat

Tandis que le ministère de l'intérieur développe la centralisation de ses renseignements

Une division de l'informatique est créée à la chancellerie

« Safari » ou la chasse aux Français

JUSTICE

LE MONDE — 21 mars 1974 — Page 9

"JE CRAINS LE JOUR OÙ LA TECHNOLOGIE DÉPASSERA L'HOMME"

ALBERT EINSTEIN

« **Oublier la cybersécurité** c'est rouler à 200km/h à moto sans casque »

(Guillaume Poupard, Pdt ANSSI, nov. 2016)

Consentement et autodétermination informationnelle

Consentement *

* *Sauf autres bases légales*

- Libre
- Éclairé
- Spécifique
- Univoque
- Réel (preuve vérifiable auprès du RT)

→ impose la délivrance d'une **information** claire et précise par le RT

Des consentements « ++ »

- Géolocalisation et autres données particulières (ex. santé, religion, biométrie,..)
- Transfert hors UE

Autodétermination

« *Pouvoir de l'individu de décider lui-même quand et dans quelle mesure une information relevant de sa vie privée peut être communiquée à autrui* »
(Cour Constitutionnelle allemande1983)

« *Toute personne dispose du droit de décider et de contrôler les usages qui sont fait des données à caractère personnel la concernant, dans les conditions fixées par la présente loi.*»
(loi *Informatique et Libertés* art.1 al1)

D'autres corpus de règles s'appliquent également :

- droit des contrats (*v. notamment contrats d'adhésion*)
- droit de la consommation

Des actions en cas de violation

Action individuelle

Bonnes pratiques, mesures de protection « techniques »

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Dessins: J. Yerpez.

Action de groupe

- Finalité : **faire cesser le dommage** *(loi République numérique, 2016)*
- Finalité : **indemniser les préjudices** *(L. 2018)*
- Voie associative

(juge judiciaire ou administratif)

Quels risques juridiques en cas d'atteintes aux données personnelles ?

Sanctions administratives

Il est important de noter que si ces sanctions sont qualifiées ainsi car elles sont prononcées par une autorité administrative indépendante. Néanmoins, elles ont, pour certaines d'entre elles, une nature pénale au sens de la jurisprudence de la Cour européenne.

Art. 45 III de la loi informatique et libertés prévoit, en cas de non respect des obligations prévues par RGPD ou de la présente loi :

- Rappel à l'ordre.
- Injonction de mettre le traitement en conformité, assortie au besoin d'une astreinte d'un montant maximal de 100 000 euros par jour de retard.
- Limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation.
- Retrait de certification.
- Suspension du flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale.
- Amende dont le montant ne pourra, en principe, excéder dix millions d'euros ou, pour une entreprise, 2% du chiffre annuel mondial de l'exercice précédent si ce montant excède 10 millions et, dans les hypothèses prévues aux cinquième et sixièmement de l'article 83 du règlement européen du 27 avril 2016, 20 millions d'euros ou 4% dudit chiffre d'affaire

Deux remarques principales quant à ces sanctions:

- Mise à l'abri de l'Etat qui, fort heureusement, n'a pas été étendue aux collectivités territoriales.
- Aggravation des sanctions ce qui s'inscrit dans la tendance répressive.

Quels risques juridiques en cas d'atteintes aux données personnelles ?

Sanctions pénales

Les articles 226-16 et suivants du code pénal incriminent diverses atteintes aux droits résultant des fichiers ou des traitements informatiques et les punissent, par principe, de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Sont ainsi incriminés :

- Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi.
- Le fait de procéder ou de faire procéder à un traitement de donner sans prendre toutes les précautions utiles pour « préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées » ou que des tiers y aient accès.
- Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite.
- Le fait de procéder à un traitement concernant une personne malgré son refus, lorsque le traitement répond à des fins de prospection, ou lorsque cette opposition est fondée sur des motifs légitimes.
- Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données « sensibles », sans le consentement exprès de l'intéressé ainsi que des données d'infraction.
- Le fait de dépasser la durée légale de conservation à l'exception des hypothèses expressément prévues, de détourner les données collectées de leur finalité ou de porter à la connaissance de tiers des informations dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée.

2ème partie

Un traitement protecteur des droits des personnes

II.- Evolutions en cours et outils pour la protection

- *Les évolutions en cours. Quelles opportunités, quelles nécessités, pour les assureurs ?*
- *Quelles méthodes pour la protection ?*

Les évolutions en cours.
Quels accès aux données des véhicules connectés ?

L'enregistreur de données : limites et droits d'accès aux données

- protection des données personnelles et de la vie privée
- valeur juridique de la preuve
- ne pas confondre causalité et corrélations
- propriété intellectuelle / industrielle, secret des affaires / droit de la concurrence

Dessins. J. Yerpez. Kissifrot (Prédit 3)

Les évolutions en cours.
Quels accès aux données des véhicules connectés ?

L'usage probatoire des données obtenues en violation des prescriptions « légales »

Deux considérations apparaissent particulièrement importantes :

Fiabilité : Ce besoin de fiabilité de la donnée obtenue et utilisée en tant que preuve a pour corollaire « *l'homologation et la vérification périodique du système technique garantissant son bon fonctionnement et la fiabilité des résultats ».* Il s'agit de s'assurer de la fiabilité de l'outil et de son bon fonctionnement dans des conditions normales.

La fiabilité nécessite également, dans l'hypothèse d'un engin technique connecté, d'encadrer le risque **cyber** ce qui, dans un cadre contentieux pose des difficultés quant à la **charge** de la preuve et les **modalités**, voire les **possibilités** de preuve.

Recevabilité:

- Distinction entre matière civile et procédure devant les juridictions pénales
- Distinction entre preuves rapportées par une personne privée et par une autorité publique dans ce dernier domaine
- Développement résiduel des droits de la défense comme cause d'irresponsabilité pénale même si cela ne semble pas concerner cette question.

Enjeu prospectif : l'utilisation *a contrario* de l'arrêt *Ibrahim* rendu par la Cour européenne des droits de l'homme peut-elle aboutir à redéfinir la recevabilité des preuves obtenues en violation de stipulations conventionnelles ? (CEDH, 13 septembre 2016)

Les évolutions en cours. *Le projet LOM*
Quels accès aux données des véhicules connectés ?

Art. 13. PL adopté par le Sénat,, n° 1831, déposé à l'AN le 3 avril 2019
→ pouvoir au Gouvernement, ordonnance art. 38 de la Constitution

En cas d'accident, sans consentement du conducteur et gratuitement **(art. 13-2°)**

Données des **dispositifs d'enregistrement de données** d'accident (EDR, *Règlement UE en cours*)

Données d'état de **délégation de conduite** enregistrées dans la période qui a précédé l'accident (ADDR / DSSAD *ECE-ONU, en cours*)

Finalité : Détermination des responsabilités ⇒ plus large que les finalités du Rgt UE / EDR

Destinataires

Forces de l'ordre

Organismes chargés de l'enquête technique et de l'enquête de sécurité (c. transports, art. L.1621-2)

Assureurs ne figurent pas, directement ou indirectement, parmi les destinataires

Propositions :

Durée de conservation à indiquer (EDR) ou à préciser (*DSSAD)*

Informer l'acquéreur du véhicule et le(s) conducteur(s) sur le mécanisme adopté

+ effacement des données « au fil de l'eau » en l'absence d'accident (*cf. eCall*)

…

Les évolutions en cours. *Le projet LOM*
Quels accès aux données des véhicules connectés ?

Données des systèmes <u>intégrés</u> aux VTM équipés de dispositifs permettant d'échanger des données avec l'extérieur du véhicule (Art. 13-1°)		
Finalité(s)	Destinataire(s)	Conditions particulières
Détection - **accidents, incidents,** - **conditions de circulation génératrices d'accidents** **localisés dans l'environnement de conduite du véhicule,** **aux fins de prévention des accidents ou d'amélioration de l'intervention en cas d'accident**	Gestionnaires d'infrastructures routières Forces de l'ordre Services d'incendie et de secours	Agrégation des données sauf celles dont l'agrégation rend impossible leur utilisation pour la détection des accidents et incidents ou des conditions de circulation génératrices d'accidents. Pas d'utilisation des données comme preuve de la commission d'infractions au code de la route
Connaissance de l'infra, de son état, de son équipement	Gestionnaires d'infrastructures routières	
Connaissance du trafic routier	Gestionnaires d'infrastructures routières AOM	

Les évolutions en cours. *Le projet LOM*
Quels accès aux données des véhicules connectés ?

Art. 13-5°. Les **données pertinentes** des véhicules	
Finalité(s)	Destinataire(s)
1) Développement des services liés au véhicule de réparation, de maintenance et de contrôle technique automobiles, d'assurance, et d'expertises automobiles 2) Différents services : gestion de flottes ; distribution de carburants alternatifs (*définis par la directive 2014/94/UE du 22 oct. 2014 sur le déploiement d'une infrastructure pour carburants alternatifs*) ; services innovants de mobilité attachée au véhicule	***Non identifiés*** *[potentiellement identifiables (1)]* Permettre un « ***accès non discriminatoire*** »

Les propositions sont imprécises

Pour les services (2)

Le consentement du conducteur devrait être requis

Le principe de minimisation devra être respecté

La possibilité de refuser l'utilisation des données le concernant pour certaines des finalités visées devrait être possible (=> *refus du service*)

Des précisions dans le texte de l'ordonnance sont particulièrement souhaitables pour garantir les droits des conducteurs

Quelles méthodes pour la protection des données ?

- Des normes, des recommandations, des guides de bonnes pratiques

- L'étude d'impact (RGPD)
- Des processus volontaires (labels, codes de conduite, certifications, …)
- Les packs de conformité sectoriels (assurances ; véhicule connecté) (CNIL)
- L'eCall, un modèle réglementé très élaboré pour la protection des DCP

Quelles méthodes pour la protection des données ? Illustration par l'eCall

Service d'appel aux secours d'urgence

embarqué dans les véhicules

Réglementation communautaire 2015 – 2016

Obligations fortes en matière de protection des données personnelles

1ère application réglementée de la directive ITS (2010)

Cadre pour le déploiement de systèmes de transport intelligents

Règles relatives au respect de la vie privée, à la sécurité et à la réutilisation des informations (art. 10)

Quelles méthodes pour la protection des données ?

Un modèle pertinent

eCall 112

Pas d'échange de données

TPS eCall

Service public d'intérêt général

Information à l'usager
Canevas des informations à fournir pour 112 et autres systèmes en distinguant bien les 2

Parmi les règles techniques
Articulation entre les 2 dispositifs
Choix de l'usager mais obligation de garantir la continuité du service eCall

Services optionnels à valeur ajoutée

Consentement

Obligation légale
31 mars 2018
véhicules M1 / N1

Base légale

Minimisation des données (MSD)
Données visées par EN 15722:2015
+ Contraintes de gestion
ex. effacement automatique et constant
Conservation exclusive des 3 dernières positions

Mesures techniques
4 procédures de vérification
Non traçabilité
Délai de conservation
Suppression automatique et continue
Absence d'échange de données

Source : M. Guilbot.

Merci pour votre attention

Michèle GUILBOT

Directrice de recherche

Ifsttar

Laboratoire Mécanismes d'Accidents

Département Transports – Santé – Sécurité

14-20 Bld. Newton
Cité Descartes
Champs sur Marne
77447 Marne-la-Vallée Cedex 2
Tél. +33 (0)1 81 66 87 29

www.ifsttar.fr
michele.guilbot@ifsttar.fr

Trystan LAURAIRE

Docteur en droit

Enseignant-Résident au Collège universitaire Français de Saint-Pétersbourg

Laboratoire de droit privé et sciences criminelles

3 avenue Robert Schuman
Site Schuman
13629 Aix-en-Provence

Tel.: +33 (0)4 86 91 43 16

lauraireTrystan@gmail.com