Véhicules connectés, communicants. Protection des données personnelles des conducteurs. Cours Ponts Formation Conseil, Paris, 3 juillet 2018

Michèle Guilbot

Institut français
des sciences et technologies
des transports, de l'aménagement
et des réseaux

Véhicules connectés, communicants
Protection des données personnelles des conducteurs

Michèle GUILBOT
IFSTTAR - Département TS2 / Laboratoire MA

IFSTTAR

PONTS FORMATION CONSEIL - Paris – 3 juillet 2018

Sommaire

- Eléments de contexte : un système de circulation routière enrichi par les réseaux de communication et le numérique
- L'identification des personnes physiques,
  un critère central de qualification des données personnelles
- Les bases juridiques de la protection des données personnelles
- Les droits des personnes physiques concernées
- La sécurité du système de circulation routière connecté, un objectif porté par le droit et la technique
- Des méthodes et des outils juridiques pour la conformité et la protection des données personnelles
- Quelques mots sur les responsabilités

1ère partie. Eléments de contexte
Un système de circulation routière enrichi par les réseaux de communication et le numérique

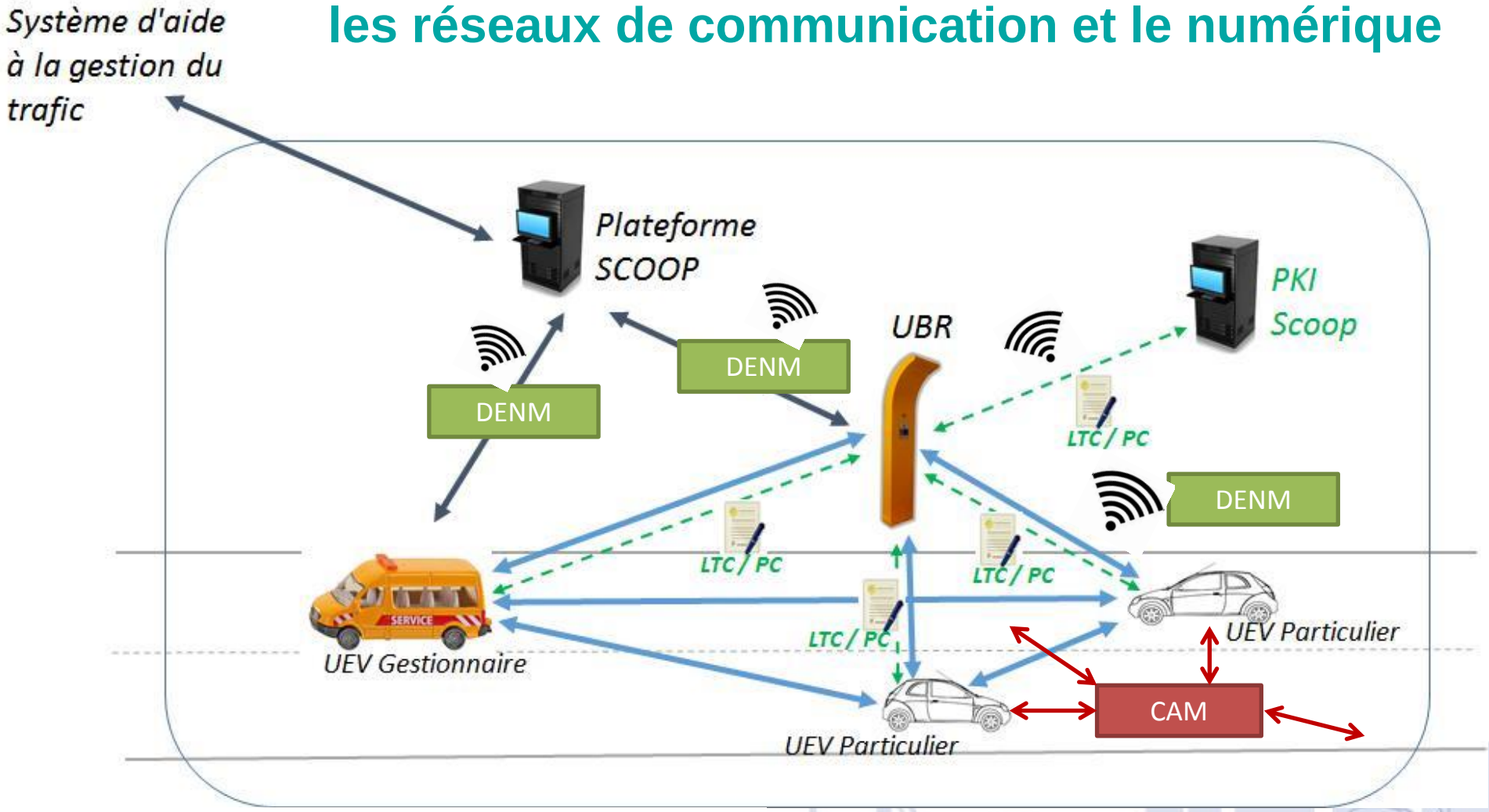


Illustration. Le projet SCOOP en France
Source. Dossier de présentation à la CNIL (2016)

Un système de circulation routière enrichi par les réseaux de communication et le numérique

Des systèmes basés sur le transfert & le traitement de données

- des transferts / échanges de données
  - à l'intérieur du véhicule (capteurs → alertes au conducteur)
  - entre les objets connectés dans les véhicules et des serveurs tiers
  - entre le véhicule et un serveur « centralisé » (ex. « véhicule étendu »)
  - entre les véhicules (V2V), les véhicules et l'infrastructure (V2I)
- en temps réel ou différé, conservées plus ou moins longtemps
  - dans le véhicule et libérées vers l'extérieur en cas de besoin
    - alerte, réparation, maintenance, appel d'urgence,…
  - dans des serveurs internes ou externes ; propriétaires ou tiers
- différentes techniques de connexion et communication
  - réseaux de communication classiques (Wifi, Bluetooth, 3G / 4G,…)
  - bande fréquence dédiée aux systèmes coopératifs (ITS-G5)
  - interne (prise OBD, USB, …)
  - géolocalisation par GPS
- une multiplication des sources
  - des objets connectés intégrés au véhicule par les constructeurs
  - des objets connectés rajoutés par les usagers ou par des tiers
  - les éléments connectés dans le contexte des STI coopératifs

Un système de circulation routière enrichi par les réseaux de communication et le numérique

Multiplication des acteurs impliqués dans le système de circulation routière

- pour collecter et traiter des données nécessaires …
  - positionnement du véhicule, description d'évènements, action sur un élément (ex. freinage, délivrance d'une alerte),…. CAM, DENM, …
- … des données à caractère personnel car potentiellement identifiantes, directement ou indirectement

Multiplication des risques d'atteintes à la sécurité des systèmes et des données dont il faut garantir la disponibilité, la fiabilité, la lisibilité, …

Respect des droits des usagers

Fonctionnement des systèmes

Des éléments pour apprécier les impacts juridiques

Véhicule connecté, communicant, à délégation de conduite, systèmes coopératifs, systèmes de transport intelligents,…

- Différentes finalités assignées aux systèmes
  - améliorer la sécurité des usagers et des agents d'exploitation
  - améliorer la gestion du trafic, l'information routière, ...
  - améliorer le confort des usagers, « *infotainment* »

  → La **finalité** au cœur de la protection des données personnelles

- Différents niveaux : information → délégation de tâches
  - systèmes informatifs ou actifs
  - fourniture de services par des acteurs privés et/ou publics
  - aides à la conduite → délégation partielle de tâches → délégation totale de tâches en certaines circonstances et/ou certains lieux → délégation de l'ensemble de l'activité de conduite

  → Le **rôle des acteurs**, un indice pour imputer les responsabilités

Quelques définitions « officielles »

- Véhicule connecté
  - « Véhicule automobile doté de technologies lui permettant **d'échanger en continu** des données avec son environnement »*
- Système d'aide à la conduite
  - « Système embarqué d'assistance et d'information destiné à faciliter la conduite du véhicule et à la rendre plus sûre »*
- Véhicule autonome
  - « Véhicule connecté qui, une fois programmé, se déplace sur la voie publique de façon automatique sans intervention de ses utilisateurs »*

*Commission d'enrichissement de la langue française. JO, 11 juin 2016

- Véhicule à délégation de conduite
  - référence aux technologies d´automatisation avancées du véhicule et mise en avant du changement fondamental de nature de l'acte de conduite

(L. 17 août 2015 + rapport de présentation, Ord. 3 août 2016 relative aux expérimentations)

2ème partie
L'identification des personnes physiques, un critère central de qualification des données personnelles

L'utilisateur final, l'usager du service, est-il vraiment anonyme ?

Comment le rendre anonyme, peut-il se déplacer -physiquement, virtuellement- de manière anonyme ?

A défaut, comment protéger les données le concernant ?

Qu'est ce qu'une « donnée personnelle ? »

La **possibilité d'identifier une personne physique**,

un critère central pour qualifier 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 2016, entré en application 25 mai 2018)*

Individualisation, corrélation, inférence

Un faisceau d'indices pour analyser le risque d'identification *(G29, 2014)*

Qu'est ce qu'une « donnée personnelle ? »

Sont des données personnelles

- le n° d'identification d'un véhicule (*immatriculation, n° VIN*)
- une adresse IP, même dynamique (*CJUE, 2016 ; C. Cass., 2016*)
- une adresse MAC, même cryptée (*CE, 2017*)
- des données de connexion (*CJUE, 2016, C. Constit., 2017*)
- les messages CAM (*coopérative awareness message, C-ITS*)

Illustrations tirées du Pack de Conformité Véhicule Connecté (CNIL, 2017)

- données techniques liées à l'état du véhicule et des pièces
- donnée liées à l'utilisation du véhicule qui permettent de
  - caractériser des modes de conduite, une action (frein, clignotant, …)
  - détecter des habitudes de déplacement (lieux fréquentés, parcours habituels, …)

Des données particulièrement intrusives

- des données biométriques
- la géolocalisation
- des données permettant de « révéler » une infraction
  - notamment la géolocalisation liée à la vitesse instantanée

La géolocalisation, une donnée personnelle

- Une donnée utile, parfois nécessaire, dans le domaine de la mobilité et des déplacements
  - mais un risque important d'identification
- Une donnée qui relève directement de la protection des données personnelles *(RGPD)*

Les objets mobiles connectés sont « *inextricablement liés aux personnes physiques* » qui en sont les porteurs *(G29, 2011)*

- traçabilité des déplacements
- connaissance des lieux fréquentés (lieux de vie, de travail), des parcours habituels, …
- révélation éventuelle de données sensibles ou considérées comme telles (santé, religion, infraction..)

Collecter et traiter une donnée personnelle ? Comment faire ?

Anonymiser pour empêcher de manière **irréversible** toute réidentification

si cette opération n'est pas possible

- Gestion d'un service d'aide à la mobilité
- Réparation, maintenance
- Facturation
- Recherche scientifique et développement
- Exercice de ses droits par la personne concernée
- Preuve à des fins contentieuses
- ……

des données identifiantes,

une authentification

sont **nécessaires pour la finalité** visée

pour des raisons techniques

Pseudonymiser

et mettre en place des **mesures techniques et organisationnelles** de **sécurité** et de **confidentialité** afin de pouvoir utiliser les données dans le respect des droits des personnes concernées

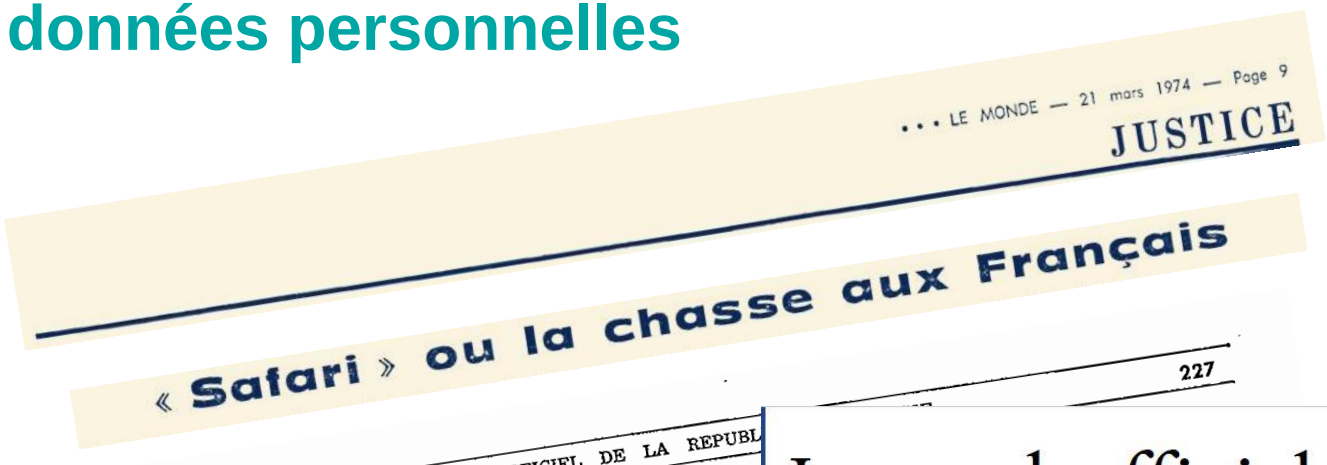
*La donnée **anonymisée** n'est plus personnelle et peut être utilisée librement*

*La donnée **pseudonymisée** reste identifiante :*
elle est soumise aux règles de protection des données personnelles

La pseudonymisation …

- n’est pas obligatoire
- n’est pas une méthode d’anonymisation, elle n’est pas irréversible
  - les données pseudonymisées <u>restent des **données personnelles**</u>
- Il s’agit d’une mesure technique et de sécurité
  - mesure technique de remplacement des données personnelles directement identifiantes par un pseudonyme non-signifiant
    - qui améliore la « protection de la confidentialité des informations à caractère personnel en réduisant les risques de mésusage » (*CNIL, Pack de conformité véhicule connecté, 2017*)
  - mesure de sécurité
    - qui permet la réduction de « la corrélation d’un ensemble de données avec l’identité originale d’une personne concernée » (*G29, 2014*)
- Elle peut être en tension avec d’autres exigences
  - changements trop fréquents ou à des moments inappropriés des certificats pseudonymes dans les véhicules coopératifs et automatisés
    - des risques pour la sécurité routière ?

3ème partie
Les bases juridiques de la protection des données personnelles


... LE MONDE — 21 mars 1974 — Page 9

JUSTICE

« Safari » ou la chasse aux Français

Convention 108

COUNCIL OF EUROPE CONSEIL

7 Janvier 1978 JOURNAL OFFICIEL DE LA REPUBL 227

LOIS

LOI n° 78-17 du 6 janvier 1978
relative à l'informatique, aux fichiers et aux libertés (1).

L'Assemblée nationale et le Sénat ont adopté.
Le Président de la République promulgue la loi dont la teneur suit :

CHAPITRE Ier

PRINCIPES ET DÉFINITIONS

Art.

Journal officiel
de l'Union européenne

L 119

Édition de langue française

Législation

59e année
4 mai 2016

Sommaire

I *Actes législatifs*

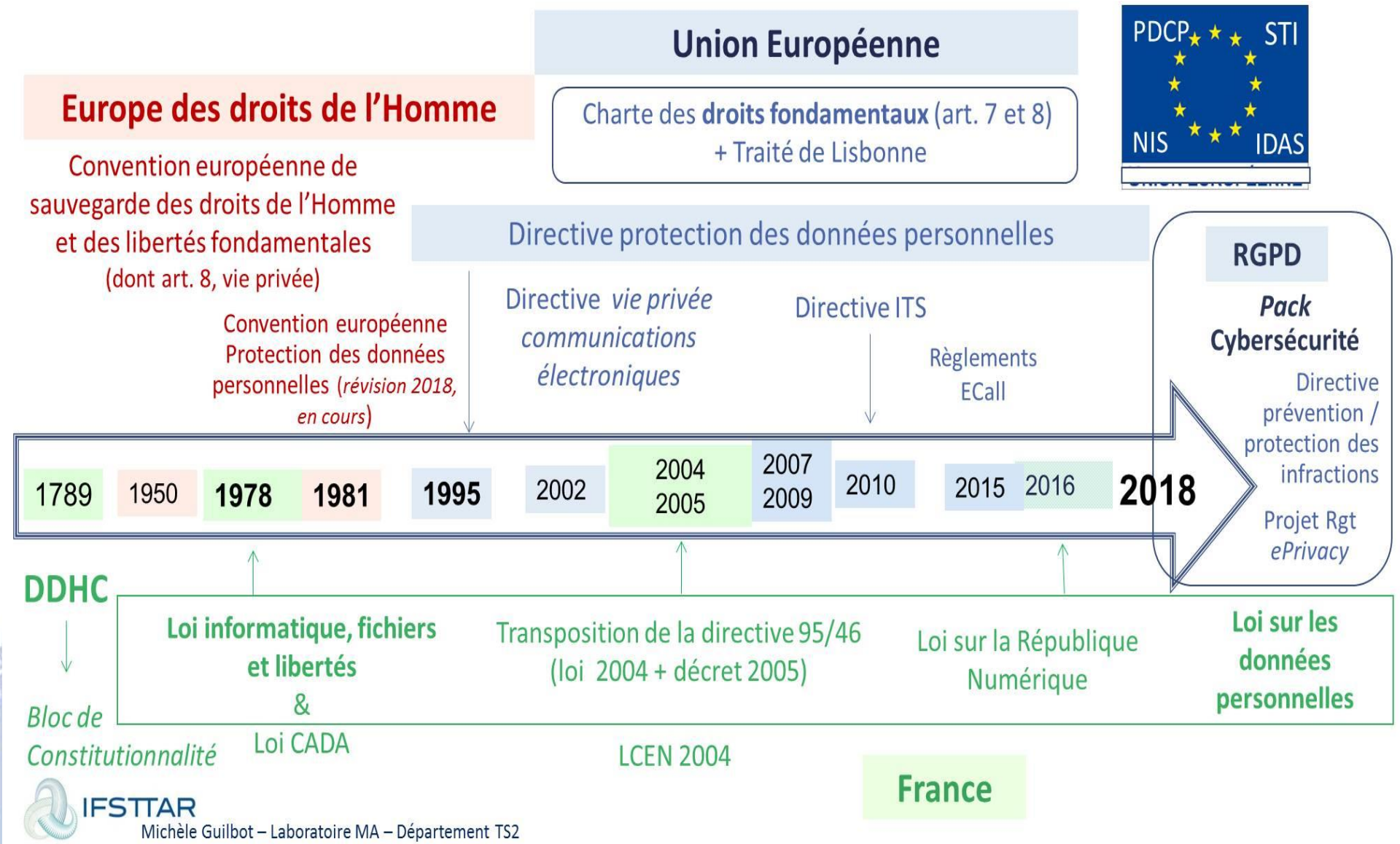
RÈGLEMENTS

★ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (1) 1

31.7.2002 FR Journal officiel des Communautés europ

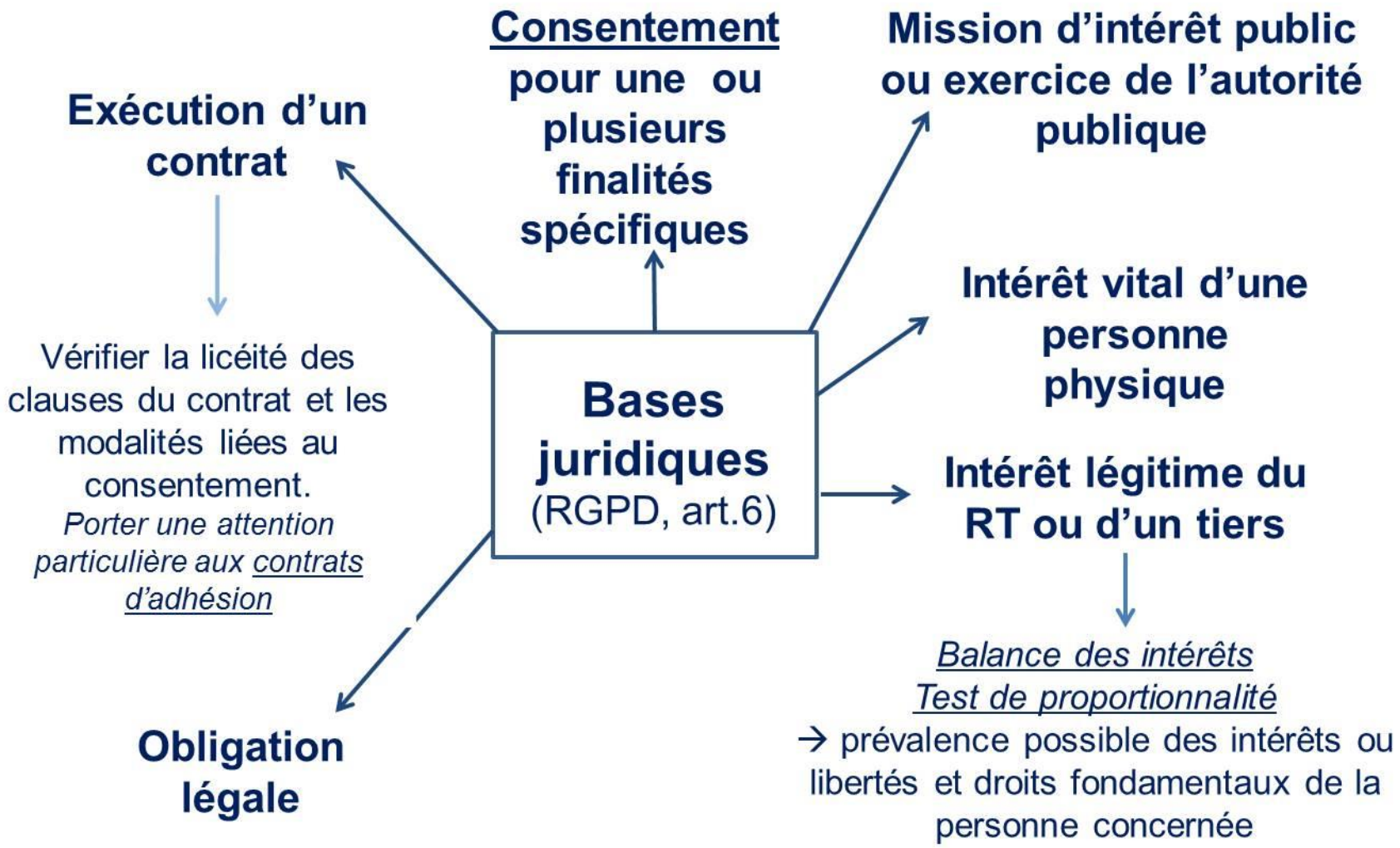
DIRECTIVE 2002/58/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL
du 12 juillet 2002
concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)

Un contexte juridique qui n'est pas spécifique à la France



IFSTTAR
Michèle Guilbot – Laboratoire MA – Département TS2

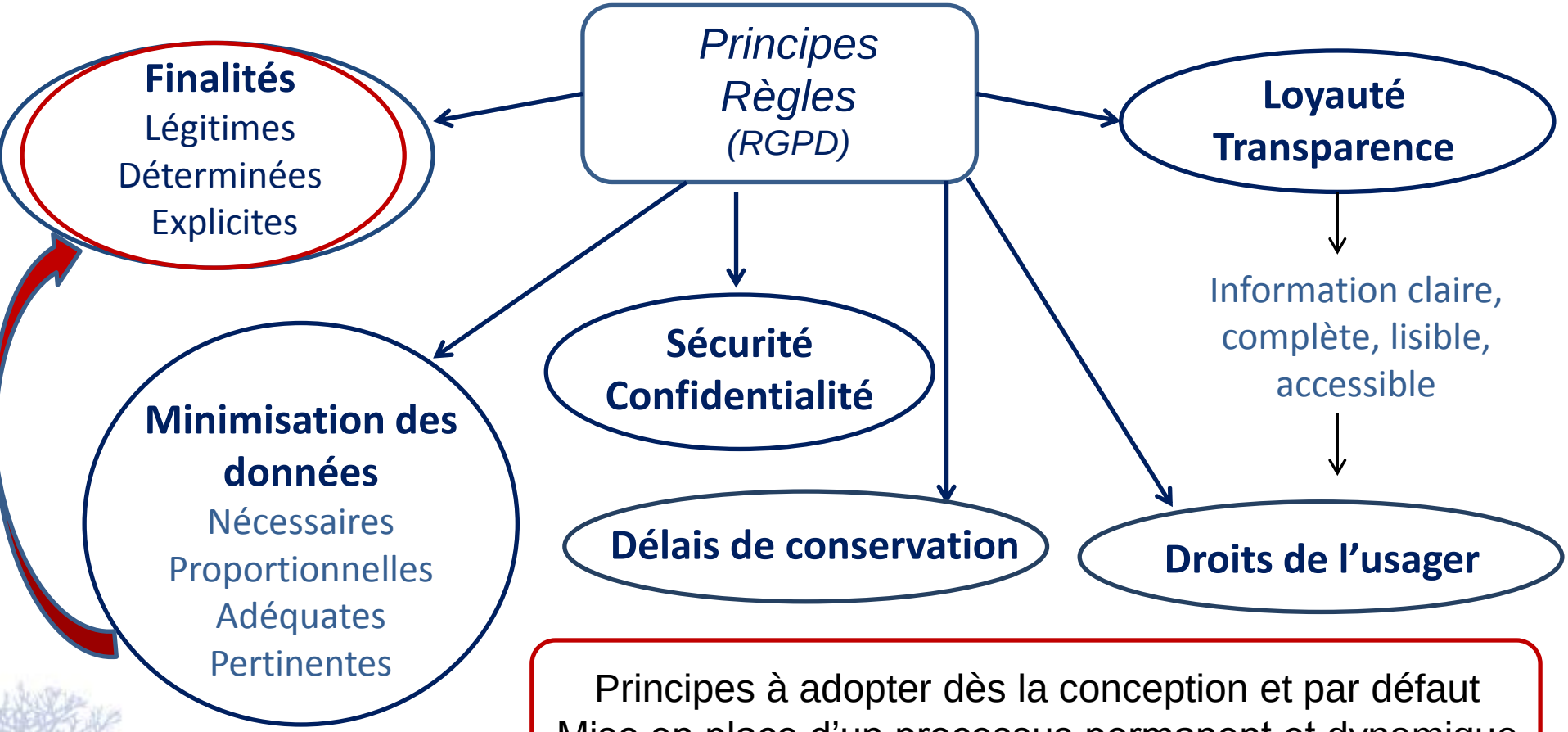
Les bases légales de la collecte et du traitement



Quelle que soit la base juridique, les règles de protection sont applicables

La protection des données à caractère personnel

Règles et principes généraux



Principes à adopter dès la conception et par défaut
Mise en place d'un processus permanent et dynamique

« *Accountability* » → responsabilisation du RT
Documentation des actions menées, preuves des mesures prises

La protection des données personnelles
Illustration par la réglementation ECall

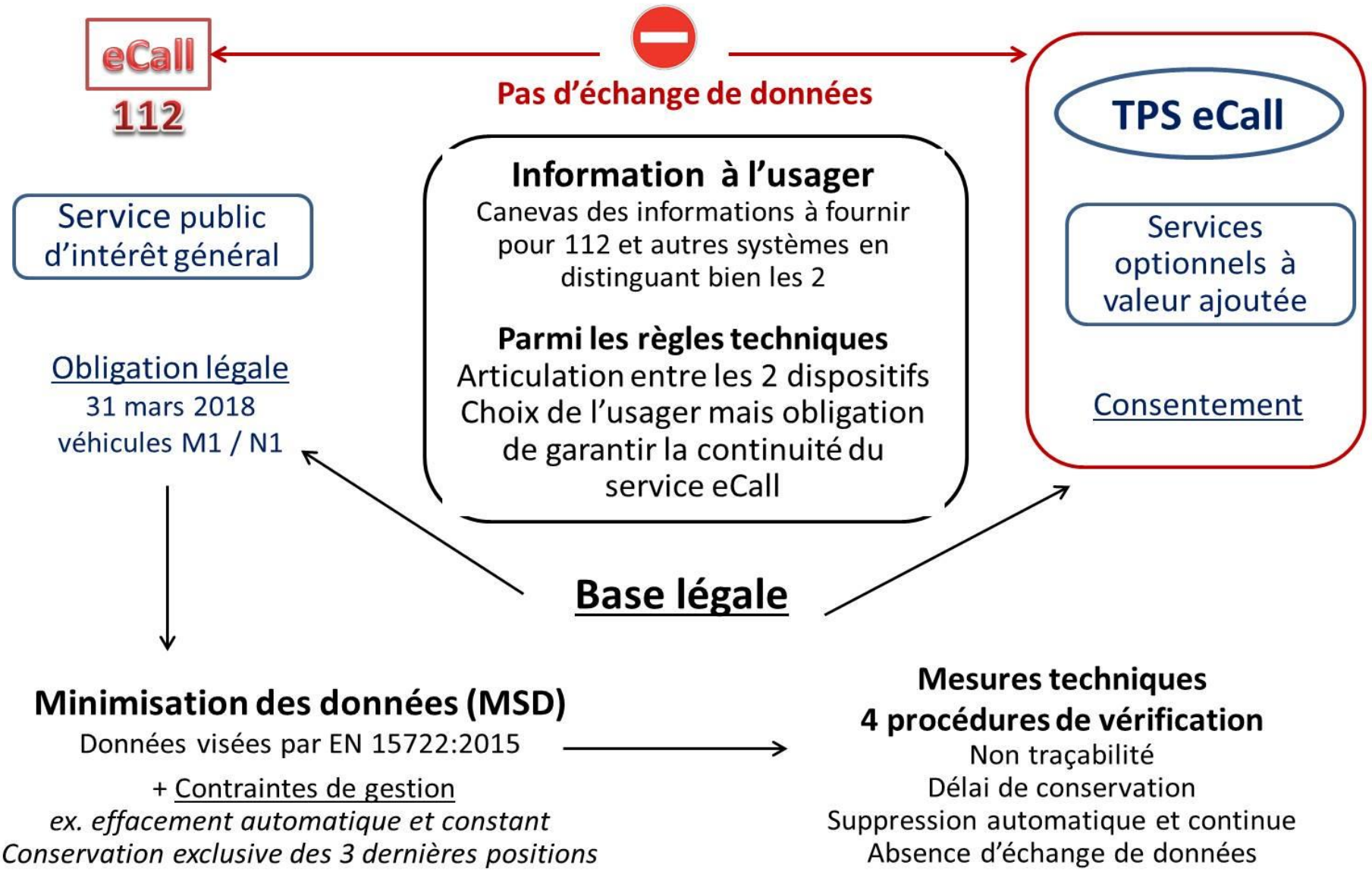
PDCP STI NIS IDA
UNION EUROPÉENNE

DIRECTIVE 2010/40/UE du 7 juillet 2010

cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport

1ère application réglementée

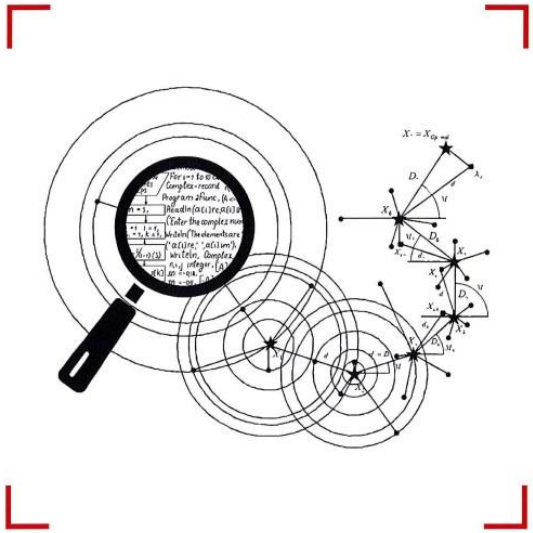
La protection des données personnelles
Illustration par la réglementation ECall



Le principe de minimisation
Illustration. Projets IFSTTAR (S_VRAI & DYMOA)

	Projet S_VRAI/2		Projet DYMOA
Finalité générale	*Etudes d'accidentologie*		
Finalités spécifiques	*Analyse des incidents ou de zones d'intérêt*	*Analyse des enjeux (zones circulées)*	*Observatoire des vitesses*
	Conservation des données dans des fichiers séparés		
Illustrations de mesures prises pour la minimisation	Fréquence de la collecte: 100Hz	Fréquence de la collecte : 1 Hz	Fréquence de la collecte : 1Hz
	Conservées uniquement en cas d'incident ou de passage sur la zone, entre les 30 sec. avant et les 15 sec. après	Collecte sur l'ensemble des parcours mais pas de possibilité de lien entre les véhicules et les traces GPS (id. véhicule ne figure pas dans le fichier)	Collecte sur l'ensemble des parcours Seules la vitesse et la géolocalisation figurent dans le fichier (id. véhicule et boitier ne figurent pas dans le fichier)
	Pas d'évènement = effacement automatique dans le boitier		
	Incident et géolocalisation : limitation temporelle de la « fenêtre de collecte »		

Illustration du principe : données « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* » (art. 5 RGPD)



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

4ème partie
Les droits des personnes physiques concernées

... LE MONDE — 21 mars 1974 — Page 9

JUSTICE

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

Données personnelles

→ attributs de la personnalité (UE) vs/ biens de consommation (EU)

La protection intégrée de la « vie privée »

– Concept élaboré dans les années 1990

- Mise en œuvre en combinant trois catégories d'applications
  - aux systèmes informatiques
  - dans les pratiques
  - dans la conception des systèmes d'information et de l'architecture des réseaux

(*Commissaire à l'information et à la protection de la vie privée de l'Ontario, 2009, mod. 2011*)

– Les 7 principes fondamentaux

- Mesures **proactives** (et non réactives) ; mesures **préventives** (et non correctives)
- Protection **implicite** de la vie privée
- Protection **dès la conception** des systèmes et des pratiques
- Fonctionnalité **intégrale**
- Sécurité de **bout en bout**
  - durant toute la période pendant laquelle les données sont conservées)
- **Visibilité** et **transparence**
- Axer les mesures sur **l'intérêt des utilisateurs**

La protection des données personnelles
Les droits des personnes physiques concernées

- Droit à ne pas être connu, reconnu, tracé, dans ses déplacements
  - risques liés à la géolocalisation
  - risques liés à la traçabilité numérique, des actions, des habitudes, ..
  - risques liés aux interconnexions de fichiers, aux associations de données
- Droit à une information claire et accessible
  - sur les finalités, les données collectées, les modalités de traitement, les destinataires des données
- Droit à consentir (sauf autre base légale)
- Droits d'accès, et selon les cas, d'opposition, de rectification, d'effacement (*droit à l'oubli*)
- Droit à la portabilité des données (*RGPD*)

Creuser le concept de décision individuelle produisant des effets juridiques ou affectant la personne de manière significative, prise sur le fondement d'un traitement automatisé

La protection des données personnelles

Consentement et autodétermination informationnelle

*Consentement **

- Libre
- Éclairé
- Spécifique
- Univoque
- Réel (preuve)

→ impose la délivrance d'une **information** claire et précise par le responsable de traitement

→ la collecte de la géolocalisation doit faire l'objet d'un consentement distinct

** sous réserve autres bases légales*

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

5ème partie
La sécurité du système de circulation routière connecté, un objectif porté par le droit et la technique

Anticiper les risques potentiels,
Mettre en application les nouvelles réglementations

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

(Guillaume Poupard, Pdt ANSSI, nov. 2016)

La sécurité du système de circulation routière connecté, un objectif porté par le droit et la technique

La faille de sécurité
- un risque à anticiper dans un univers connecté
- une source de responsabilités

Exemples de risques

- 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. système coopératif et déni de service sur le système de gestion du trafic des gestionnaires de voirie
- prise en main du contrôle par un tiers
  - d'un élément du système, d'une tâche, …
  - d'une activité (ex. gestion du trafic routier)

Dessin : J.Yerpez

La sécurité du système de circulation routière connecté, un objectif porté par le droit et la technique

La réglementation technique

La normalisation

ne couvrent pas toujours la sécurité informatique d'un système de circulation routière connecté et communicant

- pas de processus de certification obligatoire
- pas de réglementation visant directement la cybersécurité du véhicule et de l'infrastructure connectée et communicante
- des nouvelles compétences à intégrer dans l'industrie automobile et les services de gestion de la voirie pour garantir la sécurité des systèmes

Les produits et services délivrés par des personnes privées	**constructeurs automobiles, fournisseurs de services numériques, opérateurs de services essentiels**
Les ouvrages publics connectés	Gestionnaires publics
Les réseaux de communications	Opérateurs des réseaux de communication
Les serveurs et les terminaux	Hébergeurs et gestionnaires des données
Autres .. (dont sous- traitants des opérateurs publics et privés)	

La sécurité du système de circulation routière connecté, un objectif porté par le droit et la technique

Multiplication des risques d'atteintes
à la sécurité des systèmes et des données
dont il faut assurer la disponibilité, l'intégrité, la fiabilité, la lisibilité, …

le fonctionnement des systèmes → Cybersécurité

le respect des droits des personnes physiques → Protection des données personnelles

Mesures de sécurité pour le **fonctionnement des systèmes**

Réglementation communautaire
→ construction d'un **droit de la cybersécurité**

Mesures de sécurité pour la **protection des données personnelles**

RGPD, art. 32

Loi Informatique et Libertés, art. 34

La sécurité du système de circulation routière connecté, un objectif porté par le droit et la technique

Nombreux travaux de normalisation en cours, pour la sécurité du véhicule connecté, communicant

Véhicules terrestres à moteur *(ISO / SAE..)*

STI coopératifs *(ETSI et C-ITS , ISO …)*

ECE-ONU

Proposition d'un texte pour la protection des données et la cybersécurité *(mars 2017)*

→ Réglementation technique internationale des véhicules ?

Quelle articulation, quelle cohérence entre les normes ?
Quid de l'indépendance dans les processus de normalisation ?
Echéance pour intégrer la cybersécurité dans la réglementation des véhicules ?

La « règle » de sécurité, un préalable indispensable pour prévenir les risques et cerner les responsabilités

- Les « règles » concernant la sécurité …
  - des produits et services
    - véhicules et leurs équipements, équipements routiers,
    - autres « objets » …
- … de nature et de portée variables
  - générales ou particulières
  - législatives ou réglementaires
  - portées par des normes, intégrées ou pas à la réglementation
  - obligatoires ou facultatives
  - diffusées par des connaissances techniques ou scientifiques

Les caractéristiques de la « règle » de sécurité
ont un impact sur les responsabilités

Leur caractère facultatif n'exclut pas des mises en cause

6ème partie
Des méthodes et des outils pour la conformité et la protection des données personnelles

- **L'étude d'impacts** *(RGPD)*
- Des normes (*à valeur réglementaire ou pas selon les cas*)
- Des recommandations, des guides de bonnes pratiques, …
- Des processus volontaires (labels, codes de conduite, certifications, …)
- Des référentiels → **Pack de conformité véhicules connectés**

enisa European Network and Information Security Agency

DÉCLARATION COMMUNE DES AUTORITÉS EUROPÉENNES DE PROTECTION DES DONNÉES RÉUNIES AU SEIN DU GROUPE DE L'ARTICLE 29

ISO

cen

ETSI World Class Standards

Comité européen pour la protection des données *(RGPD)*

ANSSI Agence nationale de la sécurité des systèmes d'information

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Outils et méthodes pour la protection des données personnelles

Des étapes pour la conformité

Recommandations CNIL pour un processus de mise en conformité efficient

1. • Désigner un pilote
   • DPO
2. • Dresser une cartographie des traitements envisagés
   • rescensement des traitements
   • tenue d'un registre
3. • Identifier et prioriser les actions à mener pour chaque traitement
4. • Mener l'analyse d'impact sur la protection des données personnelles
5. • Déployer des procédures internes pour garantir la protection des données
   • Protection dès la conception et par défaut
6. • Documenter les actions menées pour garantir la conformité

Outils et méthodes pour la protection des données personnelles

L'étude d'impact (1)

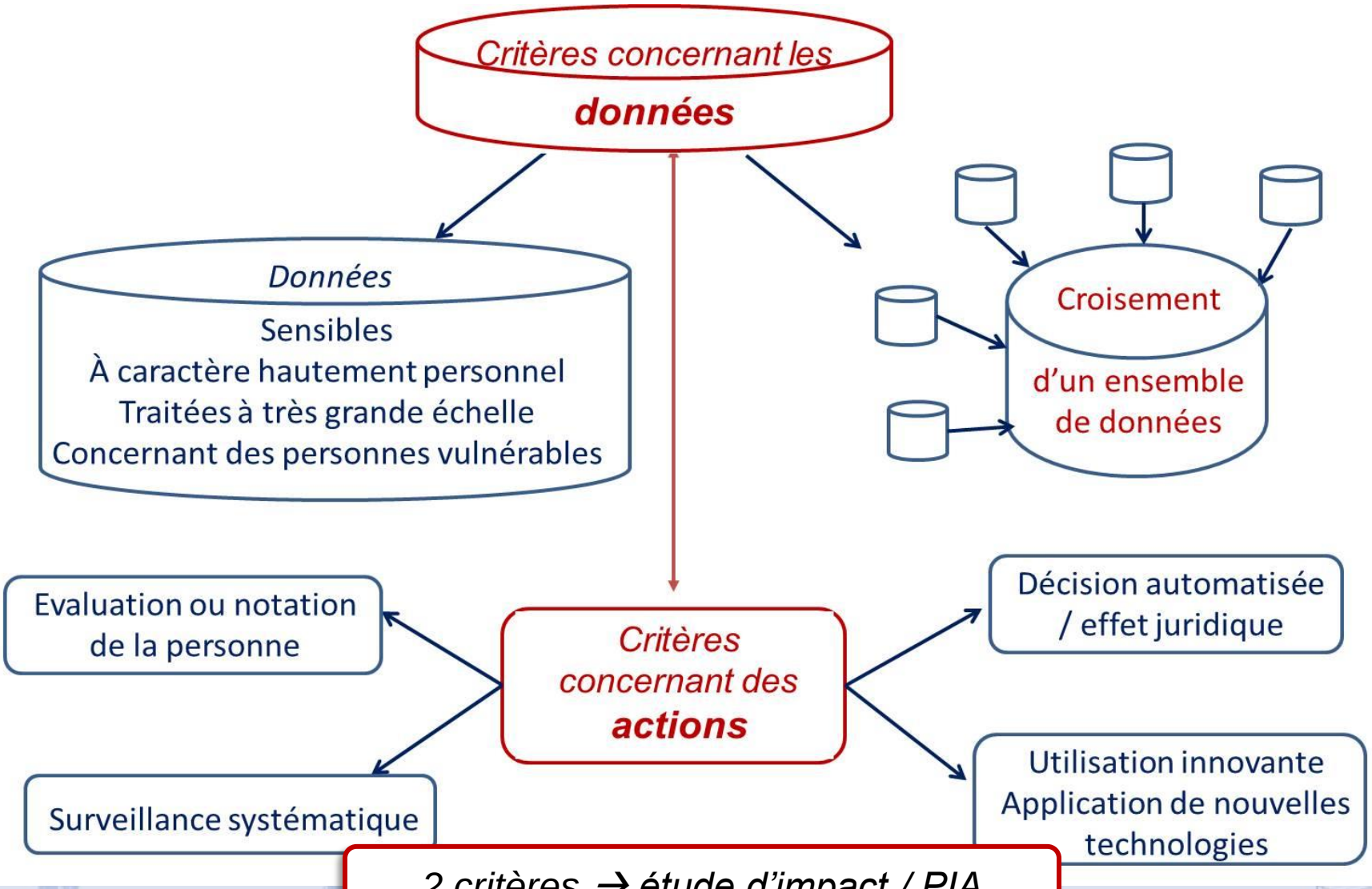
Méthodologie (G29, 2017)

1. Décrire le traitement
2. Evaluer sa nécessité et sa proportionnalité
3. Evaluer sa conformité
4. Evaluer les riques, du point de vue des personnes dont les données sont traitées
5. Déterminer les mesures à prendre pour limiter les risques
6. Documenter ce processus
7. Suivre en permanence et réexaminer ponctuellement la conformité du traitement

Outils et méthodes pour la protection des données personnelles

L'étude d'impact (2)

Les lignes directrices du G29



2 critères → étude d'impact / PIA

Outils et méthodes pour la protection des données personnelles

L'étude d'impact (3)

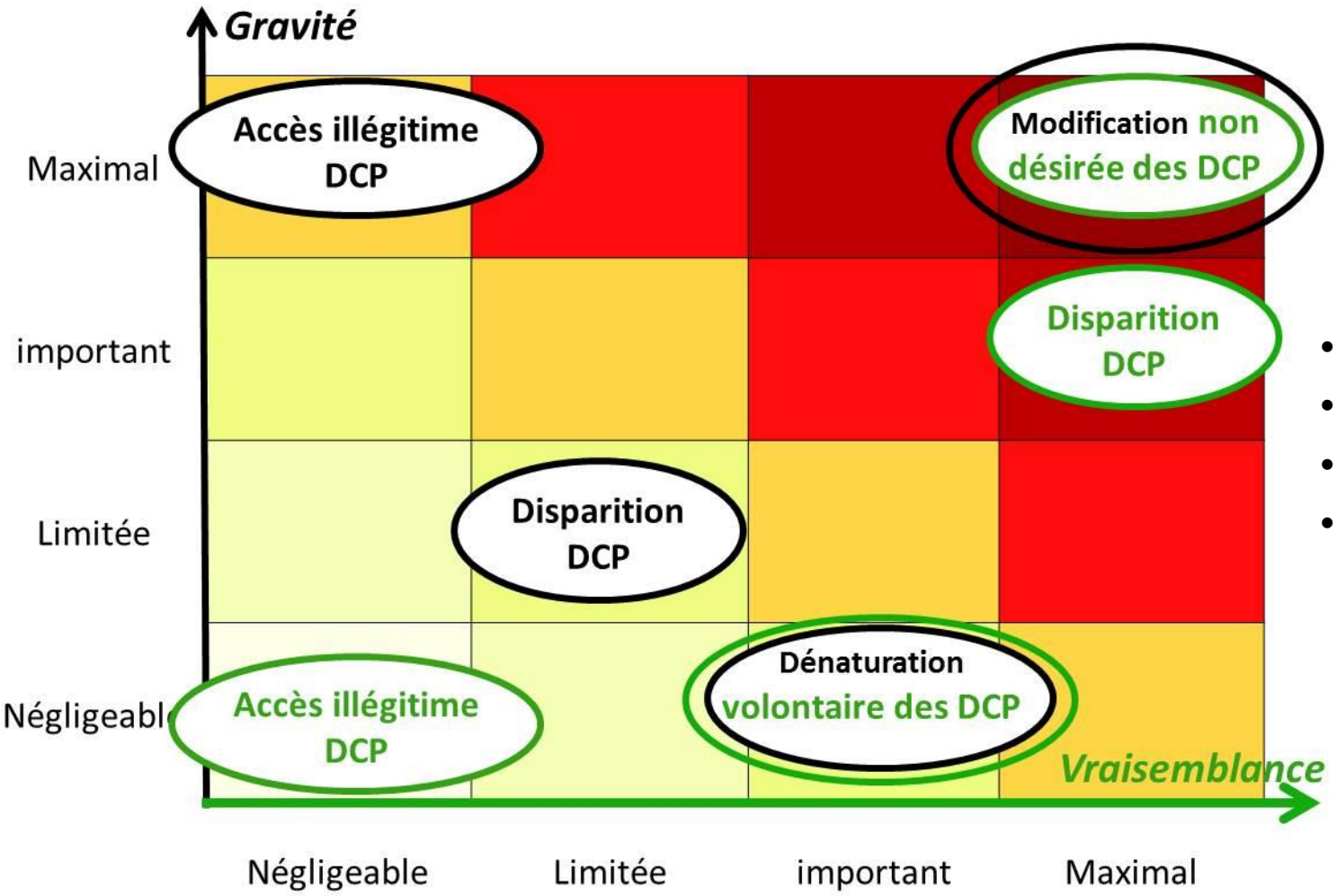
Critères du G29, illustration

Exemples de catégories de données impliquant l'application de la méthode	Exemple d'illustration par le G29
– données sensibles – données concernant des personnes vulnérables – transfert de données hors UE – traitement à grande échelle – le scoring	Recours à un système de caméras pour surveiller les comportements routiers avec pour finalité d'utiliser l'analyse vidéo intelligente pour isoler les véhicules et reconnaitre les plaques d'immatriculation automatiquement *(obs. illustration en France : le système LAPI)*. Recommandations du G29 pour cet exemple : examiner les critères suivants pour déterminer si une AIPD/PIA est requise : - le traitement engage une surveillance systématique, - le traitement met en œuvre une utilisation innovante ou l'application de solutions technologiques ou organisationnelles.

Outils et méthodes pour la protection des données personnelles

L'étude d'impact (4)

L'évaluation du risque
(d'après CNIL, Outillage du PIA)



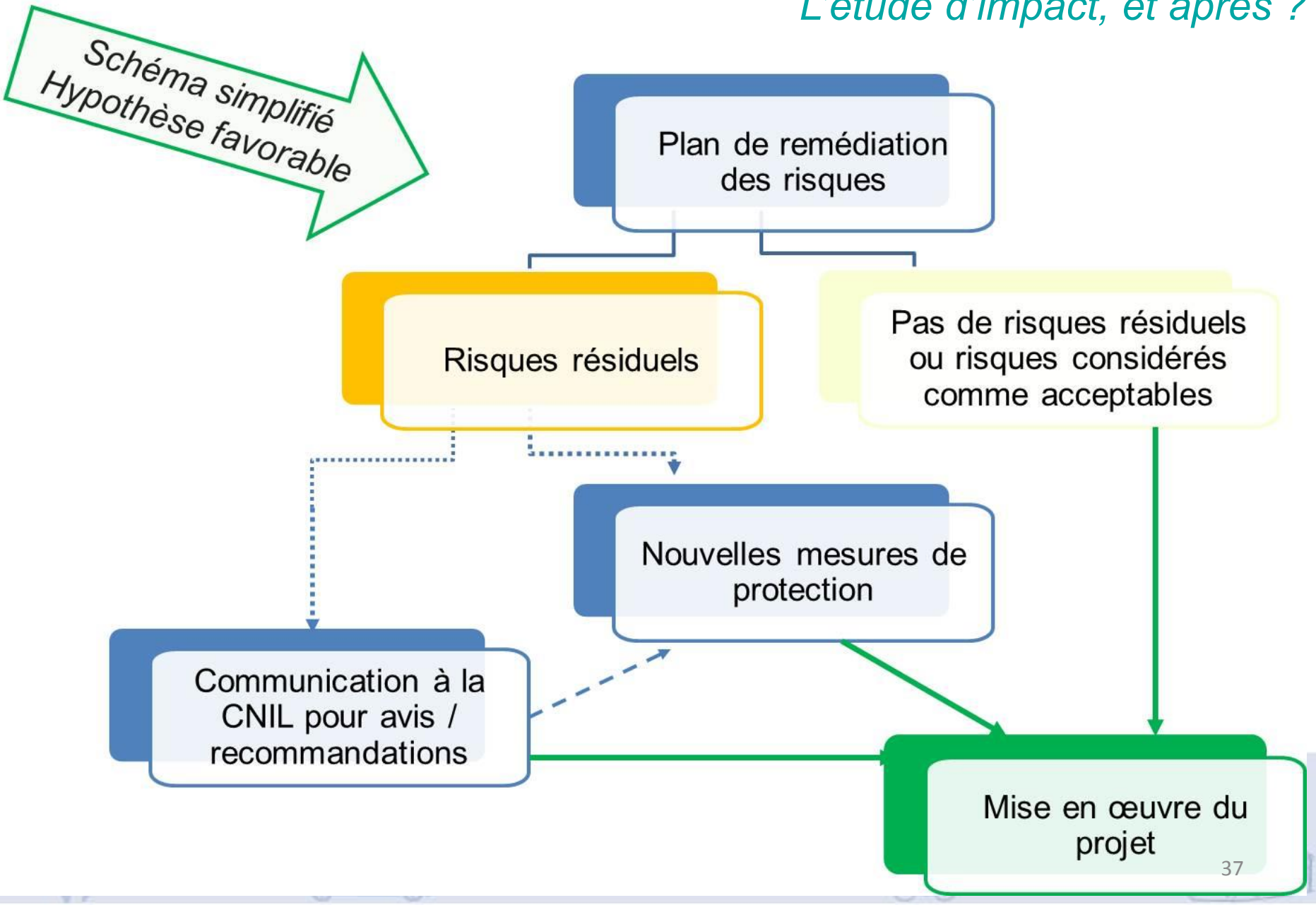
4 critères concernant les données

- Disponibilité
- Intégrité
- Confidentialité
- Traçabilité des actions sur les données

https://www.cnil.fr/fr/PIA-privacy-impact-assessment

Outils et méthodes pour la protection des données personnelles

L'étude d'impact, et après ?



Outils et méthodes pour la protection des données personnelles

Le pack de conformité véhicule connecté

Des lignes directrices pour une utilisation responsable des données dans les prochaines générations de voitures

	Scenario 1 « IN-IN »	**Scenario 2 « IN-OUT »**	**Scenario 3 « IN-OUT-IN »**
Circuit des données	Les données personnelles demeurent à l'intérieur du véhicule Pas de transmission à un tiers Certaines données peuvent sortir du véhicule via une application directement gérée par l'usager sur un objet connecté qu'il a lui-même embarqué.	Transmission à un tiers pour la fourniture de service(s) à l'usager.	Transmission des données à l'extérieur du véhicule et Retour de la donnée dans le véhicule afin de déclencher une action.
Exemples	Eco conduite	Exploitation commerciale consentie par l'usager sur une base contractuelle (type *Pay as you drive*) Lutte contre le vol Ecall (112)	Système de navigation dynamique permettant de renvoyer les informations en direct sur l'état d'encombrement des routes afin de calculer un nouvel itinéraire

https://www.cnil.fr/sites/default/files/atoms/files/pack_vehicules_connectes_web.pdf

Outils et méthodes pour la protection des données personnelles

La cartographie S_VRAI

Illustration S_VRAI/2 (extrait de la cartographie)	Fréquence (Hertz)	Table de correspondance	Base nominative	Base EMMA (accès exclusif équipe IFSTTAR)				Base incidents			
		accès limité (v. dossier CNIL)						IFSTTAR (équipe traitement des données) Partenaire 1 (équipe traitement des données) Sous traitant 1			
	ND: non disponible pour la présentation			fichier évènements (1 ligne / déclenchement)	incidents ou zones d'intérêt	traces GPS	observatoire des vitesses	fichier évènements (1 ligne / déclenchement)	incidents ou zones d'intérêt	traces GPS	observatoire des vitesses
Conducteur *											
Nom, prénom		oui	oui								
Organisme		oui	oui	oui	oui	oui	oui	oui	oui	oui	oui
Coordonnées professionnelles		oui	oui								
Sexe**		oui	oui								
date obtention permis**		oui	oui								
Km annuel parcouru les 3 dernières années**		oui	oui								
Année de naissance**		oui	oui								
Véhicule											
Id véhicule		oui		oui	oui	oui		oui	oui		
Id Boitier		oui		oui	oui			oui	oui	oui	
Marque		oui									
Modèle		oui									
Année du véhicule		oui									
Cylindrée		oui									
Présence de divers ADAS (liste masquée)		oui									
Km à l'installation du boitier		oui	oui								
Km à la désinstallation du boitier		oui	oui								
Données capteurs du boitier											
Horodatage				oui	oui	oui		oui	oui	oui	
Pas de temps	ND				oui	oui	oui		oui	oui	oui
Accélérations en X, en Y et en Z	ND			oui	oui		oui	oui	oui		oui
Vitesses angulaires X, Y et Z	ND			oui	oui			oui	oui		
Position et altitude GPS	ND			oui	oui	oui	oui	oui	oui	oui	oui
Vitesse GPS instantannée	ND			oui	oui		oui	oui	oui		oui
Autre(s) donnée(s) [...]	ND				oui	oui			oui	oui	
Données issues du CAN											
(masqué pour la présentation)	ND				oui				oui		
Vidéo											
images floutées	ND				oui				oui		

(*) (1) en toute hypothèse, un consentement écrit des personnes est exigé - (2) la désactivation par le conducteur est toujours possible

(**) si la personne fournit l'information

7ème partie
Quelles responsabilités en cas d'atteintes aux droits des personnes physiques ?

Dessin. J. Yerpez. Prédit 3 – Kissifrot

Des responsabilités, pour quoi faire ?

- Indemniser les victimes
  - Responsabilité civile
    - Personnes morales de droit privé
    - Personnes physiques
  - Responsabilité administrative
    - Etat, collectivités territoriales, … (*ex. gestionnaires d'ouvrages publics*)
  - *Rôle des assureurs*
- Sanctionner une faute : responsabilité pénale*
  - en cas d'accident
    - → imprudence, négligence, non respect des règles, éventuellement mise en danger d'autrui
  - pour non respect des règles relatives aux traitements des données et à la protection des droits des personnes concernées

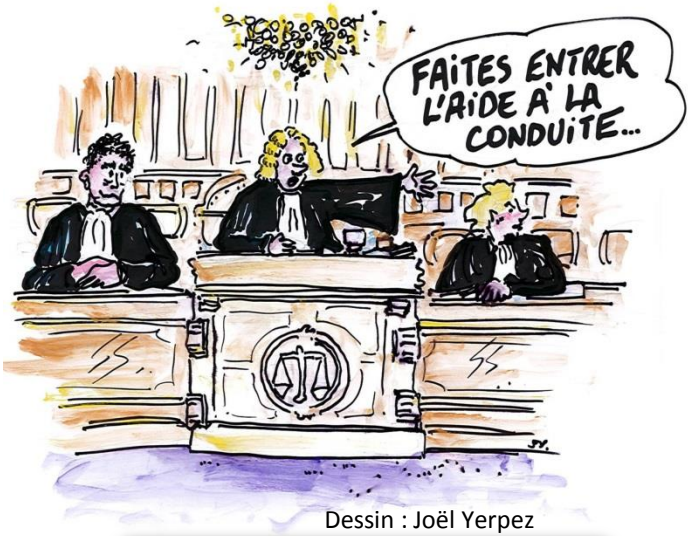
(*) RP : sauf Etat et collectivités territoriales pour activités susceptibles de faire l'objet d'un DSP

La protection des données à caractère personnel
Non respect des mesures et responsabilités

Elargissement du cercle des parties prenantes dans le système de circulation routière

diversité des responsables de traitement et des sous-traitants

- concepteurs d'un élément, programmeurs de logiciels, …
- Fabricants de produits
- fournisseur de services
- opérateurs impliqués dans la transmission des données (en distinguant selon leur mission (gestion du réseau ou fourniture d'autres services)
- hébergeurs de données
- constructeurs automobiles
- gestionnaires de la voirie connectée
- …



Dessin : Joël Yerpez

Dresser une cartographie des parties prenantes

Etre rigoureux sur les cadres contractuels

Bien déterminer en amont les missions, les pouvoirs, les moyens, de chaque acteur

La protection des données à caractère personnel
Non respect des mesures et responsabilités

Responsabilité pénale* *(c. pénal, art. 226-16 et s.)*

Non respect des règles relatives aux traitements des données personnelles, par ex.

- procéder ou faire procéder à un traitement sans mettre en œuvre les mesures de sécurité prescrites
- collecter des données personnelles par moyen frauduleux, déloyal ou illicite

La négligence est un élément constitutif de l'infraction

Autorités de régulation et de contrôle

- enquêtes, mises en demeure
- sanctions administratives *(RGPD)*
  - selon les violations
    → jusqu'à 20 millions d'euros ou 4% maximum du chiffre d'affaire mondial de l'entreprise

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

mais aussi

- développement d'outils et méthodes pour la protection des données, rédaction de guides méthodologiques, …
- conseils et accompagnement préalables à la mise en œuvre d'un traitement, notamment en lien avec le DPO

La protection des données personnelles

L'action de groupe

- Création de l'action de groupe pour la protection des données personnelles

  (*loi « modernisation de la justice 21ème siècle », 2016)*

- Action en « manquement » (2016) et en « réparation » (2018)
  - interruption de la collecte et du traitement
  - élargissement de l'action à la réparation → loi « données personnelles » (*art. 25*) (*élargissement permis par le RGPD, laissé à l'appréciation des Etats)*
- Peuvent exercer l'action
  - associations ayant pour objet la protection de la vie privée et des données personnelles, déclarées depuis au moins 5 ans
  - associations de défense des consommateurs si le traitement de données affecte des consommateurs
  - syndicats (salariés, fonctionnaires)
- Devant un juge judiciaire ou administratif

En guise de conclusion

Un contexte juridique favorable à une innovation placée sous la responsabilité des acteurs

- Une réponse <u>organisationnelle</u>
  - Désigner un DPO, identifier les acteurs, notamment
    - le responsable du traitement et ses partenaires
    - les sous-traitants, prestataires (conception, maintenance, réparation, …)
      - définir leurs missions respectives
      - prendre des dispositions contractuelles intégrant sécurité et confidentialité
    - la localisation et les conditions d'hébergement des données
    - le régime juridique applicable (territorialité)
  - clarifier et renforcer l'information de l'usager
- Développer des <u>outils technologiques</u> pour la protection
  - dès la conception, par défaut et de manière dynamique
  - en utilisant les outils proposés pour
    - mettre en place et contrôler les mesures de sécurité (réseaux, serveurs, terminaux et objets connectés au système, transfert des données)
    - gérer les accès aux données (habilitations, authentifications)

En guise de conclusion

2018 : un droit communautaire plus adapté aux nouvelles technologies

- Les mesures imposées *(réglementation)*
- ou recommandées *(normes, guides, …)*
- … sont autant de méthodes, d'outils permettant de
  - garantir la cybersécurité des systèmes
  - protéger les données personnelles des usagers
- en mettant la technologie au service de la sécurité et de la confidentialité des données

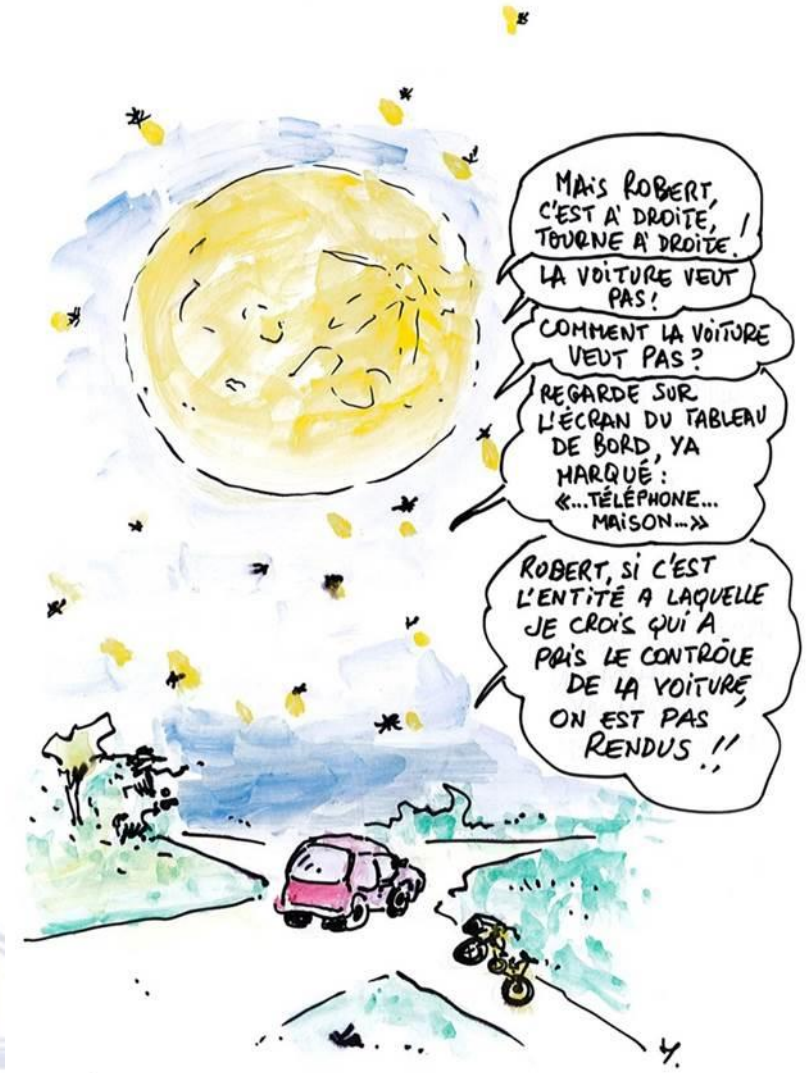
Utiliser le droit comme outil méthodologique pour garantir les droits des personnes et générer la confiance de l'utilisateur

Merci de 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
France
Tél. +33 (0)1 81 66 87 29
www.ifsttar.fr
michele.guilbot@ifsttar.fr



Dessin : Joël Yerpez