Protection des données personnelles dans un univers connecté

Michèle Guilbot

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

Protection des données personnelles dans un univers connecté

Michèle GUILBOT
Directrice de recherche
IFSTTAR - Département TS2 / Laboratoire MA

IFSTTAR

Champs-sur-Marne – Master Créacity - 16 mars 2018

Ville connectée, mobilité connectée
Données personnelles des usagers

Données personnelles

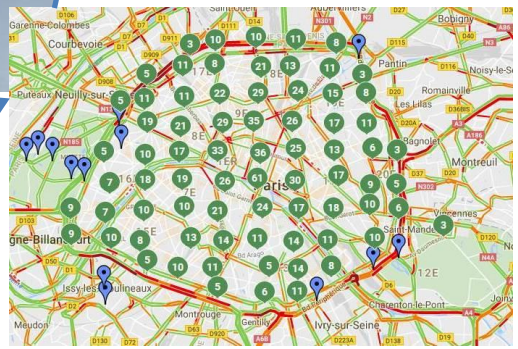
Faille de sécurité
Mise en demeure par la CNIL (déc. 2017)

Fourniture de services

Juillet 2017

Surveillance

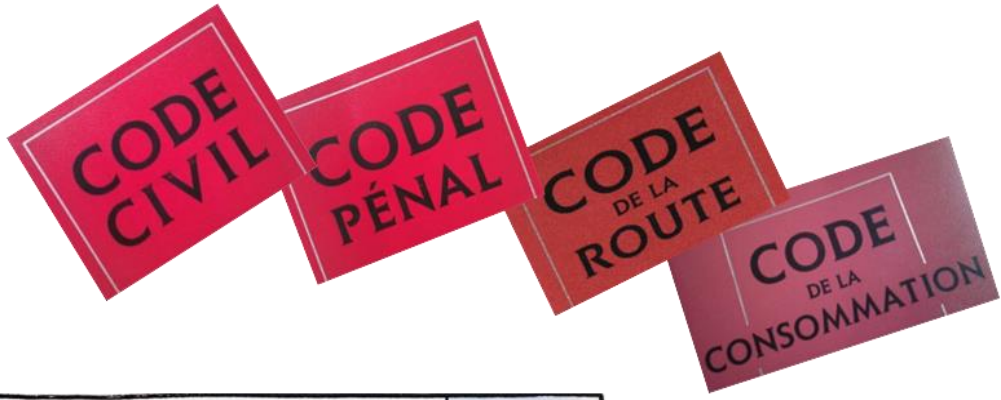
Gestion intelligente des déchets



Données non personnelles

Sources du schéma : LINC / CNIL (R. Le Chatellier) ; (L. Von Zoonen, 2016)

Ville connectée, mobilité connectée
Aspects juridiques



Responsabilité civile

Responsabilité du fait des produits défectueux

Responsabilité administrative

Responsabilité pénale

Dessin : Joël Yerpez. TS2/LMA Kissifrot - Prédit 3

Droits européens

Réglementation technique

Obligations de sécurité

Obligations de conformité

.....

Protection des données personnelles et de la vie privée

Ville connecté, mobilité connectée
Protection des données personnelles des usagers

Sommaire

- Données personnelles (notion, anonymisation, pseudonymisation)
- Les bases juridiques de la protection des données personnelles
- Les obligations des responsables de traitement et de leurs partenaires ; les grands principes à respecter
- La sécurité des objets connectés / communicants
- Des méthodes et des outils juridiques pour la conformité et la protection des données personnelles
- Les droits des personnes concernées
- Quelques mots sur les responsabilités

1ère partie
L'identification des personnes, un critère central de qualification des données personnelles

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

Comment le rendre anonyme ou, à défaut, protéger les données le concernant ?

La protection des droits de la personne physique ne se limite pas à celle de la donnée personnelle

notamment

- La 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

- La 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 »

La notion de « donnée à caractère personnel »

Critère central → possibilité d'identifier une personne physique

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, entrée en application 25 mai 2018*)

La notion de « donnée à caractère personnel »

Identification directe	**Nom, date de naissance, NIR, … n° IP, adresse MAC, n° VIN …**
Identification indirecte	pseudonyme, association de données …
La pseudonymisation n'est pas l'anonymisation	
Sont des données personnelles • une adresse IP, même dynamique (CJUE, 2016 ; C. Cass., 2016) • une adresse MAC, même cryptée (CE, 2017) • la localisation	
Prendre en compte le risque de ré-identification par individualisation, corrélation et inférence (*G29, 2014*)	

La géolocalisation, un risque majeur d'identification

– La géolocalisation
  - est une donnée identifiante
  - qui relèvera directement de la protection des données personnelles (*RGPD, 25 mai 2018)*

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

  - traçabilité des déplacements
  - connaissance des habitudes, des comportements (lieux fréquentés, achats, conduite)
  - révélation éventuelle de données sensibles (santé, religion,..)

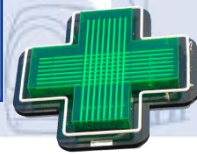


Illustration : la donnée personnelle dans le véhicule connecté

- Les illustrations du pack de conformité (CNIL, 2017)
  - données de géolocalisation
  - données techniques liées à l'état du véhicule et des pièces
  - données biométriques du conducteur
  - données liées à l'utilisation du véhicule par le conducteur/les occupants → par ex. les données qui permettent :
    - de caractériser le mode de conduite:
      - action sur le frein, sur le clignotant, activation et utilisation d'une aide ou pas, …
    - de détecter les habitudes de déplacements:
      - lieux fréquentés, parcours habituels, ...

- L'exemple du message CAM dans les C-ITS

L'anonymisation : impossibilité absolue de réidentifier la personne concernée par les données

- « résultat du traitement des données personnelles afin d'empêcher, de façon irréversible, toute identification »

  (*G29, Les techniques d'anonymisation , 2014)*

- « données rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable » (*RGPD, considérant 26*).

« Processus par lequel des informations personnellement identifiables (IPI) sont *irréversiblement altérées* de telle façon que le sujet des IPI ne puisse plus être identifié directement ou indirectement, que ce soit par le responsable du traitement des IPI seul ou en collaboration avec une quelconque autre partie. » *(ISO 29100*)

→ La donnée anonymisée n'est plus personnelle

Individualisation, corrélation, inférence ***:*** 3 critères cumulatifs permettant de caractériser l'identification, base d'une méthodologie *a contrario* (*G29, 2014*)

L'anonymisation

- Une anonymisation irréversible est-elle possible dans un univers ultra-connecté ?
  - difficile de rester anonyme dans le domaine de la mobilité avec la collecte de la géolocalisation (*ex. Mondjoye et al. 2014)*
- Une réidentification qui peut être nécessaire
  - Recherche scientifique
  - Réparation, maintenance, facturation,…
  - Exercice du droit d'accès par la personne concernée (CJUE)
  - Preuve à des fins contentieuses

→ *Mettre la technique et la technologie au service de la protection des données et du respect des droits de la personne*

La pseudonymisation

- Technique de remplacement des données personnelles directement identifiantes par un pseudonyme non-signifiant

  → amélioration de la « *protection de la confidentialité des informations à caractère personnel en réduisant les risques de mésusage* »

  (*CNIL, pack de conformité véhicule connecté, 2017*)

- La pseudonymisation n'est pas une méthode d'anonymisation :
  - c'est une mesure de sécurité qui permet de réduire « *la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée* » (G29, 2014).

- La pseudonymisation n'est pas irréversible
  - les données pseudonymisées <u>restent des données à caractère personnel</u>

- Des tensions possibles 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 ?

2ème partie
Les bases juridiques de la protection des données personnelles


... LE MONDE — 21 mars 1974 —

JUSTICE

« Safari » ou la chasse aux Français

Convention 108

COUNCIL OF EUROPE CONSEIL

227

7 Janvier 1978 JOURNAL OFFICIEL DE LA REPUBL

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 L 119

de l'Union européenne

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)

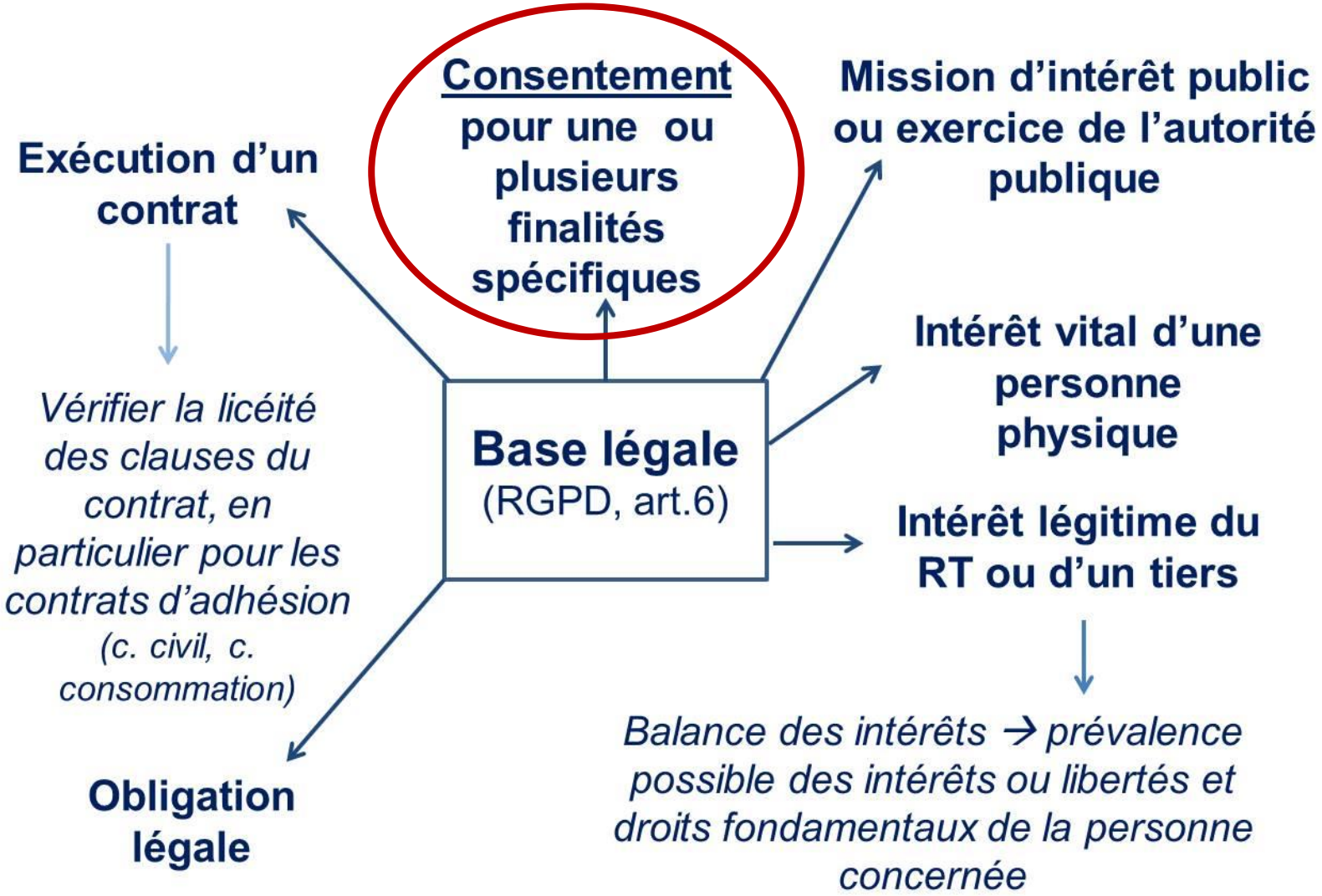
Un contexte juridique qui n'est pas spécifique à la France

- Europe des droits de l'Homme
  - Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (1950)
  - Convention européenne pour la protection des DCP (1981)
- Droit communautaire en évolution
  - Charte des droits fondamentaux de l'UE (art.7 et 8) (vie privée ; données personnelles)
  - Règlement européen pour la protection des données personnelles (RGPD)
    - application au 25 mai 2018 / abrogation de la directive de 1995
    - suppression des formalités préalables,sauf exceptions
      → accompagnement et contrôle *a posteriori* (CNIL)
  - vers un Règlement européen *e-privacy* (en cours)
    - abrogation de la directive 2002/58 *vie privée et communications électroniques*
  - Un contexte communautaire qui impacte au-delà de l'UE
    - ex. invalidation du *Safe Harbor* → CJUE, 2015 → *Privacy shield*
    - une protection pour l'ensemble des résidents de l'UE
- Droit interne → loi du 6 janvier 1978 modifiée
  - projet de loi en débat au Parlement pour adaptation au RGPD

Une nécessité rappelée par des textes spéciaux
Illustration par les STI et la conduite automatisée

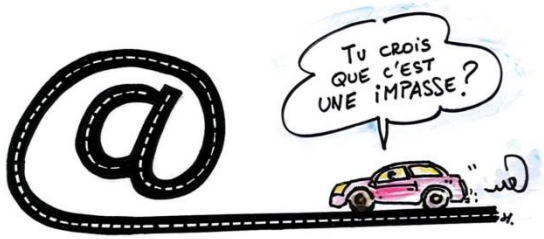
- Directive Systèmes de transport intelligents, art. 10
  - renvoi express aux directives PDCP (95/46) et *vie privée et communications électroniques* (2002/58)
    - Rapports de la plateforme C-ITS (Europe) (janv. 2016, sept. 2017)
    - comment garantir l'interopérabilité // cybersécurité et PDCP ?
    - *Un règlement délégué sur PDCP prévu (?) ;* G29, avis oct. 2017
  - 1ère application réglementée dans l'UE : eCall
- ECE-ONU, débats en cours
  - groupe informel STI / conduite automatisée
    - garantir la protection des données et la cybersécurité
      => objectifs dans le cadre de la conduite automatisée
  - WP29 → proposition de directive
    - protection des données personnelles et cybersécurité
      => à intégrer dans la réglementation technique internationale des véhicules et de leurs équipements

Les bases légales de la collecte et du traitement



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

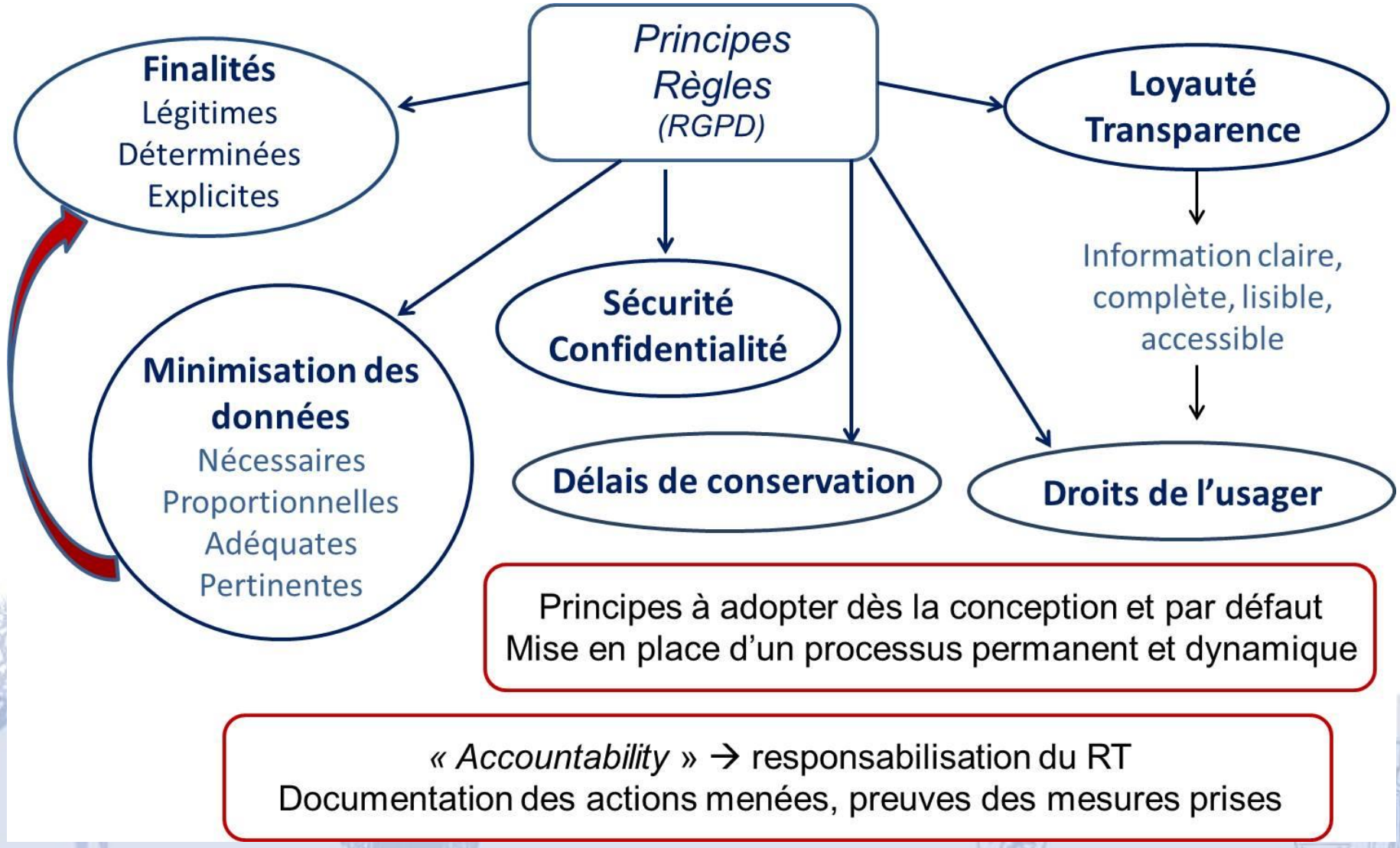
3ème partie
Obligations des responsables de traitement et de leurs partenaires
Les grands principes



Dessin : J.Yerpez

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

Des principes à respecter par les responsables de traitement et leurs partenaires



La protection des données à caractère personnel
L'exemple de l'eCall

PDCP STI NIS IDAS
UNION EUROPÉENNE

DIRECTIVE 2010/40/UE du Parlement Européen et du Conseil du 7 juillet 2010
concernant le **cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport**

Article 10

Règles relatives au respect de la vie privée, à la sécurité et à la réutilisation des informations

1ère application réglementée

Le principe de **minimisation**

Illustration par un service réglementée : l'eCall et les SVA

4ème partie
La sécurité des objets connectés / communicants

Anticiper les risques potentiels, faire évoluer la réglementation

« 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
Anticiper les risques potentiels

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
  - ou sur la régulation de la fourniture d'électricité
- prise en main du contrôle par un tiers
  - d'un élément du système, d'une tâche, …
  - d'une activité, par exemple

La sécurité du système de circulation routière connecté. Anticiper les risques potentiels

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

Fonctionnement des systèmes

Respect des droits des usagers

La cybersécurité, un impératif dans un système connecté

https://www.ssi.gouv.fr/agence/cybersecurite/mois-de-la-cybersecurite-2017/

La sécurité des systèmes connectés
Un droit en construction

Prendre des mesures pour sécuriser les données, les systèmes

Obligation légale des concepteurs, des fabricants et des responsables de traitement

Protection des données à caractère personnel

2018 : des règles renforcées

Cybersécurité

des règles à venir

Les produits et services délivrés par des personnes privées	ex. constructeurs automobiles
Les ouvrages publics connectés	Gestionnaires publics
Les réseaux de communications	Organismes télécommunication
Les serveurs et les terminaux	Hébergeurs et gestionnaires des données

La cybersécurité. Une exigence qui monte en puissance dans la réglementation

Réglementations et normes en émergence

- Renforcement du droit communautaire mais aucun texte ne concerne directement le véhicule connecté
  - pack cyber sécurité pour l'UE ? *(réunion du Conseil, 19-20 oct. 2017)*
  - sécurité des réseaux et des systèmes d'information avec notion de services essentiels (*directive cybersécurité, entrée en application prévue en 2018*)
  - identification électronique et services de confiance pour les transactions électroniques au sein du marché (*Règlement IDAS, 2014*)
- Nombreux travaux de normalisation en cours, par exemple pour la sécurité du véhicule connecté, communicant
  - Véhicules routiers (ISO / SAE..) v/ STI coopératifs (ETSI et C-ITS , ISO …)

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

- Des « 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

5ème partie
Des méthodes et des outils pour la conformité et la protection des données personnelles

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

- Des processus volontaires (labels, codes de conduite, certifications, …)
- L'étude d'impact (RGPD)
- Des packs de conformité, des référentiels

Outils et méthodes pour la protection des DCP
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 DCP

L'étude d'impact (1)

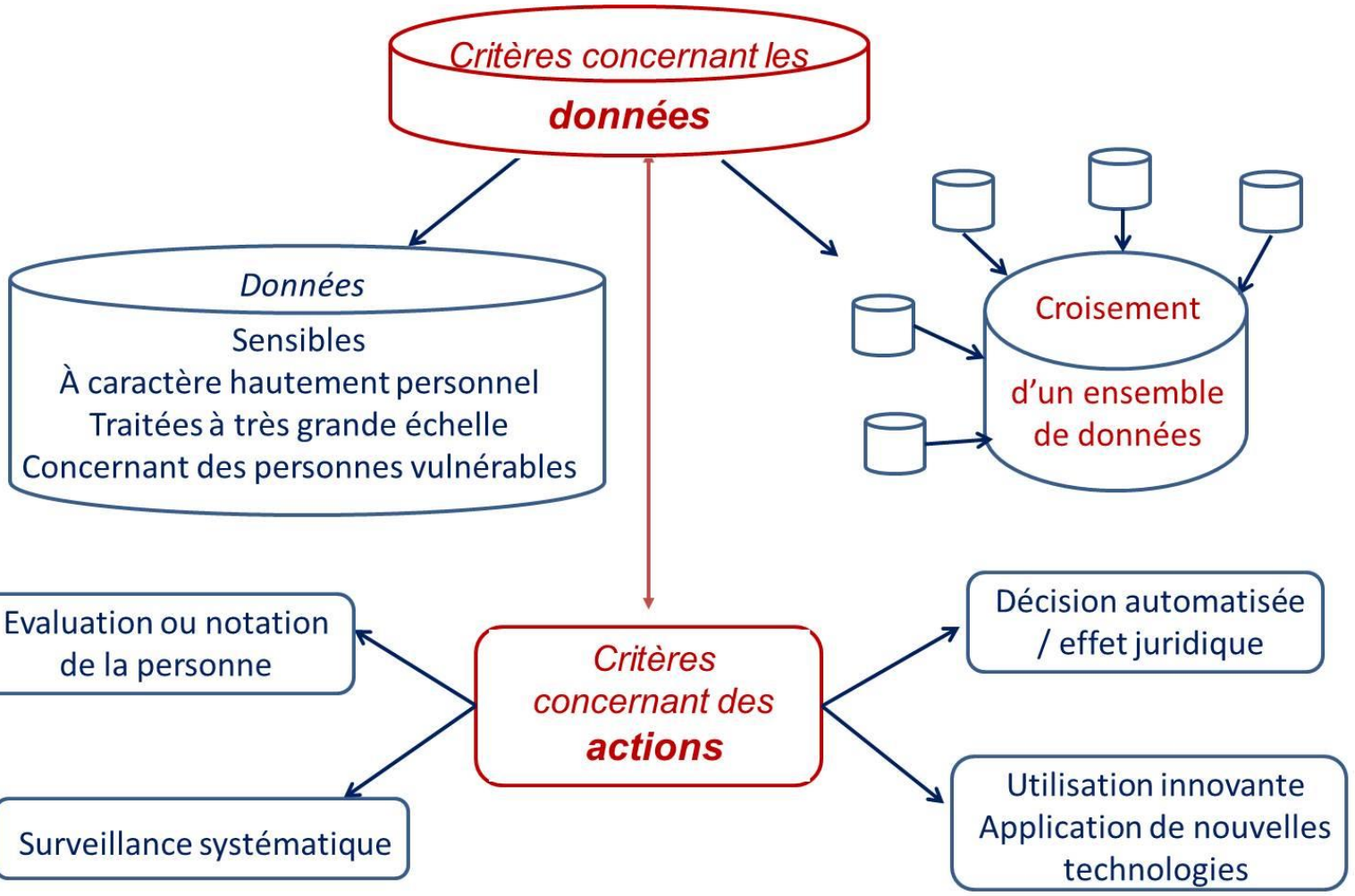
Méthodologie (G29, 2017)

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 DCP

L'étude d'impact (2)

Les lignes directrices du G29



Outils et méthodes pour la protection des DCP

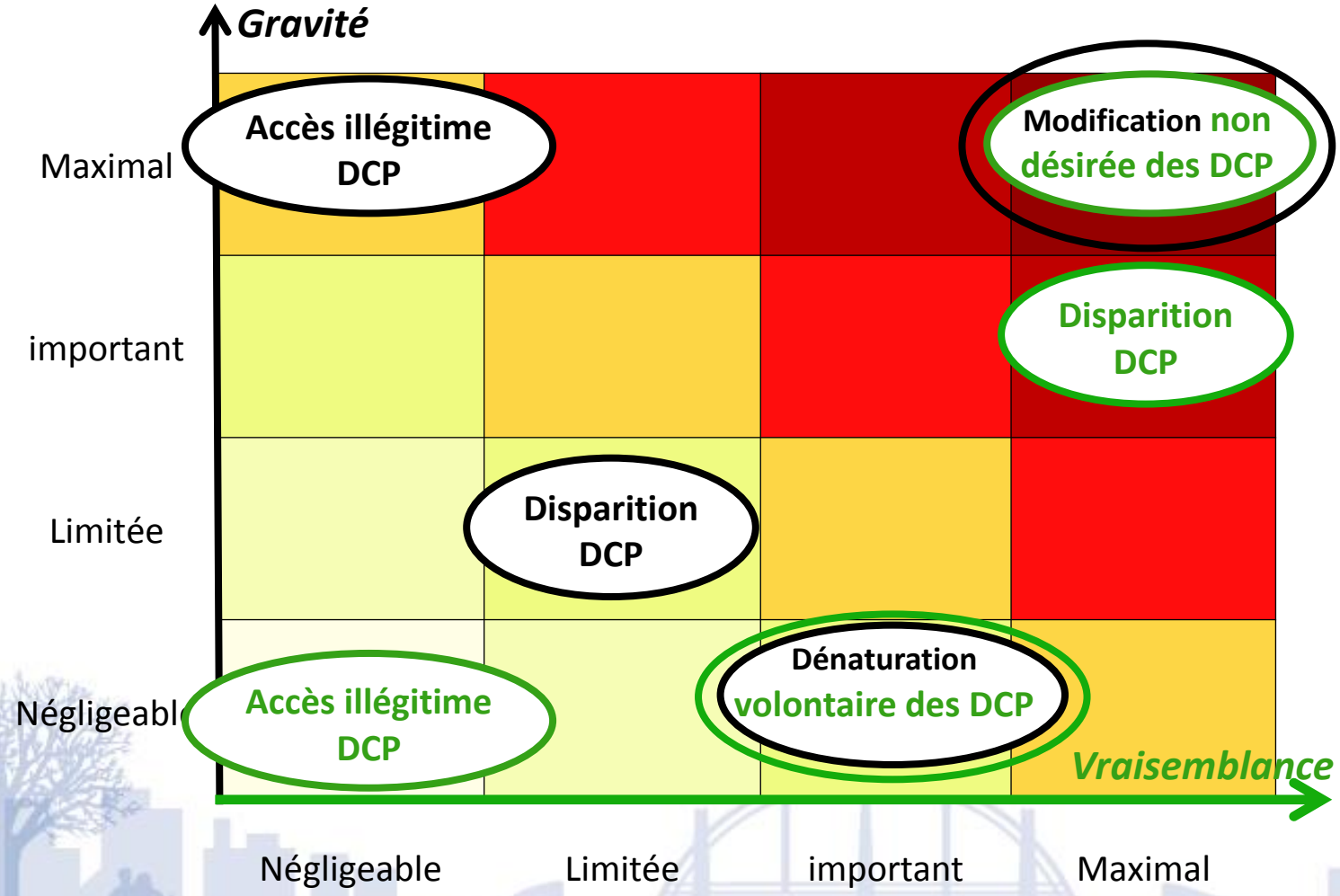
L'étude d'impact (3)

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. typiquement 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 DCP
L'étude d'impact (4)

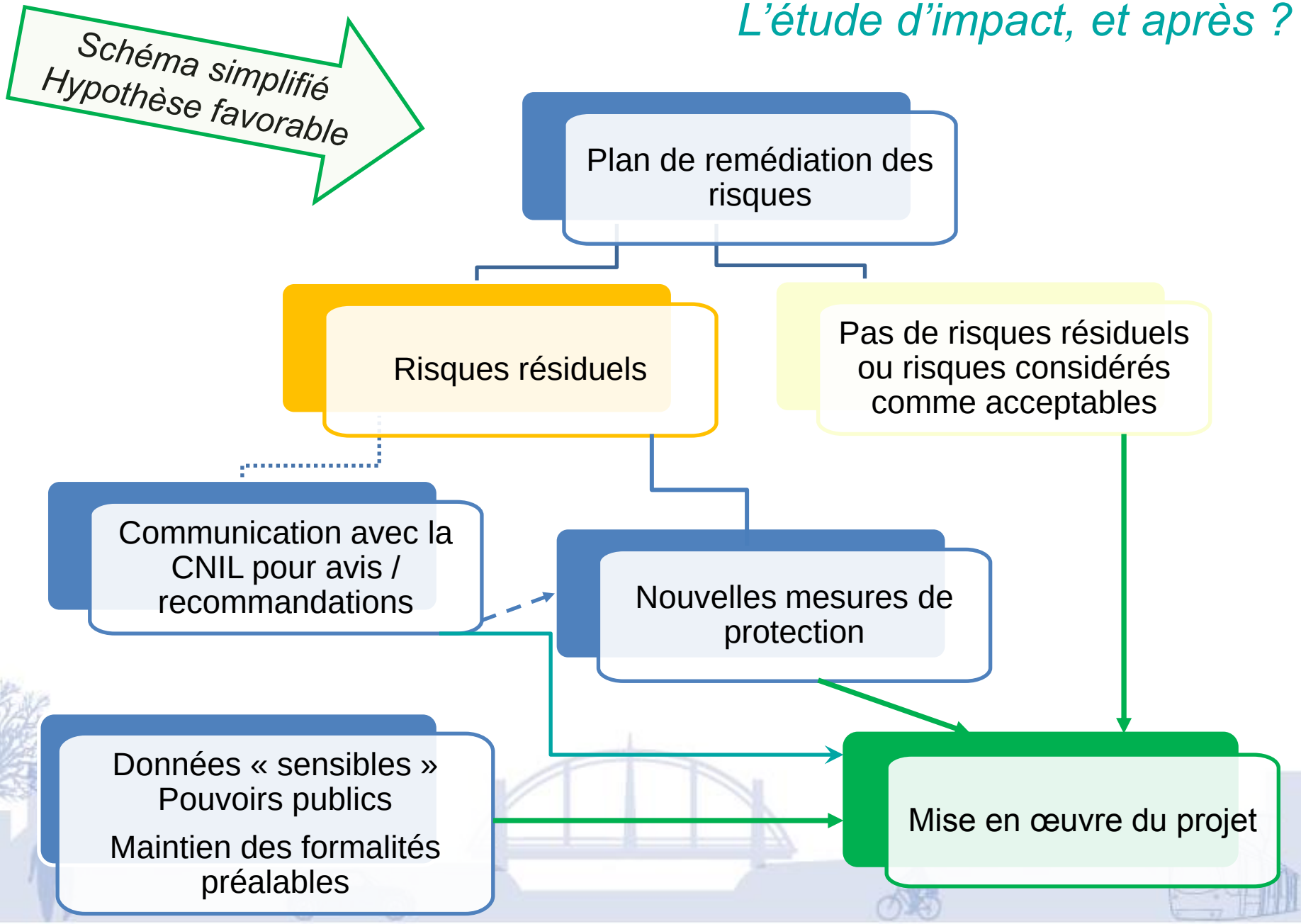
L'évaluation du risque
(d'après CNIL, Outillage du PIA)



4 critères
- Disponibilité
- Intégrité
- Confidentialité
- Traçabilité

Outils et méthodes pour la protection des DCP

L'étude d'impact, et après ?



Outils et méthodes pour la protection des DCP

Le pack de conformité véhicule connecté

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

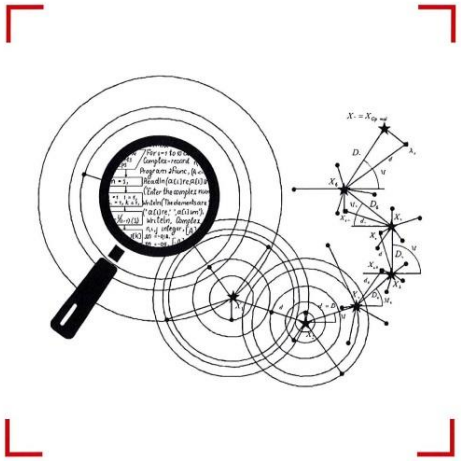
	Scenario 1 « IN-IN »	**Scenario 2 « IN-OUT »**	**Scenario 3 « IN-OUT-IN »**
Circuit des données	Les données personnelles demeurent à l'intérieur du véhicule Pas de transmission à un tiers Certaines données peuvent sortir du véhicule via une application directement gérée par l'usager sur un objet connecté 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

Outils et méthodes pour la protection des DCP

Le pack de conformité compteurs communicants

Des lignes directrices pour les compteurs communicants et la gestion des données de consommation

	Scenario 1 « IN-IN »	**Scenario 2 « IN-OUT »**	**Scenario 3 « IN-OUT-IN »**
Circuit des données	Les données sont gérées - à l'intérieur du logement - à l'extérieur sans transmission à un tiers pour réutilisation Circulation sur - réseau wifi ou local sous contrôle de l'usager - réseaux télécommunications ouverts au public (type ADSL, fibre, GSM)	Données collectées dans le logement par le prestataire pour la fourniture de service(s) à l'usager. mais sans déclenchement d'une action dans le logement. Elles peuvent être transmises à un sous-traitant	Transmission des données à l'extérieur du logement pour pilotage à distance de certains équipements
Exemples	Communication entre thermostat et chauffage Déploiement automatique de volets suivant l'ensoleillement	Proposition d'un contrat adapté au niveau de consommation Bilans énergétiques Prospection commerciale pour le compte de l'usager	Prospection commerciale pour compte du prestataire Prestation réalisée par un tiers en l'absence de l'usager (mais cadre contractuel)



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

6ème 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

En ordre dispersé, les départements ministériels tentent de développer à leur profit, à leur seul usage, l'informatique et son outil, l'ordinateur. Ce n'est pas tout à fait un hasard si, à l'époque où le journal officiel va publier un arrêté créant une « division de l'informatique » au ministère de la justice, celui de l'intérieur met la dernière main à la mise en route d'un ordinateur puissant destiné à rassembler la masse énorme des renseignements grapillés sur tout le territoire; pas un hasard non plus si le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à détruire chaque Français par un « identifiant », qui ne définisse que lui, maintenant termine, est l'objet de convoitises ardentes: le ministère de l'intérieur y souhaite jouer le premier rôle. En effet, une telle banque de données, soubassement opérationnel de toute autre collecte de renseignements, donnera à qui la possédera, une puissance sans égale.

Ainsi se trouve d'évidence posé un problème fondamental, même s'il est rebattu : celui des rapports des libertés publiques et de l'informatique. Son importance exigerait qu'il en fût, au Parlement, publiquement débattu. Tel ne paraît pas être, pourtant, la solution envisagée par le premier ministre dans les directives qu'il vient d'adresser au ministère de la justice, intéressé au premier chef si l'on s'en rapporte à la Constitution qui dans son article « 66 fait de l'autorité judiciaire le gardien des libertés individuelles.

La protection des données personnelles
Les droits des personnes physiques concernées

- Droit à ne pas être connu, reconnu, tracé, dans ses déplacements
  - notamment risques liés à la géolocalisation
- Droit à une information claire et accessible
  - sur les finalités, les données collectées, les modalités de traitement, les destinataires des données
- Droit à consentir
  - au recueil et au traitement, sauf autre base légale (ex eCall)
  - un consentement libre, éclairé (informé), spécifique (+ explicite et preuve / RGPD)
- Droits d'accès, et selon les cas, d'opposition, de rectification, d'effacement (*droit à l'oubli*), droit à la portabilité des données *fournies par la personne*

Données personnelles

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

La protection des données personnelles
Les droits des personnes physiques concernées

- Pas de décision individuelle produisant des effets juridiques
  - qui serait uniquement fondée sur un traitement automatisé de données destiné à définir un profil ou à évaluer des aspects de la personnalité
    - *sauf exécution d'un contrat avec la personne ou son consentement*
  - ou d'un traitement algorithmique sans information préalable et explicite de la personne à propos du traitement et de ses modalités
- Pas de décision de justice impliquant une appréciation du comportement d'une personne
  - qui serait fondée sur un traitement automatisé destiné à évaluer des aspects de la personnalité
- Des contraintes plus fortes pour la protection des données « sensibles » : santé, infractions, …
- Respect du droit des contrats et de la consommation par les responsables de traitements et leurs partenaires
  - V. notamment contrats d'adhésion / clauses abusives

Sources : loi de 1978, art. 10 ; RGPD, art. 22 ; c. relations du public avec l'administration, art. L.311-3-1

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
- introduction de l'action de groupe pour la protection des DCP

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 » et non pas en « réparation »
  - faire cesser le dommage → interruption de la collecte et du traitement
  - élargir l'action à la réparation → amendement proposé sur projet de loi « données personnelles »

    (*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

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

La protection des données personnelles

Non respect des mesures et responsabilités

Elargissement du cercle des parties prenantes dans les système de production et de gestion des services

diversité des responsables de traitement et des sous-traitants

- concepteurs d'un élément, programmeurs de logiciels, …
- fabricants des produits
- gestionnaires des ouvrages connectés
- fournisseurs 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
- …

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 personnelles

Non respect des mesures et responsabilités

La négligence est un élément constitutif de l'infraction

- Des sanctions pénales possibles (*)
  - non respect des formalités préalables
    - sanctions pénales → art. 226-16 al.1, code pénal
    - caractère illicite du fichier → C. Cassation, 2013
  - procéder ou faire procéder à un traitement sans mettre en œuvre les mesures de sécurité prescrites
    - sanctions pénales → art. 226-17, code pénal
  - collecter des DCP par un moyen frauduleux, déloyal ou illicite
    - sanctions pénales → art. 226-18, code pénal
- Pouvoirs des autorités de contrôle et de régulation
  - enquêter et imposer des mesures correctives
  - sanctionner → une augmentation sensible des amendes administratives
    - 3 millions d'euros (loi République numérique, en vigueur)
    - selon les violations → jusqu'à 20 millions d'euros ou 4% maximum du chiffre d'affaire mondial de l'entreprise *(RGPD mai 2018)*

    → imputables aux responsables de traitement et aux sous-traitants

(*) *sauf Etat, et collectivités territoriales pour activités susceptibles de faire l'objet d'une DSP*

Etre prêt pour l'application de la nouvelle réglementation communautaire en mai 2018 (RGPD, mais aussi cybersécurité)

- Une réponse organisationnelle
  - 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 outils technologiques pour la protection
  - dès la conception, par défaut et de manière dynamique
  - en utilisant éventuellement 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)

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

« Le monde de demain appartiendra à des mathématiciens milliardaires qui auront compris comment vous exploiter de votre plein gré.

La solution ne peut venir que d'autres génies mathématiques […] »

(Ollivier Pourriol, Xavier Lazarus, le 1 n°10, 11 juin 2014)