



Institut  
Mines-Télécom

Chaire Valeurs et Politiques  
**DES INFORMATIONS PERSONNELLES**  
||| ■ ■ ■ || ■ ■ ■ ■

# **Economie de l'Internet et des données personnelles (SES720) Janvier 2015**

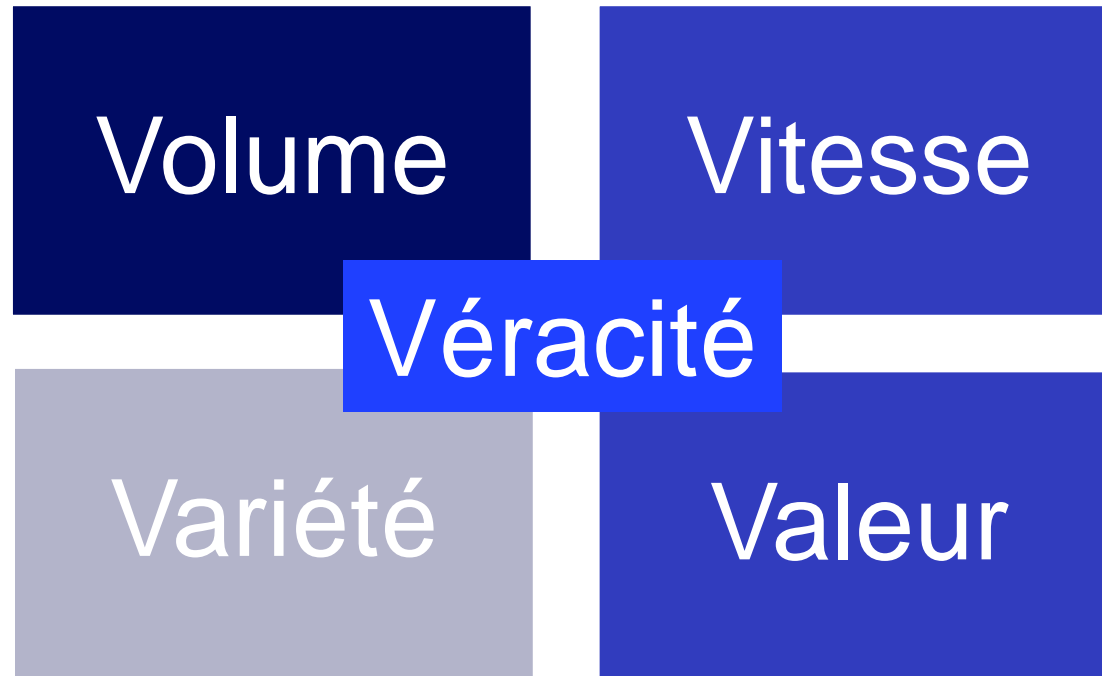
***Claire Levallois-Barth***

Maître de conférences en droit

Coordinatrice de la Chaire Valeurs et  
politiques des informations personnelles



## Définition(s)



Changement a priori quantitatif mais aussi qualitatif

# Morale et Droit

- Règle morale : règle de conduite individuelle et volontaire, fondée sur la justice et la charité
- Sa sanction émane de la conscience
- Règle juridique : règle de conduite sociale devant
  - Assurer l'ordre social
  - Garantir les libertés publiques
  - Garantir les droits des citoyens
- Sanctionnée par la contrainte



## Droit national

### Droit en vigueur dans un État

- Sources, organes et sanctions propres à cet État
  - Réglemente les rapports sociaux qui se produisent à l'intérieur de cet État
- Aucun élément relevant d'un autre État intervient dans ces relations

### Droit national public

Satisfaction d'intérêts collectifs : régit les rapports entre les particuliers et l'Etat (et ses agents)

### Droit national privé

Satisfaction d'intérêts individuels : régit les rapports entre particuliers / personnes physiques ou morales

## Droit international & européen

### Règles qui régissent les rapports entre

- Des Etats entre eux
- Des particuliers entre eux lorsqu'ils comportent un élément étranger

### Droit international public


Rapports interétatiques et organisations internationales

Ex. : Adoption de la Convention européenne des droits de l'homme

### Droit international privé

Rapport entre particuliers présentant un élément d'extranéité

Ex. : Divorce d'un français et d'une anglaise

	Droit public	Droit privé
 <b>But</b>	Satisfaire des intérêts collectifs	Satisfaire des intérêts individuels
<b>Caractère</b>	Essentiellement impératif : pas de dérogations aux règles	Large part à la volonté individuelle : la plupart des règles sont supplétives
<b>Définition</b>	Règles qui ont pour objet <b>l'organisation, les structures et les composantes de l'Etat</b> et des collectivités publiques et qui <b>gouvernent leurs rapports avec les particuliers</b>	Ensemble des règles qui gouvernent les <b>rapports des particuliers entre eux</b> ou avec les collectivités privées telles que les sociétés, les associations
<b>Composantes</b>	<p><b>Droit constitutionnel</b> : organise les pouvoirs de l'Etat (forme de l'Etat, constitution du gouvernement et des pouvoirs publics)</p> <p><b>Droit administratif</b> : organisation des collectivités publiques (Etat, régions, départements, communes ...) et des services publics ainsi que leurs rapports avec les particuliers</p> <p><b>Droit fiscal et des finances publiques</b> : détermine les conditions et les montants de la participation des sujets de droit aux budgets de l'Etat et des collectivités publiques</p>	<p><b>Droit civil</b> est le droit commun : règles applicables à la vie privée des individus (droits et obligations réciproques) et qui n'ont rien de spécifiquement commercial, social ou rural ...</p> <p><b>Droit commercial</b> : commerçants et actes de commerces</p> <p><b>Droit du travail, de la concurrence, de la consommation, des transports, des assurances, de la propriété industrielle, bancaire, de la distribution etc..</b></p>
<b>Droit pénal (Mixte)</b>	<p>Institue et aménage le droit de punir tel qu'il appartient à la société et tel qu'il est exercé en son nom par ses organes qualifiés dans le cadre de la procédure pénale.</p> <p>La procédure pénale organise le déroulement du procès devant les tribunaux judiciaires répressifs</p>	En sanctionnant les comportements constitutifs d'infraction, garantit la sauvegarde de certaines prérogatives individuelles
<b>Procédure civile (mixte)</b>	Organisation du service public de la justice	Organisation des juridictions judiciaires et fonctionnement du procès civil (matière civile)

# Différents types de données

## Données « à caractère Personnel »

Loi Informatique et Libertés  
de 1978

## Données « privées »

Sur lesquelles des tiers  
détiennent des droits

## Données « publiques »

Loi CADA de 1978

**Principe** : « Les informations figurant dans des documents produits ou reçus par les [autorités publiques], quel que soit le support, peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus »

**Nombreuses exceptions**

# Pour les données dites « privées »

## ■ Droit de propriété intellectuelle

- Droit d'auteur
- Droit des marques (marque déposée protégeant un nom)
- Droit des brevets

## ■ Droit des secrets

- Secret médical
- Secret commercial et industriel
- Secret des affaires
- Secret professionnel
- Secret statistique
- Secret de fabrication
- Secret bancaire ...

## ■ Droit des bases de données

## ■ Droit à la protection de la vie privée / droit à l'image

## ■ Droit contractuel (droit privé / droit public)

## ■ Droit de la concurrence

- Facilités essentielles
- Données essentielles



Institut  
Mines-Télécom

# **1. Le cadre légal français de protection des données personnelles**

Loi Informatique et Libertés

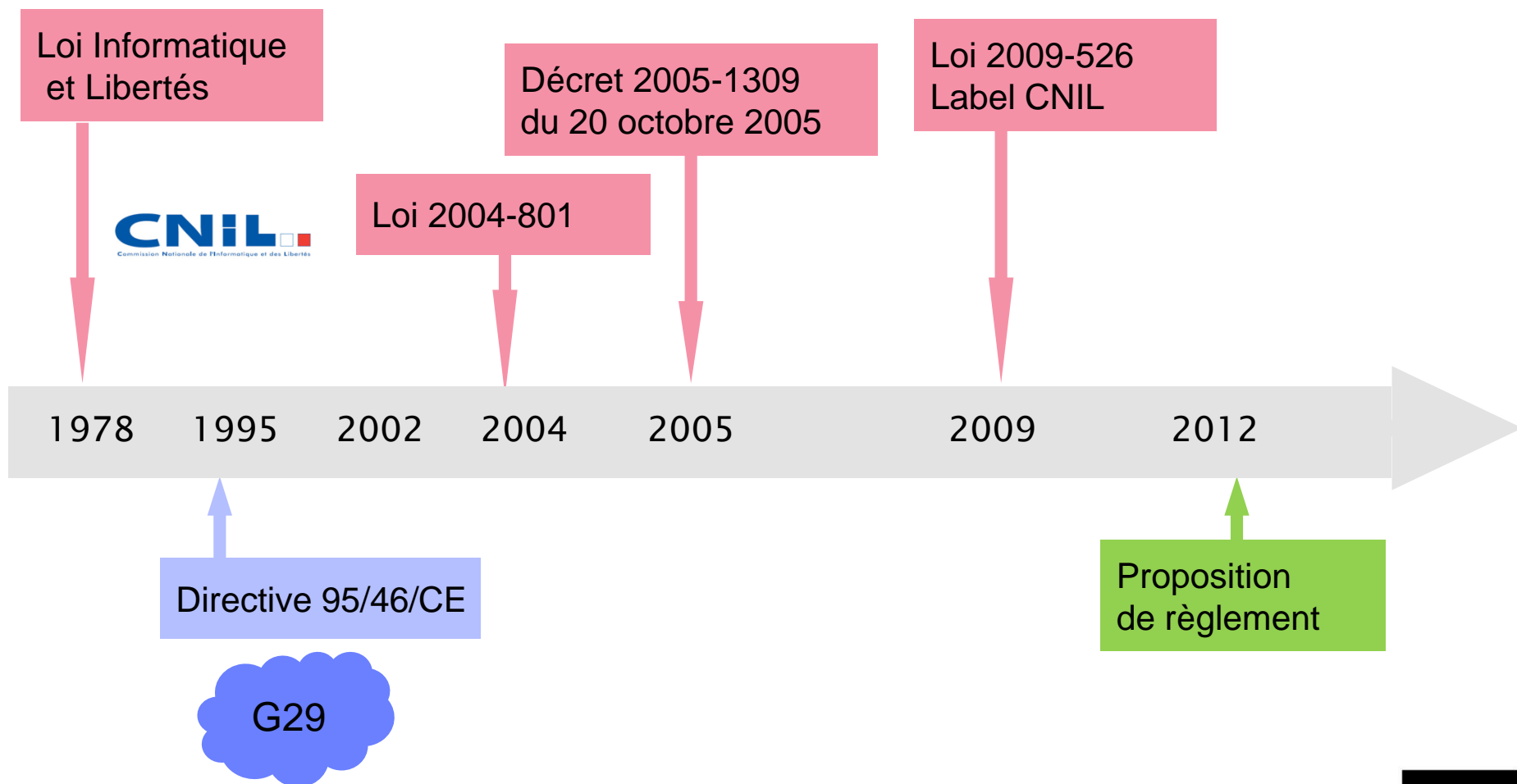






## 1.1. Objectifs et notions clés

# Protection française issue du droit de l'UE



## Protection très large

Qu'est-ce qu'une donnée à caractère personnel (donnée personnelle) ?

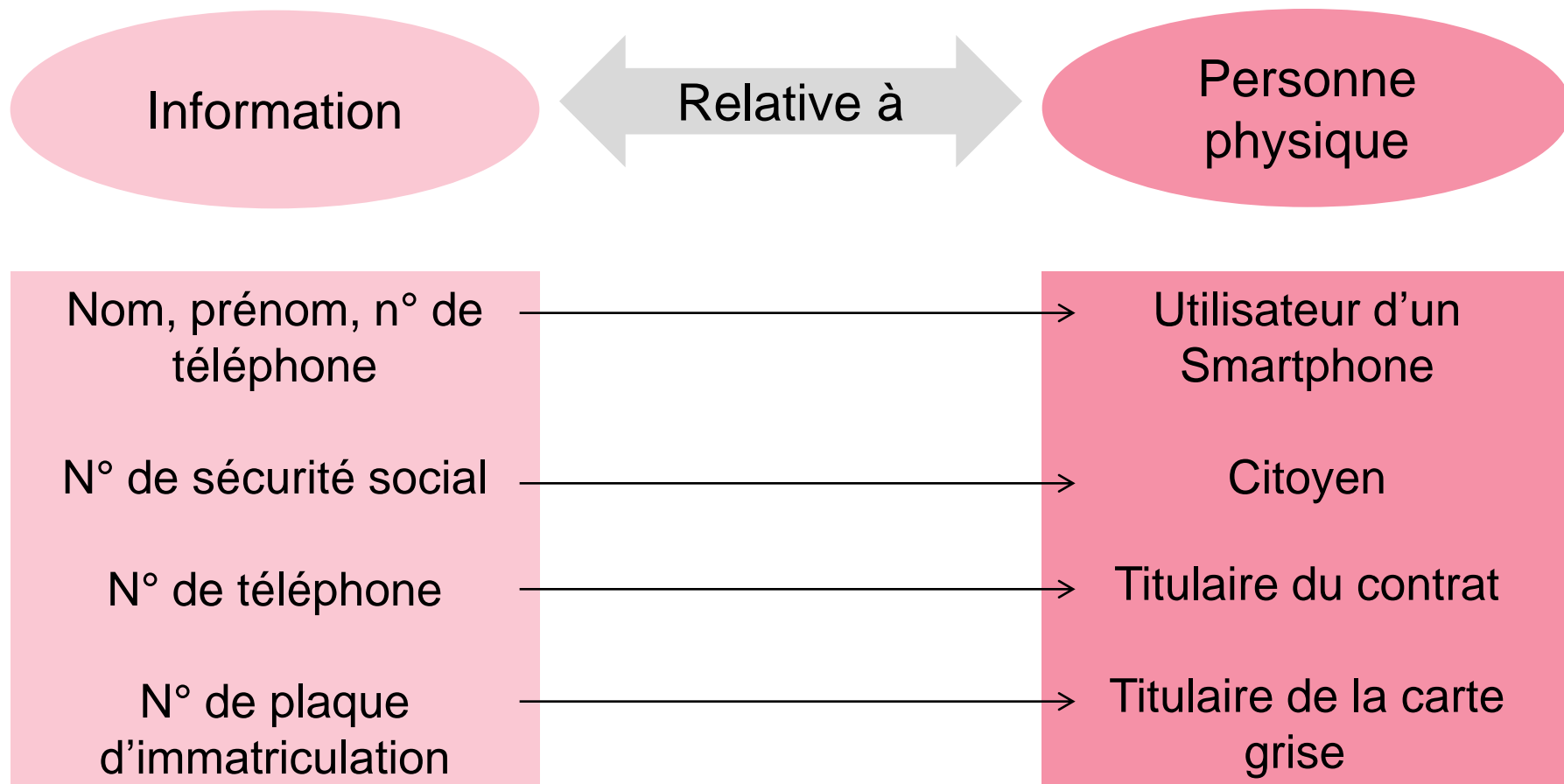


# Donnée personnelle

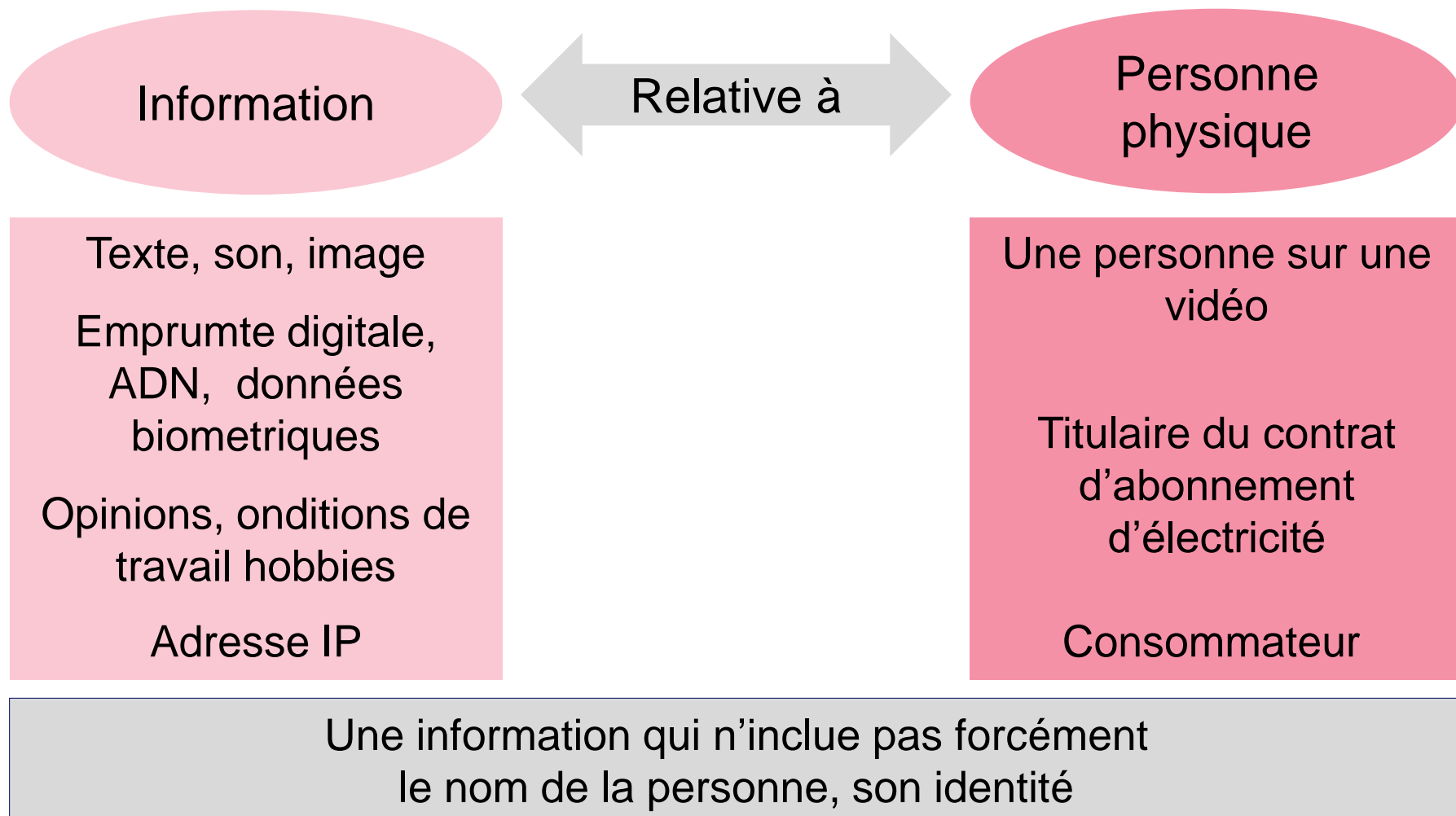
- « *Toute information relative à une personne physique*
  - *identifiée ou qui peut être identifiée,*
    - *directement ou indirectement*
- *par référence à un n d'identification ou à un ou plusieurs éléments qui lui sont propres »*

➤ **Personne identifiable** : considérer l'ensemble des moyens dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne

# Interprétation extensive



# Interprétation très extensive



# Traitement de données personnelles

- « *Toute opération ou ensemble d'opérations*
- *effectuées ou non à l'aide de procédés automatisés*
- *et appliquées à des données personnelles,*
- *telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction »*

# Objectifs

## ■ Article 1 de la loi Informatique et libertés

- « L'informatique doit être au service de chaque citoyen.
- Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »

## ■ Encadrement de l'utilisation des données personnelles

- Par les institutions, privées ou publiques, les individus

## ■ En accordant à la personne une certaine maîtrise de ses données personnelles



# Enjeux

Respect des  
droits et libertés

Compétitivité

Valeur ajoutée

Autonomie

Conformité  
juridique

Confiance

Discrimination/Exclusion  
Perte de contrôle

Image de marque

Responsabilité


# Droit applicable

## ■ Le responsable de traitement est établi dans plusieurs États

- Google street view contrôlé à la fois par la Cnil et l'autorité allemande

## ■ Le responsable de traitement n'est pas établi dans l'Union européenne mais il recourt, à des fins de traitement de données personnelles, à des moyens situés sur le territoire d'un État membre

- Respect de la législation nationale de cet État
- Des « moyens » sont constitués selon le G29 lorsque
  - Des centres de données situés sur le territoire de l'État servent au stockage et au traitement à distance
  - Des cookies et des logiciels similaires sont utilisés, le terminal l'utilisateur pouvant être considéré comme un « moyen »



## **1.2. Traitement licite et loyal des données personnelles : principes de protection des données personnelles**

# Principes 1&2 : finalités et qualité des données personnelles

## Finalités

Les données personnelles ne peuvent être recueillies et traitées que pour un usage déterminé, explicites et légitime



## Qualité

Ne collecter que les données personnelles adéquates, pertinentes et nécessaires au regard des finalités



## Durée de conservation limitée

Durée « raisonnable » en fonction de la finalité  
2 ans après le dernier contact avec le candidat à un emploi pour un fichier de recrutement

Droit à l'oubli

**Supprimer ou ANONYMISER la donnée**



# Principes 1&2 : finalités et qualité des données personnelles

- **Finalités parfois difficiles à anticiper**
- **Le volume de données imposent de traiter l'information au fil de l'eau pour au moins sélectionner celle qui devra être analysée**
- **Difficultés d'anonymisation**
  - Toute information est en train de devenir potentiellement une donnée personnelle

# Principe 3 : légitimation

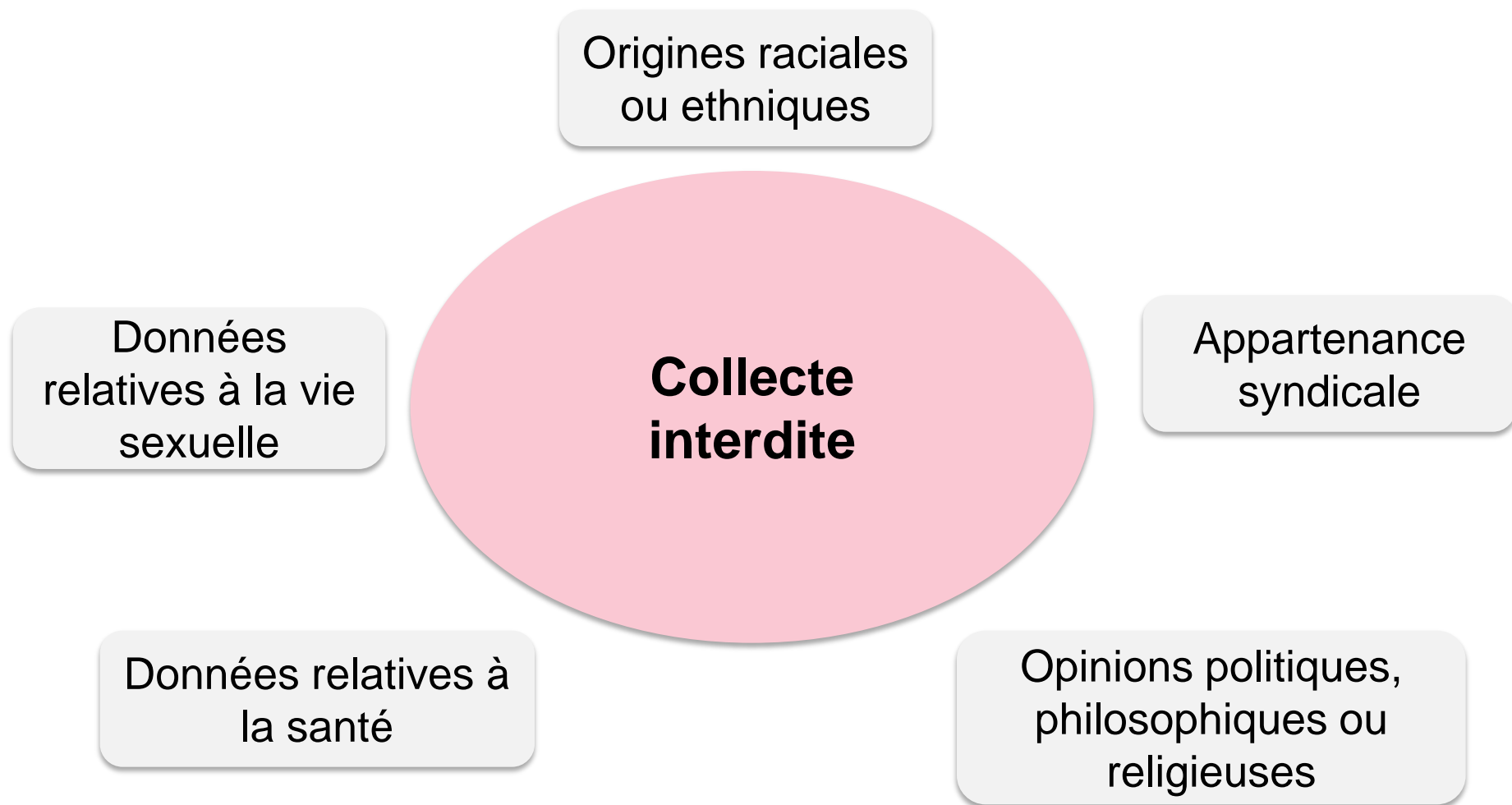
## Consentement

- Offres promotionnelles attribuées au client d'une banque en ligne **en fonction des transactions** enregistrées sur son compte : accord express ("*opt-in*") pour que ses données bancaires soient analysées à des fins commerciales.
- Recueil d'information via un formulaire sur un site web
  - Remplir le formulaire = consentement
- Case à cocher pour transmettre à des tiers ou commercialisées les données personnelles
- Consulter un service météorologique local
- **OU une des conditions suivantes**
  - 1. Respect d'une obligation légale incombant au responsable de traitement**
    - Affiliation au régime de sécurité sociale
  - 2. Sauvegarde de la vie de la personne concernée**
    - Géolocalisation d'un véhicule accidenté, ? **épidémies**
  - 3. Exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement**
    - Dossier administratif d'un étudiant
  - 4. Exécution d'un contrat auquel la personne concernée est partie ou de mesures précontractuelles)**
  - 5. Réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire**

## Principe 3 : Légitimation

- **6. Réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire**
- **Sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée**
- **Analyse au cas par cas selon des critères de pondération**
  - Nature et source de l'intérêt légitime
    - Le traitement de données est-il nécessaire pour exercer un droit fondamental ? Est-il nécessaire à l'intérêt général ? Sa plus-value est-elle reconnue par une communauté ?
      - ? valeurs sociales : ? santé publique, sécurité nationale, protection de l'environnement, application de la loi, efficacité économique
  - Impact sur la personne concernée et son "attente raisonnable" quand à la ce que ses données vont devenir
  - Garanties pouvant limiter l'impact excessif sur la personne concernée : minimisation des données, PETs, transparence, portabilité des données ...

## Principe 4 : données sensibles





## Principe 4 : données sensibles

### ■ Si la finalité l'exige, le traitement est possible si

1. Consentement **express** de la personne concernée
  - Écrit, figurant sur un document distinct du formulaire de collecte
2. Traitement nécessaire à la sauvegarde de la **vie humaine**
3. Traitement mis en œuvre par une **association ou tout autre organisme à but non lucratif** et à caractère religieux, philosophique, politique ou syndical
4. **Données rendues publiques** par la personne concernée
5. Traitement nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice
6. Traitement nécessaire aux fins de la **médecine préventive**, diagnostics médicaux, administration de soins, gestion de services de santé
7. Traitement **Statistiques** réalisées par l'INSEE
8. Traitement nécessaire à la recherche dans le domaine de la **santé**

## Principe 5 : confidentialité et sécurité

- **Seules les personnes habilitées en raison de leur mission accèdent aux données personnelles**
  - Clause de confidentialité dans le contrat de travail
  - Ex. : *pas d'accès au n° de sécurité sociale des élèves pour les enseignants chercheurs, accès aux données sur les élèves boursiers par quelques personnes habilitées ...*
  - Définir et ouvrir les droits d'accès en fonction des besoins réels selon une procédure définie
  - « Tiers autorisés » ayant qualité pour les recevoir de façon ponctuelle et motivée (ex. : police, fisc)
- **Sécurité physique et logique, sécurité des bases de données, des moyen de paiement à distance ...des mobiles**

## Principe 5 : confidentialité et sécurité

### ■ Changement régulier de mot de passe

- Login + mot de passe (minimum de 8 caractères) sont strictement personnels

### ■ Cf les documents de la CNIL

- CNIL, GUIDE La sécurité des données personnelles, édition 2010, [http://www.cnil.fr/fileadmin/documents/Guides\\_pratiques/Guide\\_securite-VD.pdf](http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf).
- CNIL, GUIDE Gérer les risques sur les libertés et la vie privée, édition juin 2012, [http://www.cnil.fr/fileadmin/documents/Guides\\_pratiques/CNIL-Guide\\_Securite\\_avance\\_Methode.pdf](http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf)
- GUIDE Mesures pour traiter les risques sur les libertés et la vie privée, édition juin 2012, [http://www.cnil.fr/fileadmin/documents/Guides\\_pratiques/CNIL-Guide\\_securite\\_avance\\_Mesures.pdf](http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_securite_avance_Mesures.pdf).

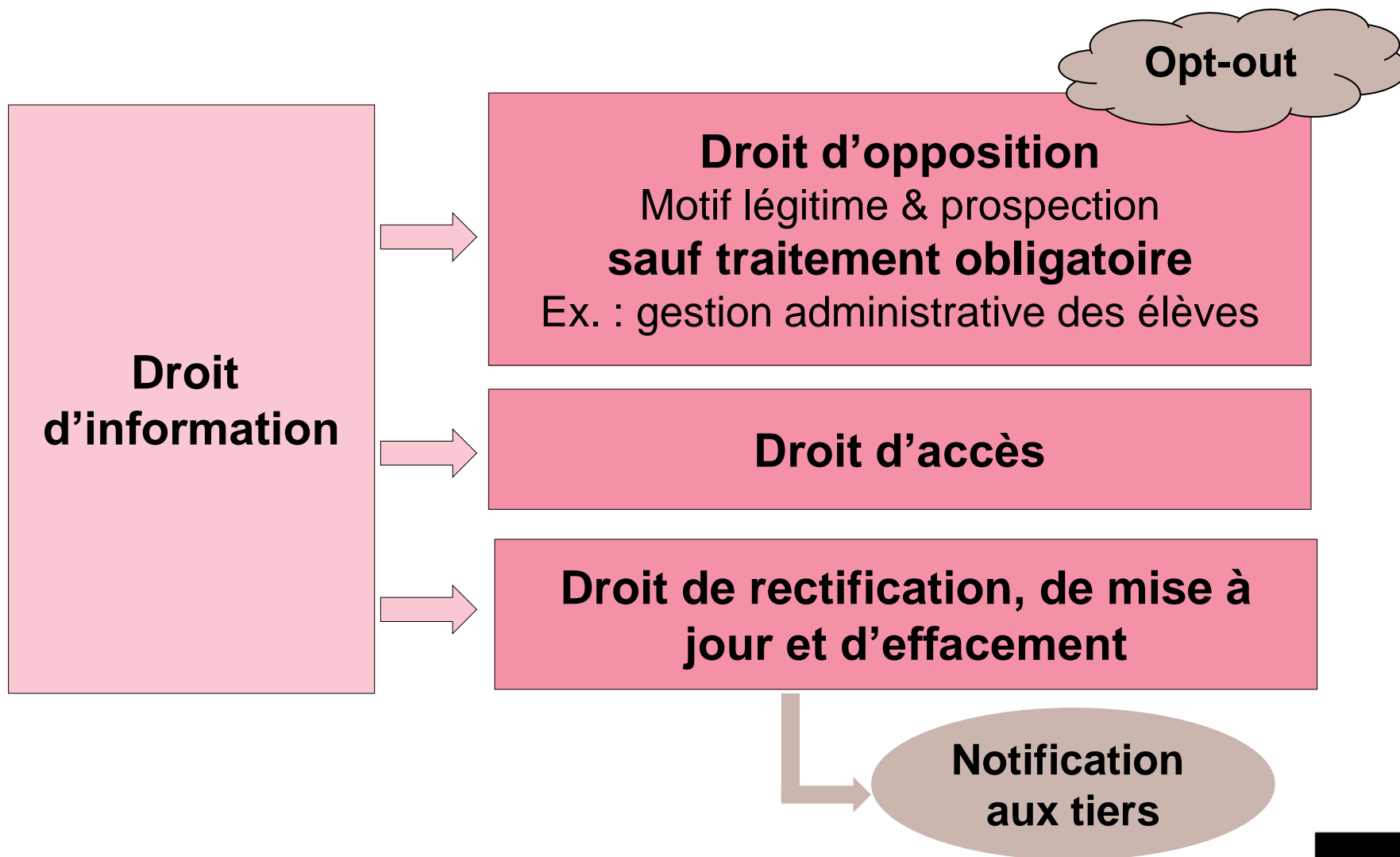
### ■ Notification des violations de sécurité à la CNIL

- Pour l'instant : secteur des communications électroniques

## Principe 6 : droit d'information

- **Au moment de la collecte ou dès l'enregistrement des données**
  1. Identité du responsable de traitement
  2. Finalités
  3. Caractère obligatoire ou facultatif des réponses à apporter
  4. Conséquence d'un défaut de réponse
  5. Destinataires des données
  6. Existence de droits pour la personne
  7. Flux transfrontières
- **+ traitement loyal des données personnelles**
- **Dérogation : pas de droit d'information si**
  - La personne est déjà informée
  - L'information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche

## Principe 7 : droit d'opposition et de suite



## Principe 8 : Décision automatisée

- « Aucune 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 ou à évaluer certains aspects de sa personnalité »
- Si la décision ne satisfait pas la demande de la personne, prévoir une procédure pour que la personne puisse être en mesure de présenter ses observations

# Principe 9 : flux transfrontières (données sortant de l'Union européenne)

## ■ Principe : vers un pays tiers ayant un niveau de « *protection suffisant* »

- Norvège, Liechtenstein, Islande, Andorre, Suisse, Canada, Argentine, Australie, Canada, Îles Féroé, Guernesey, Israël, l'Île de Man et de Jersey, Israël, l'Uruguay et la Nouvelle Zélande
- États-Unis : Safe Harbor

## ■ Exceptions

- Consentement express de la personne concernée
- Autorisation de la CNIL
- Règles internes ou clauses contractuelles
  - Clauses contractuelles de la Commission européenne

## ■ S'applique au cloud computing



## Droit fondamental à la protection des données personnelles

Finalités

Donnée sensibles

Qualité des données

Confidentialité & sécurité


Légitimation

Flux transfrontières

### Droits des personnes concernées

- Information
- Opposition, accès, rectification
- Décision automatisée





## 1.3. Mise en œuvre de la protection des données personnelles

# Responsabilité

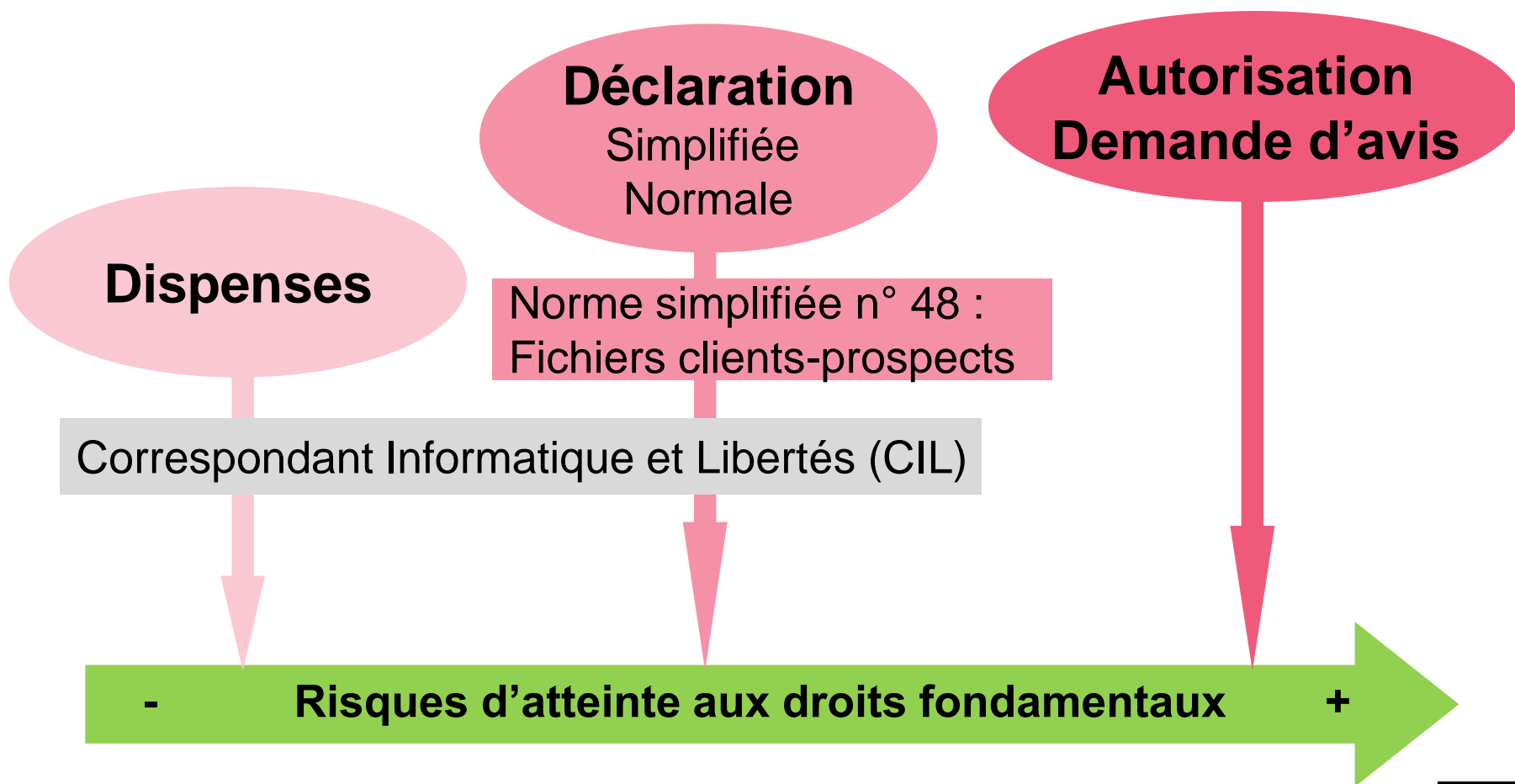
## Responsable de traitement

- « *La personne ... qui, seul ou conjointement avec d'autres,*
- *détermine les finalités*
- *et les moyens du traitement de données à caractère personnel »*
- **Exemples**
  - Versus traitement effectué par une personne physique dans l'exercice d'activités exclusivement personnelles ou domestiques
  - Fournisseurs d'application

## Sous-traitant

- « *La personne qui traite des données personnelles*
- *pour le compte du responsable du traitement »*
- **Agit sur instruction**
- **Contrat**

# Critères de risques



## Formalités préalables

- Principe : déclaration normale auprès de la CNIL
- Signature du responsable de traitement
- Récépissé délivré par la CNIL
  - $\neq$  conformité
  - Mise en œuvre du traitement dès réception du récépissé



# Correspondant Informatique et Libertés (CIL)

Un  
collaborateur

Interne ou  
externe

Pour veiller au  
respect des  
principes  
Informatique et  
Libertés

De manière  
indépendante

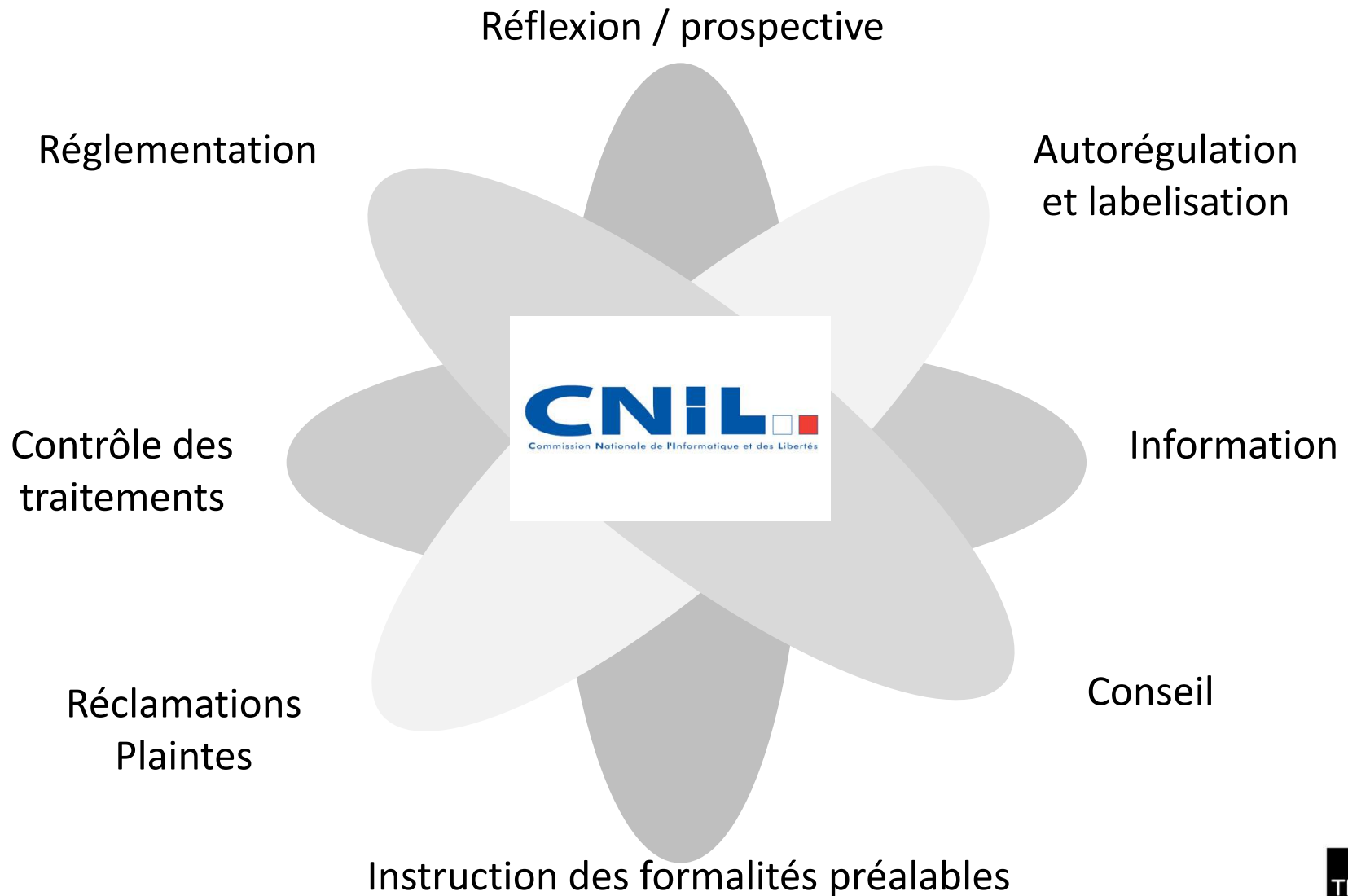
## ➤ **Tenue du registre**

- Déclarations normales et simplifiées

## ➤ **Rapport annuel**

## ➤ **Conseil et sensibilisation**

# Commission Nationale de l'Informatique et des Libertés





 **www.cnil.fr**

# Sanctions

- **Sanctions pénales : très peu appliquées**
- **Sanctions administratives et financières par la CNIL**
  - Jusqu'à 150 000 euros, 300 000 en cas de récidive
  - Nombre en hausse mais en pratique
    - Peu de contrôles : 310 en 2010, 385 en 2011, 458 en 2012
    - Peu de sanctions : 20 en 2011, 13 en 2012
      - Google & Street View : 100 000 euros pour collecte excessive en mars 2011 (1 millions d'euros par l'autorité italienne)
      - Google & non respect des règles de confidentialité : 150 000 euros en janvier 2014 et obligation de publier l'information sur sa page d'accueil
      - Pages jaunes & aspiration de 34 millions de profils : avertissement public pour collecte déloyale en septembre 2011
      - Société commercialisant des coffrets cadeaux : 50 000 euros pour non prise en compte du droit d'opposition
- **Atteinte à l'image de marque**
  - Sanction publique



# LES CHIFFRES CLÉS DE 2013

## FORMALITÉS PRÉALABLES



**92 351**

DOSSIERS DE FORMALITÉS TRAITÉS

**11 085**

DÉCLARATIONS RELATIVES À DES SYSTÈMES DE VIDÉOSURVEILLANCE

**5 514**

DÉCLARATIONS RELATIVES À DES DISPOSITIFS DE GÉOLOCALISATION

**416**

AUTORISATIONS DE SYSTÈMES BIOMÉTRIQUES

## INTERVENTIONS EXTÉRIEURES



**180**

INTERVENTIONS

## AIDE ET CONSEIL



**35 524**

COURRIERS REÇUS



**124 595**

APPELS TÉLÉPHONIQUES

## CORRESPONDANTS



**13 000**

ORGANISMES ONT DÉSIGNÉ UN CORRESPONDANT

**37**

ATELIERS D'INFORMATION QUI ONT ACCUEILLI 1 261 PARTICIPANTS



## PLAINTES ET DEMANDES DE DROIT D'ACCÈS INDIRECT



**5 640**

PLAINTES



**4 305**

DEMANDES DE DROIT D'ACCÈS INDIRECT (FICHES DE POLICE, DE GENDARMERIE, DE RENSEIGNEMENT, FICOM, ETC.)

## LABELS



**29**

LABELS DÉLIVRÉS (sur 14 février 2014)

## MOYENS DE LA CNIL



**16,9**

MILLIONS D'EUROS DE BUDGET



**178**

AGENTS

## NOTIFICATIONS DE VIOLATIONS DE DONNÉES PERSONNELLES



**15**

NOTIFICATIONS EN 2013

## DÉCISIONS ET DÉLIBÉRATIONS



**2 542**

DÉCISIONS ET DÉLIBÉRATIONS

dont 247 autorisations,  
3 autorisations uniques,  
1 229 avis,  
3 recommandations

## CONTRÔLES



**414**

CONTRÔLES

dont 130 contrôles de vidéoprotection

## MISES EN DEMEURE ET SANCTIONS

**57**

MISES EN DEMEURE  
dont 4 rendus publics,  
8 concernant des dispositifs de vidéoprotection



**14**

SANCTIONS  
dont 7 sanctions financières



**5**

AVERTISSEMENTS  
dont 2 publics,  
1 négligé,  
1 non lésé



## 2. Cas pratiques

# Conformité à Télécom Paristech

Zimbra: Réception (1235) x EOLE

https://eole.telecom-paristech.fr/vie-ecole/pratique/cnil/


cnil déclaration

Accueil Site Télécom ParisTech Zimbra Min&Tel Admin Se déconnecter

Mon Espace Vie de l'école Pilotage des études Formations International / Entreprises Recherche Ressources Humaines Bibliothèque/CRDN

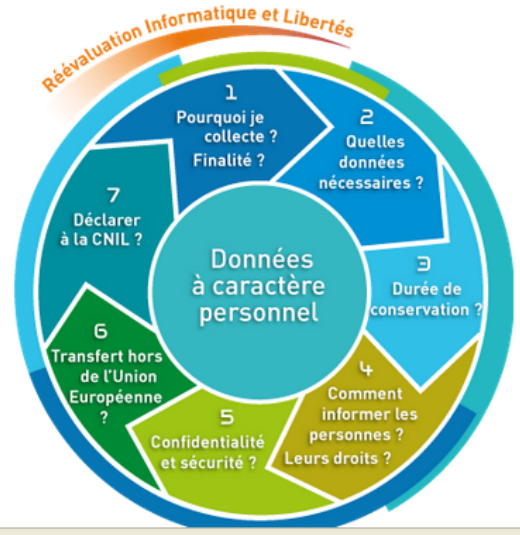
## Informatique & Libertés

Que ce soit pour des projets de recherche, pour la gestion de la scolarité, dans votre vie quotidienne ou au travers des réseaux sociaux, vous accédez, collectez et gérez des **données dites « à caractère personnel »**. L'utilisation de ces données est strictement réglementée par la **loi Informatique et Libertés**.



Ce pictogramme que vous retrouvez dans les pages d'EOLE attire votre attention sur le fait que vous accédez à des données à caractère personnel.

### Processus de conformité Informatique et Libertés



Le diagramme illustre le processus de conformité Informatique et Libertés, centré sur les **Données à caractère personnel**. Le processus est structuré en sept étapes numérotées, entourées par une courbe orange indiquant la **Réévaluation Informatique et Libertés**.

- 1 Pourquoi je collecte ? Finalité ?
- 2 Quelles données nécessaires ?
- 3 Durée de conservation ?
- 4 Comment informer les personnes ? Leurs droits ?
- 5 Confidentialité et sécurité ?
- 6 Transfert hors de l'Union Européenne ?
- 7 Déclarer à la CNIL ?

À noter... **INFORMATION**

- Correspondante Informatique et Libertés (CIL)
  - Nomination du CIL à Télécom ParisTech
- En savoir plus sur...
  - La CNIL
  - La CNIL et les sanctions
  - La CNIL & les jeunes
  - La loi Informatique et Libertés
- S'informer sur...
  - L'actualité Informatique et Libertés
  - Ce qu'il se passe à Bruxelles
- Vos pratiques Métiers...
  - Le guide de l'enseignement supérieur (CNIL - 2011)

https://eole.telecom-paristech.fr/accueil.php

google Phrase non trouvée

Tout surligner Respecter la casse x

43 15/01/2015

Institut Mines-Télécom

Claire Levallois-Barth

ParisTech

# Condamnation de Google par la CNIL

- **Sanction pécuniaire de 150 000 euros**
- **Le 3 janvier 2014**
- **Les règles de confidentialité mises en œuvre depuis le 1er mars 2012 ne sont pas conformes à la loi « Informatique et libertés ».**
- **Référence :**
  - Délibération n°2013-420 du 3 janvier 2014 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Google Inc.
  - <http://www.cnil.fr/linstitution/actualite/article/article/la-formation-restreinte-de-la-cnil-prononce-une-sanction-pecuniaire-de-150000-EUR-a-lencontre/>

# Condamnation des pages jaunes par la CNIL

- Avertissement public
- Le 21 septembre 2011
- Pour aspiration illégale de données personnelles sur des réseaux sociaux
  - Collecte déloyale
  - Défaut de mise à jour
  - Non respect des droits des personnes
- **Références**
  - Délibération n°2011-203 du 21 septembre 2011 de la formation restreinte n°2011-203 du 21 septembre 2011 portant avertissement à l'encontre de la société Pages Jaunes
  - <http://www.cnil.fr/linstitution/actualite/article/article/carton-rouge-pour-les-pages-jaunes/>

# Anonymisation

## ■ Groupe Article 29, Opinion 05/2014 on Anonymisation Techniques adopté le 12 juin 2009, WP 216

([http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index\\_en.htm#h2-1](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-1))

- Respecter 3 critères
  - L'individualisation : un individu ne doit pas pouvoir être isolé
  - La corrélation : il ne doit pas être possible de relier entre eux des ensembles de données distincts concernant un même individu
  - L'inférence : il ne doit pas être possible de déduire de l'information sur une personne.
- Choisir la technique d'anonymisation ou la combinaison de techniques adaptée à un contexte donné



# Cloud computing

- **CNIL**
- **« Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing »**



# Navigo

Références : C. Levallois-Barth,  
Navigo : simplification ou  
traçabilité absolue ?, 2009



# Navigo

## Passe



➤ Puce sans contact

Données

Energie

## Valideur



➤ Antenne

➤ Lecteur

Données

## Serveur



Métro



Tramway



Transilien



RER



Bus

# Enjeux

## RATP

- **Lutte contre la fraude**
- **Etablissement de statistiques**
- **Souhait initial : revente de données**

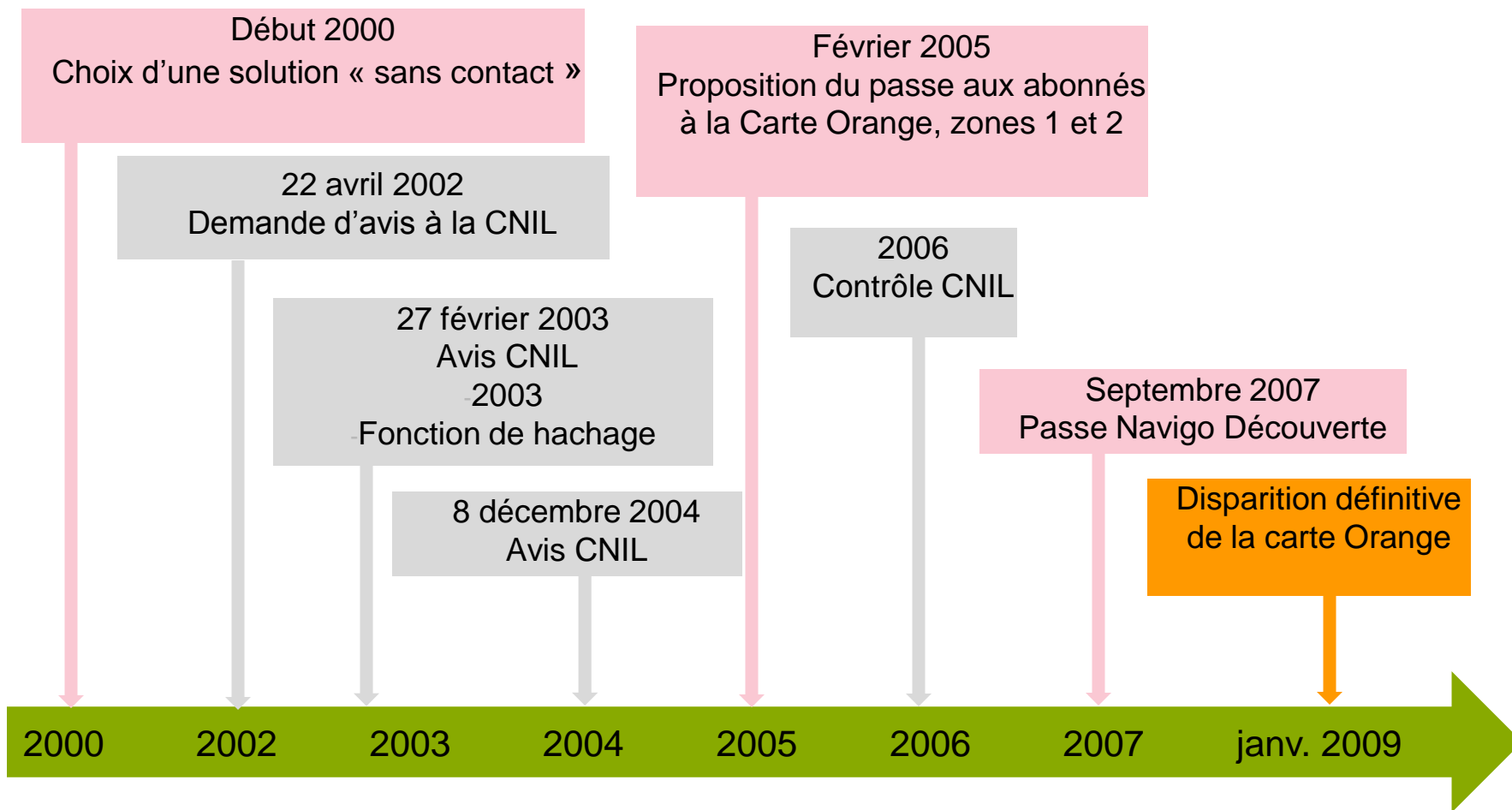
## Voyageur

- **Fluidité : gain de temps**
- **Localisation imposée au voyageur**
- **Traçabilité**
  - Moyen « intolérable et pourtant toléré » de pistage systématique à des fins de marketing et de lutte contre la fraude
  - Vie privée / Liberté de déplacement



Gestion de la mise en liberté surveillée des 9 millions de voyageurs jour  
Réflexion commune CNIL / RATP sur la création et l'usage des données

# Chronologie



# Création minimale de données

## Finalités

Collecte de données  
pour des finalités  
déterminées,  
explicites et légitimes



## Finalités

1. Lutte contre la fraude
2. Réalisation des opérations d'après-vente
3. Établissement de statistiques



## Proportionnalité



## Qualité des données personnelles

Adéquates  
Pertinentes  
Non excessives



## Données personnelles créées

1. N° de série du passe à 11 chiffres, Authentifiant du passe et période de validité
2. N° d'abonnement
3. Type de contrat (annuel, mensuel, jour)
4. Validité temporelle et géographique
5. Type d'évènement : date, heure et lieu, entrée, sortie, correspondance, réseau
6. Si refus de validation : date, heure, lieu, motif du refus
7. Photo



# Limitation des informations transmises



- 1. Identifiant anonyme
- 3. Type de contrat
- 5. Type d'événement
- Résultat de la validation

*Données écrasées dans la nuit*

5. Date, Heure, lieu

Base de  
Données  
Clients

## Serveur central

### Serveur de tri et redistribution

*Données effacées en fin de journée  
qu'elles soient transmises ou non*

Serveur 1 - **Fraude**

Serveur 2 – **Statistiques**

Fréquentation  
Compensations financières

# Durée de conservation

## Serveur central

### Serveur 1 Fraude

#### Données indirectement nominatives

- Données de validation associées au n° de série de la carte : J + 1 (2 heures en pratique)
- S'il y a alarme : 2 semaines pour analyse (1 alarme sur 1 million de validation)



#### Traitement Infractions

- Si fraude avérée : 6 mois
- Instruction judiciaire

### Serveur 2 Statistiques

#### Données anonymes

- Utilisation d'un identifiant anonyme du passe calculé à partir du n° de série de la carte et de l'authentifiant du passe inscrit en usine via une fonction de hachage
- ? **Irréversibilité de la fonction de hachage**
- ? **Statistique si peu de voyageur à un endroit**

# Gestion de l'accès aux données

## Obligation de sécurité et de confidentialité

### Contrôleurs et agents de guichet

1. N° de série à 11 chiffres
3. Type de contrat (annuel, mensuel, jour)
5. Date, heure et lieu des 3 dernières validations (écrasement)
7. Photo

### Voyageur

Données du passe : guichets et contrôleurs  
Liste noire : département commercial  
Profil client : site Internet

### Agents

Accès à la BDD clients  
Nom, prénom, adresse, etc.

### Personnes non autorisées

- Carte Navigo
- Distance de lecture : 10 cm (sans cryptage)
- Juillet 2006 : accès aux formulaires en ligne via l'URL

# Non création de données personnelles

Consentement  
de l'utilisateur



## Arguments RATP

1. Liberté de souscrire au contrat Navigo
2. Gestion volontaire de validation qui correspond à une acceptation explicite
3. Passe Navigo découverte



- Pas d'association à un numéro d'abonné ou à un nom de client
- Données : 5. Date, heure et lieu des 3 dernières validations
- Serveur Statistiques uniquement





# Anonymisation : cout

## Liberté d'aller et venir

- **Demande de la CNIL dans son avis du 8 avril 2004**
  - Lancement 6 ans après de Navigo Découverte le 1<sup>e</sup> septembre 2007
- **Pas de fichier central**
  - Pas d'émission automatique de nouvelle carte ou de remboursement

## Cout

- **5 euros pour une validité annoncée de 10 ans**
  - Et non une caution
  - Navigo : 0 euro, puis 8 euros
- **La Cnil regrette ce surcoût « qui remet en cause la liberté d'aller et venir »**
  - Pas de principe d'anonymat gratuit dans la loi
  - Décision politique du STIF

# Manque de transparence

## Droit d'information

- Pas d'information précise sur le fonctionnement du système
- Agence : peu d'information sur **Navigo Découverte**
  - Test CNIL dans 20 stations en janvier 2009 : condition d'information et d'obtention médiocre

## Droit d'accès et de rectification

- Droit d'accès qui s'exercent à différents endroits selon le type d'abonnement et de transport
  - Agence carte Orange à Cergy-Pontoise
  - Agence Carte intégrale au Futuroscope
  - RATP, OPTILE, SNCF

# Accès aux données par les autorités policières et judiciaires

## ■ Commission rogatoire : le CIL veille

- Peu utilisée car accès limité à 48 heures MAXIMUM

## ■ ? Nouvelle loi

- Mouvement sécuritaire
  - Les opérateurs de communications électroniques doivent conserver les données de trafic pendant un an
  - Vidéosurveillance/Vidéoprotection
- ? Délai de conservation des données
- ? Finalités : sécurité versus libertés
  - Lutte contre le terrorisme et la grande criminalité
  - Recherche d'un mineur
  - Criminalité « ordinaire »



### **3. La protection des données personnelles au delà du cadre français**

# Un droit fondamental

## ■ Droit à la protection de sa vie privée : art. 7 de la Charte des droits fondamentaux de l'Union européenne

- Droit de ne pas voir révéler des informations liées à sa sphère intime (sphère physique mais aussi expression d'une relation avec autrui), pour permettre à la personne de s'épanouir
- Protège l'opacité
- Droit défensif : l'atteinte doit avoir eu lieu pour bénéficier de la protection

## ■ Droit à la protection des données à caractère personnel : art. 8 de la Charte des droits fondamentaux de l'Union européenne

- Droit préventif : protéger l'individu par rapport à un risque précis, celui lié à l'usage des technologies de l'information
- Protège la vie privée mais aussi d'autres libertés (libertés d'expression, de communication, etc.) et la non discrimination
- Objectif atteint
  - En limitant les activités de traitement
  - En permettant à la personne de maîtriser la circulation de son image informationnelle

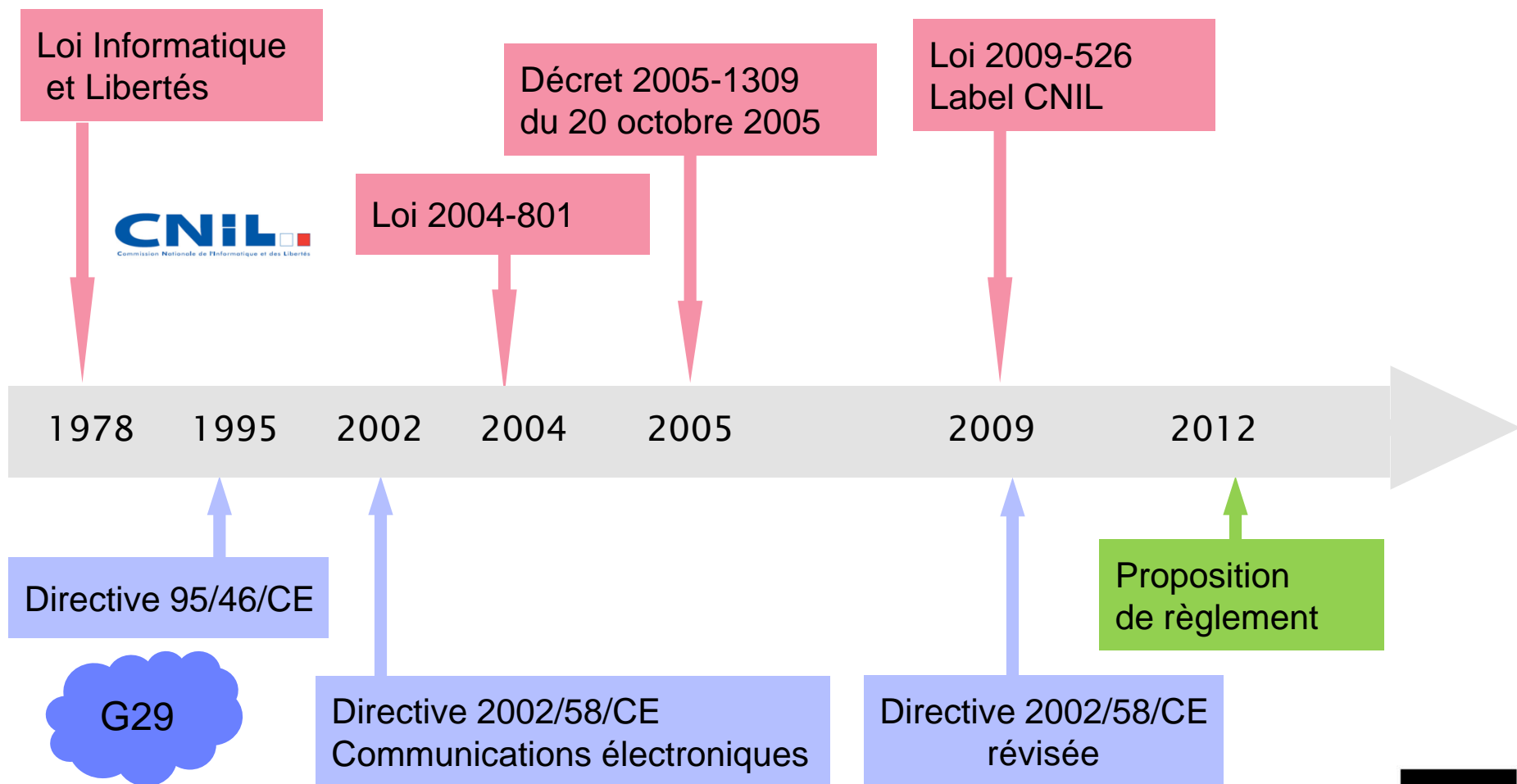
# Données personnelles : Monde

- **La protection des données personnelles est un droit de l'homme**
- **Union européenne**
  - Charte des droits fondamentaux de l'UE du 18 déc. 2000 : article 8
  - Traité de Lisbonne sur le fonctionnement de l'UE du 1<sup>er</sup> nov. 2009 : article 16
  - Directive 95/46/CE en cours de révision
- **Conseil de l'Europe : 47 Etats**
  - Convention européenne des droits de l'homme
  - Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 ratifiée par 44 États (Seul instrument international juridique contraignant)
- **OCDE : 34 pays : Lignes directrices de 1980 révisées en 2013**
- **APEC : 21 pays : Privacy Principles, December 2005**
- **Réglementation dans 85 pays dont les États-Unis**
- **Pour aller plus loin : The Futures of Privacy, colloque international, Institut Mines, 17/10/2013** (Global Privacy Governance and Legal Issues : <http://www.canalc2.tv/video.asp?idEvenement=715> )



# Les négociations actuelles au niveau de l'Union européenne

# Union européenne





# 1. Conseil Européen

Réunion des chefs d'Etats et de gouvernement 4 fois par an

Président permanent élu pour 2,5 ans, renouvelable 1 fois

Définit les grandes orientations et donne les impulsions

## 2. Commission européenne

*Exprime l'intérêt général européen*

Monopole de l'initiative législative

1 commissaire par Etat membre sans limitation de durée

Investie par le Parlement européen

Propose les directives et les règlements aux 2 organes législatifs

Assure le respect des traités

Responsable des politiques communes

Haut représentant pour les affaires étrangères  
également vice-président de la Commission

## 5. Cour de Justice de l'Union européenne

Assure le respect du droit de l'UE dans son interprétation et son application

Election du président de la Commission par le Parlement sur proposition du Conseil

## 3. Conseil des ministres

*Représente les Etats membres*

Organe législatif

Conseils techniques

Conseil Affaires générales

Conseil Affaires étrangères

## 4. Parlement européen

*Représente les citoyens*

Organe législatif : vote les lois et le budget européen avec le conseil des ministres

Législateur principal avec le Conseil des ministres

préside

Opère les arbitrages au sein du Conseil des ministres

# De la directive 95/46/CE au règlement (Union européenne)

## Directive

- Doit être transposée en droit national pour entrer en application dans chaque Etat
- Transposition obligatoire dans des délais fixés
- Lie tout Etat membre quant au résultat à atteindre en leur laissant la compétence quant à la forme et aux moyens
- Laisse une marge de manœuvre aux États
- La transposition varie selon le contexte historique, sociologique ...

## Règlement

- Directement applicable et obligatoire dans tous les États
- Publié au journal officiel de l'Union européenne : en générale s'applique 20 jours après
- Il n'est pas nécessaire d'adopter des dispositions d'exécution dans la législation nationale
- 2 ans pour se mettre en conformité
- ? Harmonisation totale

# Révision de la directive 95/46/CE

## ■ Février 2009 : Groupe d'experts désignés par la Commission européenne chargé de faire des propositions sur la révision

- Composé de 4/5 de personnalités représentant les intérêts américains
- Les Etats-Unis exercent une pression pour diminuer le niveau de protection
- Dissolution à la demande du Sénat français (et d'Alex Turk)

## ■ Ambition de Viviane Reading : réformer en profondeur

- Les principes essentiels sont toujours valables
- Moderniser le cadre légal, en particulier
  - Faire face aux défis posés par la globalisation et les nouvelles technologies : réseaux sociaux, vidéosurveillance, big data
  - Neutralité technologique
- Renforcer les droits des individus
- Réduire les formalités administratives pour assurer la libre circulation des données
- Renforcer la cohérence et clarifier les règles
- Rendre la protection effective

# Révision de la directive 95/46/CE

- **Décembre 2009** : consultation publique via un questionnaire
  - A l'époque, la proposition de la Commission était prévue pour novembre 2010 (soit 3 mois pour rédiger la proposition)
- **Août 2010** : l'agenda est reporté sous la pression des CNILs européennes (notamment de la CNIL)
  - Viviane Reading s'est rendu compte qu'il y avait un gros travail à fournir compte tenu de ses ambitions de réforme, chose que son personnel limité ne lui permettait pas
- **4 novembre 2010** : communication de la Commission européenne : Une approche globale de la protection des données à caractère personnel dans l'Union européenne
- **Jusqu'au 15 janvier 2011** : consultation publique sur les propositions faites dans la communication
- **25 janvier 2012** : proposition de règlement pour le cadre général + proposition de directive pour le domaine Police-justice
- **16 janvier 2013** : projet de rapport sur la protection de règlement, Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen (LIBE), rapporteur Jan Philipp Albrecht
- **22 octobre 2013** : adoption par la Commission LIBE du Parlement européen
- **12 mars 2014** : adoption en 1<sup>e</sup> lecture par le Parlement européen

# Révision de la directive 95/46/CE

- **22 – 25 Mai 2014 : élection des députés européens**
- **15 juillet 2014 : discours au Parlement européen de Jean-Claude Junker, Président de la Commission européenne**
  - Annonce son intention dans les six mois « de prendre d'ambitieuses mesures législatives visant à créer un marché unique du numérique connecté, notamment en concluant rapidement les négociations relatives à des règles européennes communes en matière de protection des données ».
  - A propos de l'accord de libre-échange avec les États-Unis, il est très clair : « je serai aussi très clair: je ne sacrifierai pas les normes européennes de sécurité, de santé, les normes sociales, les normes de protection des données ou notre diversité culturelle sur l'autel du libre-échange »

# Projet de règlement

## ■ Droit à l'oubli numérique

- Droit de demander l'effacement de ses données s'il n'existe pas de motif légitime pour les conserver (recherche historique ou scientifique, santé publique ...) avec informations au tiers
- Arrêt CJUE Google Spain
- Problème notamment des copies de sauvegarde

## ~~■ Droit à la portabilité~~

- ~~• Droit de demander, sous un format structuré et compréhensible, une copie de toutes ses données, éventuellement pour les transmettre à un autre prestataire~~

## ■ Renforcement du consentement préalable : consentement "explicite"

## ■ Traitement de données relatives aux enfants

- Si des biens ou des services sont offerts à des enfants de moins de 13 ans : consentement par un parent ou un responsable

## ■ Privacy by design

- Protection des données dès la conception d'un système
- Protection des données par défaut

# Projet de règlement

## ■ Passage d'une logique binaire

- Formalités préalables / contrôle a posteriori

## ■ A une logique de mise en conformité évolutive

- Peu de formalités
- Renforcement des contrôles et sanctions
- Responsabilisation des acteurs : obligation de rendre des comptes (principle of accountability)
  - Mise en place de **politiques internes de conformité**
  - Processus permanent permettant de démontrer que l'entreprise respecte la réglementation
    - Tenue d'une documentation interne
    - Désignation d'un correspondant Informatique et Libertés
    - Etudes d'impacts pour les traitements à risque
    - Réalisations régulières d'audits ...

# Projet de règlement

## ■ Critère de l'établissement principal

- Guichet unique : compétence d'une seule autorité, celle où le responsable de traitement a son principal établissement
- Contesté par la CNIL
  - Plainte d'un citoyen auprès d'une autorité étrangère / puis d'un tribunal étranger
  - // droit de la consommation : lieu de résidence du citoyen
  - Forum shopping : choix d'implantation d'une entreprise fonction de la législation



# Conclusion



- Un traçage et des risques accrus
- Une société de la surveillance ? Cf PRISM
- De nouveaux équilibres à atteindre ?
- Possibilité de « bon » big data

# Bibliographie : France

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF du 7 janvier 1978, p. 227 ; modifiée notamment par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, JORF du 7 août 2004 (Loi dite Informatique et Libertés).
- Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO n° 182 du 7 août 2004, p. 14063. (Directive 95/46 du Parlement et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données).
- Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004, JORF du 22 octobre 2005 ; modifié par :
- Décret n° 2007-451 du 25 mars 2007 modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004, JORF du 28 mars 2007.
- Code Pénal Articles 226-16 à 24 (Section 5 Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques)
- Commission générale de terminologie et de néologie, Vocabulaire des télécommunication, termes et définitions de la radio-identification, JORF du 9 septembre 2006.
- Décret n° 2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique et modifiant le code de la santé publique (dispositions réglementaires), JORF du 16 mai 2007, p. 9362.

# Bibliographie : Union européenne

- Charte européenne des droits fondamentaux de l'Union européenne signée le 7 décembre 2000 à Nice, JOCE C 364 du 18 décembre 2002, p. 1.
- Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE L 281 du 23 novembre 1995, p. 31. (Directive "Protection des données").
- 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, JOCE L 2001 du 31 juillet 2002, p. 37. (Directive « Vie privée et communications électroniques »)
- Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, JOUE L 105 du 13 avril 2006, p. 54.
- Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, JOUE L 337 du 18 décembre 2009, p. 11.

# Bibliographie : Union européenne


- Proposition de règlement du Parlement européen et du Conseil 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 du 25 janvier 2012, COM (2012)11 final
  - Dernière version : Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données) ([COM\(2012\)0011](#) – C7-0025/2012 – [2012/0011\(COD\)](#))
- Groupe de travail Article 29 : [http://ec.europa.eu/justice/data-protection/article-29/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/index_en.htm)
  - *Avis 4/2007 sur le concept des données à caractère personnel*, adopté le 20 juin 2007, WP 136.
- Cour de Justice de l'Union européenne
  - Droit à l'oubli : Arrêt du 13 mai 2014 dans l'affaire C-131/12, Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González
  - Invalidation de la directive Conservation des données ; Arrêt du 8 avril 2014, affaires jointes C-293/12 et C-594/12, Digital Rights Ireland et Seitlinger e.a.

## Bibliographie : sites web


- Commission européenne : [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)
- Groupe article 29 : [http://ec.europa.eu/justice/data-protection/article-29/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/index_en.htm)
- CNIL : [www.cnil.fr](http://www.cnil.fr)
  - « Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing »
- Assemblée nationale : <http://www.assemblee-nationale.fr>
- Sénat : [www.senat.fr](http://www.senat.fr)

# Chaire Valeurs et politiques des informations personnelles

[www.informations-personnelles.org](http://www.informations-personnelles.org)



Les rencontres de la Chaire  
Valeurs et politiques des informations personnelles



**Quelles pistes concrètes pour  
la réappropriation des informations  
personnelles par le citoyen ?**

**mardi 17 juin 2014**


**17h à 19h Amphi B 312**

Avec

**Daniel Kaplan**  
Délégué général de la FING

**Benjamin Sonntag**  
Entrepreneur et informaticien  
Co-fondateur de La Quadrature du Net

[www.informations-personnelles.org](http://www.informations-personnelles.org)



Les précédents débats de la Chaire ont notamment exploré la dissymétrie existant aujourd'hui entre les citoyens et les acteurs étatiques ou privés qui détiennent les informations personnelles. Cette rencontre s'est concentrée sur les initiatives concrètes, y compris techniques, qui ont pour but de permettre à l'utilisateur final de se réappropriier les données le concernant, et de devenir par-là même un véritable acteur dans la société dont les mécanismes économiques et sociaux sont aujourd'hui basés sur la circulation des données. Pour permettre cette réappropriation, suffit-il que l'utilisateur bénéficie d'outils techniques limitant la circulation de ses données ? Le citoyen doit-il intervenir dans la définition des conditions de leur utilisation et si oui, de quelle manière ? Sur quels types de valeurs, économiques ou sociétales, cette réappropriation doit-elle s'appuyer ? Quels sont les outils techniques existants ou en cours de développement, mais peu connus du grand public ?