# La protection des données personnelles vue par un informaticien

Guillaume Piolle
CentraleSupélec / Inria, équipe CIDRE (Rennes)
guillaume.piolle@centralesupelec.fr

Journées thématiques LYRICS,
27 mai 2015

# Le cadre juridique

- **ONU :**
  - 1948 - Déclaration universelle des droits de l'homme (art. 12) ;
  - 1966-1980 : Pactes à force contraignante (droits civils et politiques, droits économiques, sociaux et culturels).
- **Conseil de l'Europe :**
  - 1950 - Conv. de sauvegarde des droits de l'homme et des libertés fondamentales (art. 8) ;
  - 1981 - **Conv. pour la prot. des pers. à l'égard du traitement automatisé des données à caractère personnel** (en particulier préambule, art. 5).
- **Union européenne :**
  - 1992-2007 - Traité de l'Union européenne (inclut la CSDHLF) ;
  - 2000-2010 - Charte des droits fondamentaux de l'Union européenne ;
  - 1995 : **Directive 95/46/CE**
  - 2002 : Directive 2002/58/CE
  - 2015 ? - Projet de réglement européen en remplacement de 95/46.
- **France :**
  - 1978-2004 : **Loi 78-17 « Informatique et Libertés »**

# Droit à la vie privée *vs* Protection des données personnelles

## Droit à la vie privée

**Droit « correctif »**
Notion de préjudice et de réparation
Il faut démontrer le préjudice

# Droit à la vie privée *vs* Protection des données personnelles

## Droit à la vie privée

**Droit « correctif »**
Notion de préjudice et de réparation
Il faut démontrer le préjudice

## Protection des données personnelles

**Droit « préventif »**
Règles visant à éviter les violations de la vie privée
La violation des règles constitue un préjudice en soi, par principe

# Les principes fondamentaux de la PDP

## Donnée à caractère personnel (donnée personnelle)

Loi I&R, article 2 :

Constitue une donnée à caractère personnel **toute information relative à une personne physique identifiée ou qui peut être identifiée**, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer **l'ensemble des moyens** en vue de permettre son identification dont dispose ou auxquels peut avoir accès **le responsable du traitement ou toute autre personne**.

Directive européenne et projet de réglement : notion de « moyens susceptibles d'être raisonnablement mis en œuvre ».

# Informatique et Libertés : Principes

- **Principe de légalité :** Les traitements sur certains types de données sont interdits (voir plus loin) ;
- **Principe de finalité :** On collecte des données en vue d'une finalité déterminée, et qui doit être respectée ;
- **Principe de légitimité :** La finalité poursuivie doit être légitime pour le responsable du traitement ;
- **Principe de proportionnalité :** La collecte doit être proportionnelle (nature, quantité et durée de conservation des données) à la finalité.

# Informatique et Libertés : Principes

## Données sensibles

Il est interdit de procéder à des traitements portant sur des données sensibles :

- Origines raciales ou ethniques ;
- Opinions politiques, philosophiques, religieuses ;
- Appartenance syndicale ;
- Santé et vie sexuelle.

Exceptions : consentement exprès, sauvegarde de la vie humaine, gestion des listes de membres, données déjà rendues publiques par la personne concernée, services de santé, statistiques officielles, recherche médicale, procédures judiciaires, « intérêt public » (strictement encadré).

# Informatique et Libertés : Formalités préalables

## Régime de déclaration

Cas par défaut (pas de données sensibles). Dispense de déclaration si présence d'un CIL dans l'organisation.

## Régime d'autorisation (ou avis)

Traitements portant sur des données sensibles, génétiques, biométriques, relatives aux infractions ou condamnations, ou susceptibles de priver d'un droit, ou utilisant le numéro INSEE...

# Informatique et Libertés : Droits et obligations

## Droits des personnes concernées

- Obligation d'information sur le responsable de traitement, la transmission des données à des tiers. . . (notion de **collecte loyale**) ;
- Droit d'accès et de rectification ;
- Droit d'opposition *pour des motifs légitimes* ;
- Droit de suppression *en cas de non-conformité*.

## Obligations du responsable de traitement

Il doit garantir les principes de légalité, de finalité, de légitimité et de proportionnalité.
Il doit garantir les droits des personnes concernées (notamment via les « mentions obligatoires ») et est responsable de la confidentialité des données dont il a la garde.

# Mobilité et géolocalisation

## Cadre juridique

- La géolocalisation n'est pas citée dans le texte de la loi ;
- En particulier, pas soumis (a priori) au régime d'autorisation ;
- Cadre général : déclaration, droits et devoirs « standards » + jurisprudence et recommandations de la CNIL.

# Mobilité et géolocalisation

## Cadre juridique

- La géolocalisation n'est pas citée dans le texte de la loi ;
- En particulier, pas soumis (a priori) au régime d'autorisation ;
- Cadre général : déclaration, droits et devoirs « standards » + jurisprudence et recommandations de la CNIL.

## Oui mais. . .

- Et si les données de mobilité permettent d'inférer des données sensibles, ou relatives à des infractions (par exemple) ?

# Les exceptions applicables en recherche

## La mauvaise nouvelle

La loi Informatique et Libertés s'applique aux activités de recherche.

# Les exceptions applicables en recherche

## La mauvaise nouvelle

La loi Informatique et Libertés s'applique aux activités de recherche.

## Les bonnes nouvelles

- Possibilité de conserver les données au-delà des nécessités de la finalité initiale, à des fins historiques, statistiques et de recherche scientifique (mais en base « inactive ») ;

# Les exceptions applicables en recherche

## La mauvaise nouvelle

La loi Informatique et Libertés s'applique aux activités de recherche.

## Les bonnes nouvelles

- Possibilité de conserver les données au-delà des nécessités de la finalité initiale, à des fins historiques, statistiques et de recherche scientifique (mais en base « inactive ») ;
- En cas de réutilisation de données collectées par d'autres :

# Les exceptions applicables en recherche

## La mauvaise nouvelle

La loi Informatique et Libertés s'applique aux activités de recherche.

## Les bonnes nouvelles

- Possibilité de conserver les données au-delà des nécessités de la finalité initiale, à des fins historiques, statistiques et de recherche scientifique (mais en base « inactive ») ;
- En cas de réutilisation de données collectées par d'autres :
  - Les finalités historiques, statistiques et scientifiques sont considérées *a priori* comme compatibles avec toute finalité initiale ;

# Les exceptions applicables en recherche

## La mauvaise nouvelle

La loi Informatique et Libertés s'applique aux activités de recherche.

## Les bonnes nouvelles

- Possibilité de conserver les données au-delà des nécessités de la finalité initiale, à des fins historiques, statistiques et de recherche scientifique (mais en base « inactive ») ;
- En cas de réutilisation de données collectées par d'autres :
  - Les finalités historiques, statistiques et scientifiques sont considérées *a priori* comme compatibles avec toute finalité initiale ;
  - Pas d'obligation d'informer si l'information « se révèle impossible ou exige des efforts disproportionnés ».

# Les exceptions applicables en recherche

## La mauvaise nouvelle

La loi Informatique et Libertés s'applique aux activités de recherche.

## Les bonnes nouvelles

- Possibilité de conserver les données au-delà des nécessités de la finalité initiale, à des fins historiques, statistiques et de recherche scientifique (mais en base « inactive ») ;
- En cas de réutilisation de données collectées par d'autres :
  - Les finalités historiques, statistiques et scientifiques sont considérées *a priori* comme compatibles avec toute finalité initiale ;
  - Pas d'obligation d'informer si l'information « se révèle impossible ou exige des efforts disproportionnés ».

Il peut demeurer des problèmes liés à l'information des personnes concernées lorsque le chercheur crée/collecte lui-même les données (non couvert par la précédente exception).

# Le projet de réglement européen

## Quelques modifications envisagées

- Renforcement de l'importance du consentement (distinct et révocable pour chaque traitement) ;
- Renforcement d'un droit à l'effacement explicitement mentionné ;
- Obligations de journalisation et d'auditabilité plus lourdes pour les responsables de traitement (cf charge de la preuve) ;
- Obligation de notification (à l'autorité de contrôle et aux personnes concernées) de toute « brèche de vie privée » constatée, sous 72h ;
- Obligation d'effectuer un *privacy impact assessment* avant la demande d'une autorisation de traitement ;
- Le « délégué à la protection des données » (CIL) devient obligatoire dans les organisations publiques et les entreprises de 250+ salariés. Son indépendance doit être garantie ;
- Sanctions administratives graduées (en sus des sanctions pénales nationales), allant jusqu'à 100 M€ ou 5% du CA mondial.

# Données personnelles et vie privée au travail

## Principe général

Dans le cas général, le salarié a le droit d'utiliser ponctuellement les moyens mis à sa disposition par son employeur pour des fins personnelles.
Il ne doit bien sûr pas en abuser...

## L'accès de l'employeur aux e-mails

Arrêt « Nikon » (2001) de la chambre sociale de la Cour de cassation
Si un e-mail est marqué comme personnel, ou classé dans un dossier confidentiel, l'employeur ne peut en prendre connaissance (secret des correspondances).
Dans les autres cas, il y a présomption de caractère professionnel.

# Données personnelles et vie privée au travail

## L'accès de l'employeur aux fichiers

Arrêt « The Phone House » (2007) de la chambre sociale de la Cour de cassation : extension du principe aux fichiers (y compris la présomption de caractère professionnel).

Arrêt de 2005 : « sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé ».

# Données personnelles et vie privée au travail

## L'accès de l'employeur aux fichiers

Arrêt « The Phone House » (2007) de la chambre sociale de la Cour de cassation : extension du principe aux fichiers (y compris la présomption de caractère professionnel).

Arrêt de 2005 : « sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé ».

Chambre sociale, 2011 : « Si l'employeur peut toujours consulter les fichiers qui n'ont pas été identifiés comme personnels par le salarié, il ne peut les utiliser pour le sanctionner s'ils s'avèrent relever de sa vie privée. »

# Données personnelles et vie privée au travail

Arrêt de 2009 : l'administrateur « est tenu d'une **obligation de confidentialité** » (même vis-à-vis de l'employeur) et peut accéder aux données des courriers électroniques échangés par les salariés uniquement « dans le cadre de sa mission de sécurité du réseau informatique ».

# Données personnelles et vie privée au travail

Arrêt de 2009 : l'administrateur « est tenu d'une **obligation de confidentialité** » (même vis-à-vis de l'employeur) et peut accéder aux données des courriers électroniques échangés par les salariés uniquement « dans le cadre de sa mission de sécurité du réseau informatique ».

## Et pour la consultation de sites web ?

À ma connaissance, pas d'arrêt de la Cour de cassation dans ce sens. . .

L'employeur a, a priori, le droit d'accéder à tous les sites web consultés par les salariés.

# Données personnelles et vie privée au travail

## Géolocalisation des salariés

Particulièrement pertinent pour les sociétés de transport : maintien de statistiques sur les trajets, contrôle des itinéraires...

La CNIL considère que le salarié doit pouvoir désactiver le dispositif à l'issue de son temps de travail.

Attention à la finalité déclarée du traitement : si c'est les stats et l'optimisation, impossible de s'en servir à titre disciplinaire contre le salarié.
Attention également si le salarié dispose de la liberté d'organisation de son temps de travail.

## Documents CNIL

- *Travail et données personnelles : la géolocalisation des véhicules*
- *Guide de la géolocalisation des salariés*

# Données personnelles et vie privée au travail

## Vidéosurveillance au travail

Finalités autorisées : sécurité des biens et des personnes (dissuasion, identification des responsables)

- **On peut filmer :** entrées et sorties des bâtiments, issues de secours, voies de circulations, zones de stockage de marchandises. . .
- **On ne peut pas filmer :** employés sur leur poste de travail, zones de pause ou de repos, toilettes, locaux syndicaux et de RP (y compris leur accès).

→ Accès limité (personnel de sécurité)
→ Conservation limitée à **un mois**

Formalités auprès de la CNIL, de la préfecture, des instances représentatives du personnel.
Chaque employé doit être informé **individuellement**, en sus de l'affichage obligatoire.