# Big data et protection des données personnelles

Séminaire Aristote – Ecole Polytechnique

15 octobre 2015

Sophie Nerbonne

Directrice de la conformité à la CNIL

# La CNIL : autorité en charge de la protection des données personnelles

- Autorité administrative indépendante créée en 1978, en charge de l'application de la **loi Informatique et Libertés** du 6 janvier 1978 modifiée.

- Qu'est-ce que la protection des données personnelles ?
  - Toute personne a droit à la **protection de ses données personnelles**. Il s'agit d'un droit fondamental et des règles encadrent les traitements de données personnelles.
  - Toute personne peut saisir **l'autorité de contrôle** lorsque ses données ne sont pas traitées conformément aux règles applicables.
  - Le régime juridique applicable a été notamment adopté au niveau européen, pour assurer un **haut niveau de protection**. Il est actuellement en cours de révision.
  - Des autorités de protection des données sont établies dans les différents pays européens.
  - La situation est différente dans le reste du monde. De nombreux pays ont des autorités de protection des données, mais peu assurent un niveau de protection équivalent.

# Ce haut niveau de protection est-il adapté aux nouveaux défis du Big data ?

- **Qu'est-ce que le « Big data » ?**

  - Définition officielle adoptée par la Commission générale de terminologie et de néologie en août 2014. Les « *mégadonnées* » sont des « *données structurées ou non dont le très grand volume requiert des outils d'analyse adaptés* ».
  - Etude du cabinet Gartner et la célèbre règle des 3 V : Volume, Vitesse et Variété. De nouveaux V apparaissent (Valeur, Véracité, etc.).

- **Quels sont les nouveautés et enjeux liés au Big data?**

  - Phénomène de datafication (lié à la multiplication des objets connectés, des smartphones, etc.) : il est estimé que 90% des données récoltées depuis le début de l'humanité ont été créées durant les deux dernières années.
  - Révolution dans le stockage et les capacités de traitement permettant de traiter tous types de données, en vue de créer de la valeur.
  - Une nouvelle ère cognitive ?

# Big data et protection des données personnelles

- **La « vague » Big data semble toucher tous les domaines** : marketing, e-commerce, assurance, lutte contre la fraude, tourisme, ressources humaines, domaine scientifique et environnemental, santé, etc.

- **Tous les projets Big data sont-ils concernés ?**
  - Certains projets sont mis en place sans recourir au traitement de données à caractère personnel (par exemple, dans les domaines de la géologie ou de la météorologie où des capteurs permettent de surveiller et de préciser le déclenchement de phénomènes naturels).
  - Mais de nombreux traitements impliquent le traitement de données personnelles, issues de sources variées (données internes à l'organisme mais aussi des données issues d'objets connectés, de capteurs, de cartes de fidélité, de l'open data, etc.).

- **Quelles incidences du Big data sur les personnes concernées ?**
  - Le Big data offre la possibilité d'une connaissance plus fine des populations ciblées.
  - Le Big data peut permettre la construction de modèles prédictifs de comportements – voire de prise de décision.

# Enjeux Informatique et libertés liés au Big data

- **La grille d'analyse de la protection des données : les 5 règles d'or**
  - Principes de finalité et de proportionnalité.
  - Pertinence des données traitées.
  - Conservation limitée des données.
  - Sécurité et confidentialité.
  - Respect des droits des personnes concernées : loyauté et transparence (droit à l'information, consentement, droits d'opposition, d'accès et de rectification).

- **Position des CNIL européennes** (Statement du G29 de septembre 2014 et Working paper du Groupe de Berlin de mai 2014)
  - Le Big data doit se développer en conformité avec les principes fondamentaux de la protection des données personnelles.
  - Dans le contexte du Big data, une approche ouverte de ces principes semble nécessaire. Les organismes doivent également innover pour pouvoir les appliquer.
  - Si le recours à des techniques d'anonymisation des données est utilisé pour sortir du champ d'application de la loi, il faut veiller à mettre en place des procédures robustes d'anonymisation (avis du G29 sur les techniques d'anonymisation).
  - Une approche de *privacy by design* et d'*accountability* doit être encouragée.

# Exemple concret : le partenariat FIEEC-CNIL

- **Objectifs du groupe de travail créé en 2012 :**

  - Aboutir à la publication d'un référentiel de bonnes pratiques visant à accompagner l'innovation des industriels en intégrant la *privacy by design.*

  - Ces travaux concernent uniquement les traitements de données collectées via des appareils ou logiciels installés par les usagers en aval des compteurs électriques (prise sur le compteur ou tableau électrique).

  - Sont donc exclus les traitements de données réalisés directement via les compteurs électriques.

  - La démarche de travail était avant tout centrée sur l'usager.

  - Caractère souple et évolutif de ces lignes directrices.

- **Résultats :**

  - En un an: 4 réunions de travail et échanges en sous-groupe également (4 réunions) au cours de l'année 2013, présentation au collège de la CNIL, transmission à la CRE.

# Recommandations du groupe de travail FIEEC-CNIL

3 cas d'usage des données de consommation électrique ont été identifiés par le groupe de travail:

1. **'IN → IN'**
   - Les données collectées dans le logement restent dans le logement

2. **'IN → OUT '**
   - Les données collectées dans le logement sont transmises à l'extérieur

3. **'IN → OUT → IN'**
   - Les données collectées dans le logement sont transmises à l'extérieur pour permettre un pilotage à distance de certains équipements de logement

■ **Des recommandations ont été produites dans chaque cas, détaillant les types de traitement possibles.**

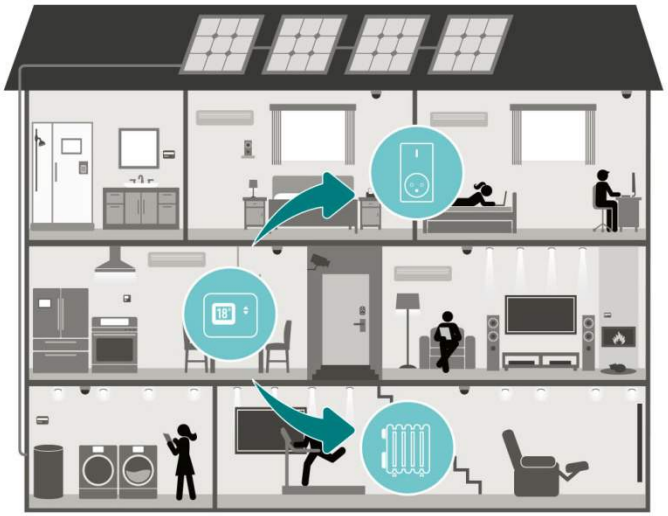
# Scénario IN→IN

Les données collectées dans le logement restent ***sous la maitrise unique du client.***

2 cas de figure:

## 1. Applications purement IN → IN

- Aucune sortie des données vers l'extérieur, les différents produits communiquent à l'intérieur du logement.
- *Exemples*: communication entre le thermostat et le chauffage, mise en veille de la maison au départ de l'occupant etc.



## 2. Applications avec une sortie des données du logement

- Les données ne sont pas transmises à un tiers, mais peuvent communiquer sur des réseaux de communications (type Wifi, ADSL, réseau local etc.).
- *Exemple*: application Smartphone qui communique directement avec le matériel du client.

- **Finalités**
  - Gestion des équipements et information sur la consommation.
  - Information sur la consommation dans les logements neufs au titre de la Règlementation thermique 2012.

- **Destinataires**
  - Seule la personne concernée peut avoir accès aux données.

- **Données collectées**
  - Seules les données nécessaires à la finalité poursuivie par le traitement peuvent être collectées.

- **Durée de conservation**
  - Temps de conservation déterminé par le client.
  - La suppression des données s'effectue grâce à un moyen prévu dans le dispositif lui-même.
  - Suppression systématique des données existantes lorsque le prestataire récupère le dispositif.

- **Sécurité**
  - Mise en place de mesures garantissant la confidentialité des données traitées en empêchant la prise de contrôle par toute personne non-autorisée.

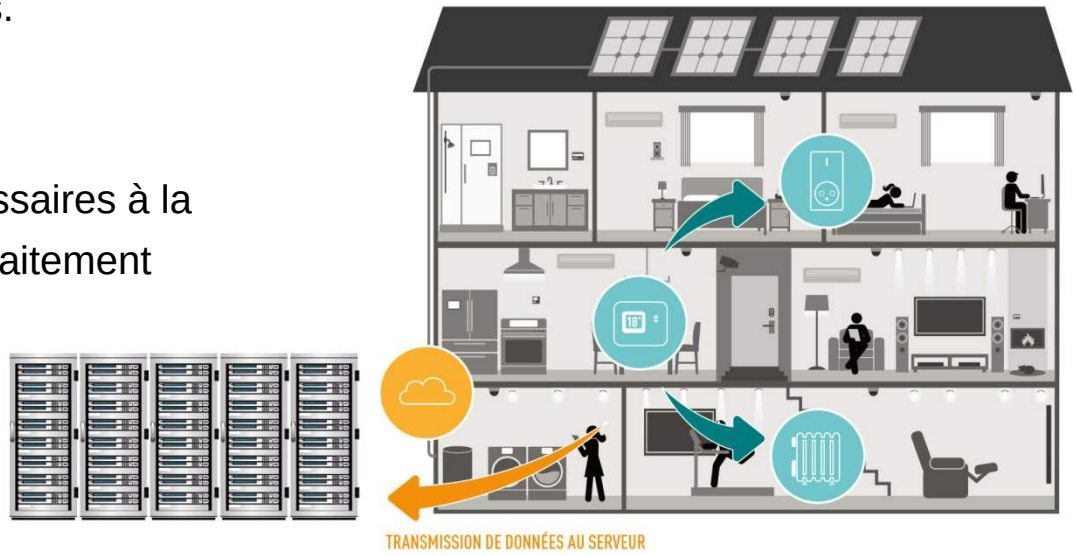
- **Démarche auprès de la CNIL**
  - Pas de formalités à effectuer auprès de la CNIL.

# Scénario IN→OUT

Les données collectées dans le logement sont transmises à l'extérieur.

- **Finalités**
  - Suivi de la consommation du logement par le prestataire ou par les bailleurs sociaux.
  - Réalisation de bilans énergétiques.
  - Prospection commerciale.
  - Optimisation des modèles.

- **Données collectées**
  - Seules les données nécessaires à la finalité poursuivie par le traitement peuvent être collectées.



## Durée de conservation

- Données commerciales: conservation pendant toute la durée du contrat.
- Données de consommation: conservation pendant une durée déterminée du contrat.
- Pour l'optimisation des modèles, les données peuvent être conservées pour une durée illimitée.

## Destinataires

- Client et prestataire.
- Le prestataire peut transmettre les données à un sous-traitant ou partenaire commercial.

## Information et droits des personnes

- Obligation d'informer le client lors de la signature du contrat de prestation de service.
- Droit d'accès du client, et de rectification ou suppression de ses données.

## Sécurité

- Mise en place de mesures garantissant la confidentialité des données traitées en empêchant la prise de contrôle par toute personne non-autorisée.

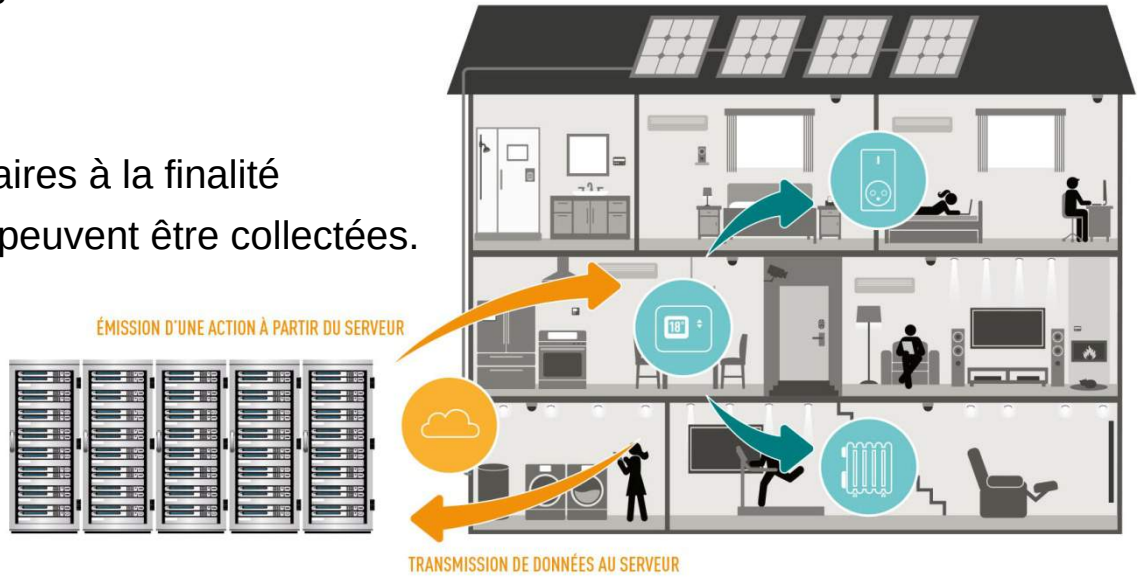
## Démarche auprès de la CNIL

- Déclaration du prestataire auprès de la CNIL.

# Scénario IN→OUT→IN

Les données collectées dans le logement sont transmises **à l'extérieur pour permettre un pilotage à distance de certains équipements du logement.**

- **Finalités**
  - Effacement de la consommation du logement.
  - Efficacité énergétique du logement.
  - Prospection commerciale.
- **Données collectées**
  - Seules les données nécessaires à la finalité poursuivie par le traitement peuvent être collectées.



## Durée de conservation

- Données commerciales: toute la durée du contrat.
- Données de consommation: pendant une durée limitée sous forme détaillée, puis agrégées pour le reste de la durée du contrat.
- Pour la prospection commerciale, les données collectées peuvent être conservées pendant 3 ans à compter de la fin de la relation commerciale.

## Destinataires

- Client et prestataire.
- Le prestataire peut transmettre les données à un sous-traitant ou partenaire commercial.

## Information et droits des personnes

- Obligation d'informer le client lors de la signature du contrat de prestation de service.
- Droit d'accès du client à la rectification ou suppression de ses données.
- Pour la prospection commerciale, le client doit être mis en mesure de s'opposer, sans frais, au traitement de ses données par le prestataire.
- Le prestataire doit prévoir des moyens permettant au client de contrecarrer les actions à distance sur les équipements de son logement.

## Sécurité

- Mise en place de mesures garantissant la confidentialité des données traitées en empêchant la prise de contrôle par toute personne non-autorisée.

## Démarche auprès de la CNIL

- Déclaration du prestataire auprès de la CNIL.

# L’avenir de ces recommandations

- **Diffuser largement le « pack de conformité énergie ».**

- **Les porter au plan européen** pour permettre aux acteurs de se positionner à un niveau européen, voire mondial.

- Les **mettre à jour** régulièrement

- De manière générale, **utiliser les packs de conformité comme des outils permettant d’atteindre un marché unique numérique pour l’Europe.**

(cf. Communication de la Commission européenne concernant “un marché unique numérique pour l’Europe” datée du 6 mai 2015).

Merci de votre attention

Des questions ?