5. Gestion des données et vie privée du citoyen urbain

- Architectures de gestion de données face au respect de la vie privée
- Gestion de la vie privée dans les réseaux sociaux mobiles
- Privacy-by-design: gestion de données confinée (puces et capteurs)
- **Gestion de la vie privée dans les applications mobiles participatives**
- Traitements de données globaux respectueux de la vie privée

Aujourd'hui, on va parler de la gestion de la vie privée dans les applications mobiles participatives.

Comme on l'a déjà vu dans la 3ème semaine de ce cours, il existe des applications participatives mobiles, des objets connectés, mais aussi des citoyens connectés avec les capteurs qu'ils portent et même avec leurs smartphones.

Les citoyens partagent des informations professionnelles et leur avis personnel pour améliorer la qualité de la vie communautaire.

Mais dans ces applications, il y a un très grand défi : comment protéger ses informations personnelles ?
Comme on l'a déjà vu, le respect de la vie privée et de l'anonymat est une exigence primordiale lorsque des informations personnelles sont manipulées.

Il y a plusieurs types d'atteintes potentielles à la vie privée dans les applications participatives mobiles.
Tout d'abord, des **applications malicieuses peuvent collecter plus de données que nécessaire** au fonctionnement. Cela peut inclure par exemple, votre liste de contacts, votre messagerie ou votre localisation.

Atteintes à la vie privée dans les applications participatives mobiles

- Les applications malicieuses peuvent collecter plus de données que nécessaire
- Les utilisateurs peuvent essayer d'accéder à une large quantité de données d'autrui

7

Les autres utilisateurs peuvent également essayer d'**accéder à une large quantité de données d'autrui**.

Atteintes à la vie privée dans les applications participatives mobiles

- Les applications malicieuses peuvent collecter plus de données que nécessaire
- Les utilisateurs peuvent essayer d'accéder à une large quantité de données d'autrui
- Les agents (gouvernement, opérateurs télécom) peuvent sauvegarder les données transmises dans les réseaux

8

Troisièmement, les agents, par exemple le gouvernement ou même les opérateurs telecom, peuvent **sauvegarder les données transmises dans les réseaux**.

Atteintes à la vie privée dans les applications participatives mobiles

- Les applications malicieuses peuvent collecter plus de données que nécessaire
- Les utilisateurs peuvent essayer d'accéder à une large quantité de données d'autrui
- Les agents (gouvernement, opérateurs télécom) peuvent sauvegarder les données transmises dans les réseaux
- Les « hackers » peuvent voler les données directement dans le serveur !

9

Enfin, les **hackers peuvent voler les données directement dans les serveurs**.

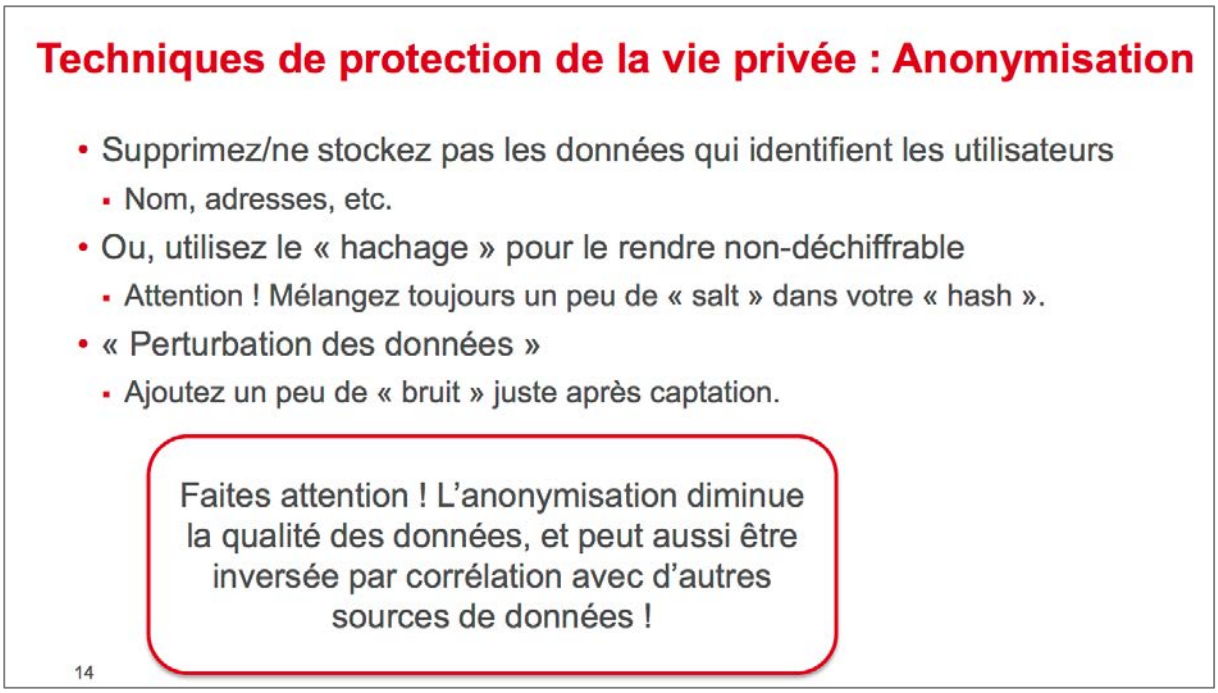
Face à ces atteintes, comment vous, soit en tant qu'utilisateur des applis participatives, soit en tant que développeur d'applis, pouvez-vous vous protéger ?

Pas d'inquiétude en France, nous sommes protégés par la loi (gérée par la CNIL) relative à la protection de la vie privée et à l'informatique.

En fait, que nous soyons développeur, ou utilisateur d'une appli, nous avons des obligations et des droits liés au respect de la vie privée.
Chaque développeur doit informer les utilisateurs sur le type de données qui sont collectées et aussi sur les objectifs de cette collecte de données.
Chaque personne qui utilise une appli peut connaître les données stockées et, s'il le souhaite, supprimer ou modifier les données.

Vous devez connaître vos droits et vos responsabilités.

Un premier groupe de techniques pour la protection de la vie privée est lié à l'anonymisation.
Tout d'abord, en tant que développeur d'applis mobiles, **supprimez ou plutôt ne stockez pas les données qui identifient les utilisateurs**. Cela peut être par exemple les noms et adresses, etc.
Si vous devez stocker ce type d'information, essayez d'utiliser le **hachage** pour les rendre non déchiffrables. Le hachage est une technique mathématique qui crypte les données d'une façon unidirectionnelle. Attention, il faut toujours mélanger votre "hash", avec un peu de "salt", c'est-à-dire du texte qui augmente la complexité mathématique du "hash".
Enfin, essayez de **perturber les données**, c'est-à-dire d'**ajouter un peu de bruit**, juste après la captation, et avant le stockage des données personnelles.



Mais, il faut tout de même faire attention : côté développeur d'application, l'anonymisation diminue la qualité des données. Elle peut aussi être inversée par corrélation avec d'autres sources de données.
Je vous conseille de vous renseigner davantage sur ce sujet.

Techniques de protection de la vie privée : Chiffrement

- Le chiffrement rend les données inutiles pour ceux qui n'ont pas la clé.

15

Une autre technique pour la protection de la vie privée est le chiffrement, qui **rend les données inutiles pour ceux qui n'ont pas la clé**.

Techniques de protection de la vie privée : Chiffrement

- Le chiffrement rend les données inutiles pour ceux qui n'ont pas la clé
- Il est important de chiffrer les données « au repos » afin d'éviter un désastre au cas où quelqu'un vole votre base de données

16

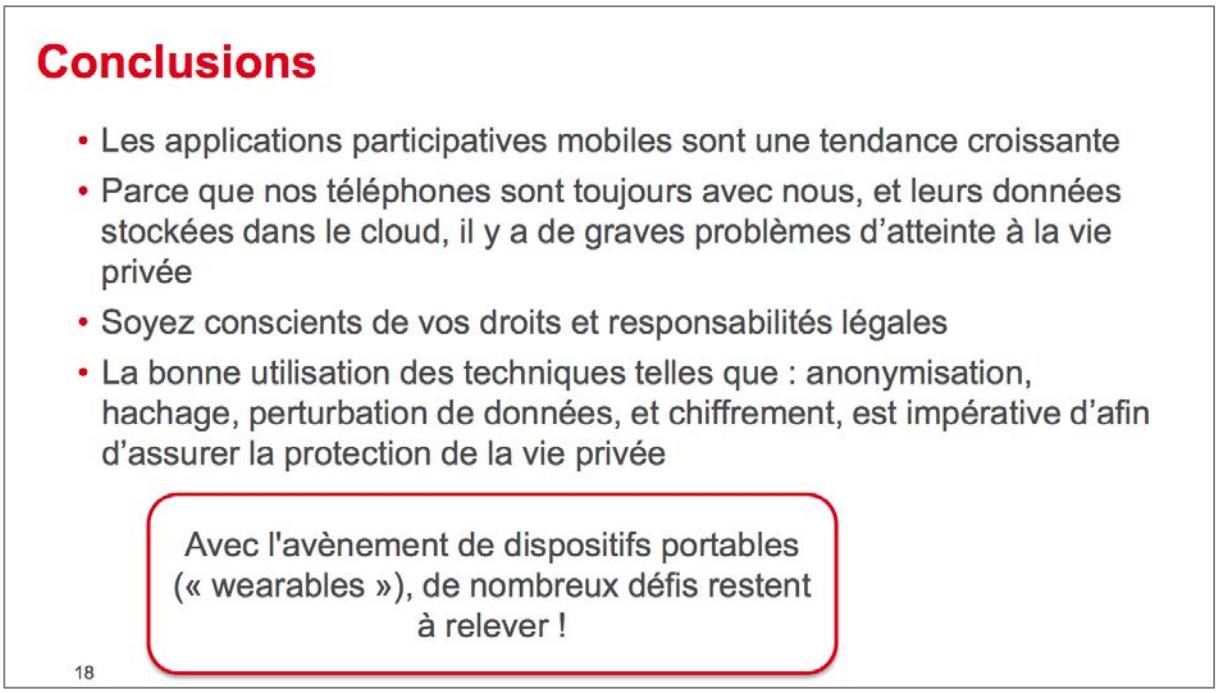
Tout d'abord, il est très important de **chiffrer les données "au repos"**, afin d'éviter un désastre, au cas où quelqu'un volerait votre base de données

Techniques de protection de la vie privée : Chiffrement

- Le chiffrement rend les données inutiles pour ceux qui n'ont pas la clé
- Il est important de chiffrer les données « au repos » afin d'éviter un désastre au cas où quelqu'un vole votre base de données
- Il est aussi important de chiffrer les donnés « en vol » afin d'éviter l'espionnage

17

. Il est aussi très important de **chiffrer les données « en vol »** afin d'éviter l'espionnage, par les gouvernements ou par les opérateurs Télécom.



Comme nous l'avons vu, les applications participatives mobiles sont une tendance croissante.
Mais, parce que nos téléphones sont toujours avec nous et que leurs données sont stockées dans le cloud, il y a de graves problèmes potentiels d'atteinte à la vie privée.
Il faut que nous soyons conscients de nos droits et responsabilités légales.
Il faut que nous utilisions bien les techniques, telles que l'anonymisation, le hachage, la perturbation des données et le chiffrement afin d'assurer la protection de la vie privée des utilisateurs.
Soyez prudents parce qu'avec l'avènement des dispositifs portables ou "wearables", de nombreux défis restent à relever.

Références

- CNIL: Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/
- CNIL: Vos Droits : http://www.cnil.fr/vos-droits/
- CNIL: Vos Obligations : http://www.cnil.fr/vos-obligations/vos-obligations/
- InfoSec Institute, "Crowdsensing: State of the Art and Privacy Aspects" : http://resources.infosecinstitute.com/crowdsensing-state-art-privacy-aspects/
- Krontiris, Ioannis, Marc Langheinrich, and Katie Shilton. "Trust and privacy in mobile experience sharing: future challenges and avenues for research." Communications Magazine, IEEE 52, no. 8 (2014): 50-55.

19

Illustrations & photos : crédits

p. 2-4 : © Consuelo Barreto,123RF
p. 3-4 : © Denys Prykhodov, Shutterstock
p. 5 : © Tiko Aramyanen, Fotolia
p. 6 : © Onidji, Fotolia
p. 7 : © Praneat, Fotolia
p. 8 : © Innovated Captures, Fotolia
p. 9 : © Antonio Gravante, Fotolia
p. 7 : © Praneat, Fotolia
p. 13 : © ptnphotof, Fotolia
p. 15-17 : © varandah, Fotolia