Analyse juridique et conformité RGPD

Stockage de données identifiantes dans le projet Wi-Fi Geolocation

Équipe Wifi-Géolocalisation.

Contexte du sujet

Dans le cadre du projet de géolocalisation Wi-Fi, nous devons déterminer si le stockage d'identifiants techniques comme les adresses MAC ou d'autres données issues des trames Wi-Fi est conforme à la législation en vigueur. Même dans un cadre éducatif ou de recherche, la capture et la conservation de telles données peuvent constituer un traitement de **données à caractère personnel** au sens du **Règlement Général sur la Protection des Données (RGPD)**.

Analyse juridique

Selon l'article 4(1) du RGPD, toute information permettant d'identifier directement ou indirectement une personne physique est considérée comme une donnée personnelle. Les adresses MAC, bien que techniques, peuvent être reliées à un individu à travers son appareil, et sont donc considérées comme des *identifiants indirects*.

La CNIL (Commission Nationale de l'Informatique et des Libertés) considère explicitement la collecte d'adresses MAC via des bornes Wi-Fi ou capteurs comme une activité soumise au RGPD, notamment lorsqu'elle permet de suivre le déplacement ou la présence de personnes dans un espace donné. De même, d'autres autorités européennes (AEPD, Autoriteit Persoonsgegevens) ont confirmé que le suivi via Wi-Fi ou Bluetooth requiert des garanties strictes de transparence, d'anonymisation et de finalité limitée.

Cas et références notables

- **CNIL – Guide de sécurité des données personnelles (2024)** : recommande la minimisation et l'anonymisation des identifiants techniques. `https://www.cnil.fr/sites/cnil/files/2024-03/cnil_guide_securite_personnelle_ven_0.pdf`
- **AEPD – Wi-Fi Tracking Technologies : Guidance for Data Controllers (Espagne)** : confirme que la collecte d'adresses MAC sans consentement constitue un traitement de données personnelles. `https://www.aepd.es/guides/wi-fi-tracking-technologies-guidance-for-data-controllers.pdf`
- **Autoriteit Persoonsgegevens (Pays-Bas)** – « Legal bases for Wi-Fi and Bluetooth tracking » : décrit les bases légales possibles (intérêt légitime, consentement explicite). `https://www.autoriteitpersoonsgegevens.nl/en/themes/internet-and-smart-wifi-and-bluetooth/legal-bases-for-wifi-tracking-and-bluetooth-tracking`
- **TechGDPR Blog (2023)** – Analyse des obligations RGPD liées au Wi-Fi tracking en milieu commercial. `https://techgdpr.com/blog/wifi-tracking-retail-analytics-`

— **Cas « Bluetooth bins » à Londres (2013)** – Exemple réel de sanction : des poubelles connectées collectaient les adresses MAC des passants sans leur consentement. Projet arrêté après intervention des autorités. `https://www.theguardian.com/technology/2013/aug/12/city-london-bins-stop-tracking-public`

Synthèse des constats

— Les adresses MAC sont considérées comme des données personnelles lorsqu'elles peuvent être reliées à un appareil identifiable.
— Le stockage brut d'adresses MAC sans consentement est contraire au RGPD.
— La pseudonymisation ou le hachage n'exonèrent pas automatiquement du RGPD si la donnée peut être ré-identifiée.
— En contexte éducatif, les mêmes principes s'appliquent, mais la CNIL peut tolérer la collecte temporaire à des fins d'apprentissage, sous réserve d'anonymisation stricte et d'absence de finalité commerciale.

Recommandations pour notre projet

1. **Ne pas conserver d'adresses MAC en clair.** Toute donnée identifiante doit être supprimée ou hachée (ex : SHA-256 avec salt).
2. **Limiter la durée de conservation.** Supprimer automatiquement les logs après analyse (par exemple, sous 24 h ou à la fin du test).
3. **Documenter la finalité.** Indiquer explicitement que la collecte est réalisée dans un but pédagogique et de recherche, non commercial.
4. **Informer les utilisateurs potentiels.** Ajouter une mention légale visible dans la documentation ou l'application web : « Prototype académique – Aucune donnée personnelle n'est conservée durablement. »
5. **Préférer l'anonymisation complète.** Remplacer les adresses MAC par un identifiant généré aléatoirement côté capteur avant transmission au serveur.

Conclusion

Le stockage d'identifiants techniques (adresses MAC, BSSID, etc.) n'est pas anodin juridiquement. Même dans un projet académique, ces données sont couvertes par le RGPD dès lors qu'elles peuvent servir à identifier un individu ou un appareil spécifique. La seule approche conforme consiste à appliquer les principes de minimisation, d'anonymisation, de durée limitée et de transparence. Notre projet devra donc restreindre la conservation des données à des fins purement expérimentales et anonymisées.