INFORME DE CONSULTORÍA EN PROTECCIÓN DE DATOS

Caso Práctico: ***Marketing Urbano y sus Dispositivos IoT***

> **Empresa:** "Marketing Urbano", una consultora que instala pequeños dispositivos (beacons) en tiendas y centros comerciales. Estos dispositivos usan Bluetooth para detectar la presencia de móviles cercanos (capturando su identificador MAC) y medir cuánto tiempo pasan los clientes en diferentes secciones de la tienda.

1. Análisis del Escenario y Riesgos

Descripción del tratamiento

La empresa ***Marketing Urbano*** instala dispositivos IoT (beacons) en centros comerciales. Estos detectan móviles cercanos a través de Bluetooth, capturan su dirección MAC y registran la duración de la estancia en cada zona.

Identificación de datos personales

- **Dirección MAC**: La dirección MAC es un identificador único vinculado a un dispositivo, pero en este contexto se considera un dato personal (art. 4.1 RGPD), ya que permite identificar indirectamente a una persona en el tiempo al vincularse con hábitos de visita o patrones únicos.
- No se tratan categorías especiales, pero sí datos que pueden afectar gravemente la privacidad (localización y comportamiento).

Principales riesgos para la privacidad

En general, el seguimiento constante puede invadir la privacidad, permitir la creación de perfiles, y exponer a ataques si la información no se gestiona adecuadamente. Existen riesgos de acceso no autorizado y vulnerabilidades inherentes al Bluetooh.

- **Rastreo invisible** de ciudadanos sin consentimiento ni información.
- **Perfilado de hábitos de consumo** que puede vincularse a identidades reales.
- **Reidentificación** a partir de la combinación con otros datos (apps, programas de fidelización).
- **Vulneración del derecho a la información y oposición**.

2. Medidas de Seguridad

Medidas técnicas

1. **Pseudonimización inmediata** de la dirección MAC antes de su almacenamiento. De esta forma se dificulta la identificación de los usuarios. Podríamos utilizar scripts personalizados con Python o Node js usando librerías de hash, bases de datos con funciones de enmascaramiento o tokenización integradas (ej. PostgreSQL) o herramientas de anonimización como ARX o Apache Atlas.

2. **Cifrado y control de acceso** a la base de datos de seguimiento. El cifrado de los datos tanto en tránsito como en almacenamiento para evitar los accesos no autorizados y un control estricto al sistema de tratamiento de datos, permitiendo sólo al personal autorizado a manipular la información recopilada.

   Herramientas en el cifrado de control:

   En tránsito: el uso de TLS/SSL en todas las comunicaciones o herramientas como Let' s encrypt u OpenSSL

   En reposo: el cifrado de bases de datos.

   Herramientas en al control de acceso y auditoría: como azure Active Directory, AWS, etc.

3. **Limitación temporal de conservación**: eliminación o anonimización en un plazo máximo (ej. 30 días). Mediante scripts programados para el borrado automático. Con Cron (Linux) o Task Scheduler (Windows).

Medidas organizativas

1. **Carteles visibles e informativos** en los establecimientos que usen beacons, explicando el uso de dispositivos de captación y los derechos de las personas (acceso, oposición, etc)

2. **Implementación de políticas internas y protocolos de seguridad**, incluyendo formación del personal.

3. **Procedimiento sencillo** para que los usuarios ejerzan su derecho de oposición a ser rastreados.

4. **Designación de un DPO o responsable de privacidad**, para garantizar cumplimiento continuo.

5. **Mecanismo para ejercer derechos ARSULIPO**, en especial el derecho de oposición al rastreo. Con software de gestión de privacidad como Data Grail, TrustArc o PrivacyEngine o formularios con Google Forms.

3. Evaluación Legal y Sanciones

¿Se requiere una Evaluación de Impacto (EIPD)?

Sí; al existir un tratamiento sistemático de datos de localización capaces de identificar a personas y al conllevar riesgos elevados para los derechos y libertades, la EIPD es obligatorio según el RGPD (art. 35 RGPD).

Base jurídica del tratamiento

Puede emplearse el interés legítimo de la empresa para análisis de afluencia y mejora de los servicios, pero esto exige informar debidamente a los afectados y facilitar el ejercicio del derecho de oposición.

- **Consentimiento explícito** → opción más segura (ej. app del cliente con activación de Bluetooth voluntaria).
- **Interés legítimo** → posible, pero arriesgado: requiere un test de ponderación y fuertes garantías.

Sanción por no informar

Recoger datos sin informar constituye una infracción grave o muy grave bajo la LOPDGDD, con sanciones que pueden alcanzar hasta 20 millones de euros o el 4% del volumen de negocio anual, además de otras medidas accesoria (art. 83 RGPD).

Posibles infracciones según la tabla del PDF

Si *Marketing Urbano* recopila estos datos sin informar ni obtener base jurídica válida:

- **Leves**
  - Incumplimiento del principio de transparencia (no informar).
  - No atender el derecho de oposición de los afectados.
- **Graves**
  - Falta de medidas técnicas adecuadas (ej. no cifrar, no seudonimizar).
  - No disponer de un registro de actividades.
  - Encargar tratamiento a terceros (proveedores) sin contrato.
- **Muy graves**
  - Incumplir requisitos sobre el consentimiento válido.
  - Omitir el deber de informar al afectado.

- Usar los datos para fines incompatibles con los declarados (perfilado oculto).

4. Conclusión

El caso de *Marketing Urbano* muestra cómo una tecnología innovadora, la captación y tratamiento de direcciones MAC representa un alto riesgo para la privacidad, por lo que es imprescindible adoptar medidas técnicas y organizativas adecuadas, informar transparentemente a los afectados y cumplir rigurosamente con la legalidad. No hacerlo puede exponer a la empresa a sanciones económicas significativas y a pérdida de reputación.

- **Garantizar información clara y visible** al público y mecanismos para ejercer derechos.
- **Adoptar como base jurídica el consentimiento**, en vez de depender solo del interés legítimo.
- **Realizar una EIPD documentada** antes de desplegar el sistema.

Estas medidas no solo reducen la exposición a infracciones graves o muy graves, sino que fortalecen la confianza del cliente y la reputación de la empresa en el mercado digital.