Lo que tu empresa debe considerar al integrar reconocimiento facial en México

Guía de implementación responsable para cadenas comerciales en México

Atención compliance: Los rostros *sí* son datos personales bajo la LFPDPPP, incluso sin nombre asociado. Los datos biométricos se clasifican como **DATOS SENSIBLES** y requieren el nivel de protección más alto que contempla la ley.

OBLIGACIONES LEGALES — LFPDPPP (MÉXICO)

Aviso de privacidad visible
Colocar avisos en sucursales informando sobre reconocimiento facial y su finalidad específica (prevención de robo).

Finalidad específica
Uso exclusivo para prevención de robo. Prohibido reutilizar para marketing, análisis de comportamiento u otros fines.

Acceso restringido
Solo personal autorizado de seguridad, compliance y legal puede consultar la base de datos de vectores.

Retención definida
Plazo máximo de conservación documentado y eliminación automática de vectores al vencerlo.

Seguridad técnica
Cifrado en reposo y tránsito, autenticación multifactor, logs de auditoría por cada consulta realizada.

No compartir sin base legal
Protocolo claro para compartir con autoridades. Prohibido vender o ceder la información biométrica.

CÓMO FUNCIONA FACEME® — PROTECCIÓN TÉCNICA POR DISEÑO

f Embeddings matemáticos, no fotos
FaceMe no almacena fotografías de los rostros. Genera una representación matemática (vector numérico) de cada cara. Incluso si la base de datos fuera comprometida, sería imposible reconstruir el rostro original. Esto reduce significativamente el riesgo de exposición ante un incidente de seguridad.

PASOS RECOMENDADOS PARA IMPLEMENTAR CORRECTAMENTE

1. **Involucrar al área legal antes del despliegue**
   Un abogado especialista en privacidad de datos debe revisar y formalizar el aviso de privacidad y las políticas internas antes de que el sistema entre en operación.
2. **Redactar y publicar el aviso de privacidad**
   Colocar señalética en cada sucursal indicando que opera reconocimiento facial, su propósito específico y los datos de contacto del responsable del tratamiento.
3. **Definir política de retención y eliminación**
   Establecer por escrito el plazo máximo de conservación de vectores y el proceso de eliminación automática al vencerlo.
4. **Implementar controles técnicos de seguridad**
   Cifrado en reposo y tránsito, MFA, logs de auditoría de cada consulta y separación de la base de datos respecto a otros sistemas.
5. **Definir el protocolo de uso y acceso interno**
   Especificar qué perfiles pueden consultar el sistema, bajo qué circunstancias y con qué autorización. Documentar cada acceso.
6. **Revisar periódicamente y ante cambios de ley**
   Revisar el esquema de cumplimiento al menos una vez al año o cuando haya reformas a la LFPDPPP u otras leyes aplicables.

LO QUE EL SISTEMA PUEDE HACER CORRECTAMENTE

- ✓ Identificar personas previamente registradas como riesgo
- ✓ Alertar en tiempo real al personal de seguridad
- ✓ Almacenar vectores matemáticos (no fotografías)
- ✓ Operar sin recopilar nombre u otros datos personales adicionales

LO QUE NO DEBE HACERSE

- ✗ Usar los datos para fines distintos a seguridad
- ✗ Compartir o vender información a terceros sin base legal
- ✗ Operar sin aviso de privacidad visible en sucursales
- ✗ Conservar datos indefinidamente sin política de eliminación