



LA SEGURIDAD Y PRIVACIDAD EN EL MARCO DE LAS TELECOMUNICACIONES

**Seminario Iberoamericano de Protección de
Datos: nuevas tecnologías, seguridad y
privacidad**



**Alejandro Del Conde Ugarte
Secretario Ejecutivo IFAI**

**Cartagena de Indias, Colombia
Julio 2010**



Antecedentes

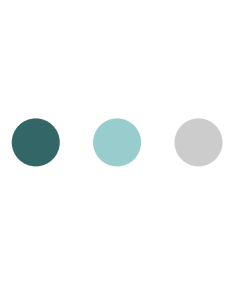
- Las Tecnologías de Información y **Comunicaciones** (TICs) son parte integrante de nuestras vidas.
 - Amplían posibilidades de almacenar, procesar y **transmitir** información
 - Aspecto estratégico en el desarrollo de cualquier país moderno
 - Aumentan los riesgos de ser afectado en nuestra intimidad y por el tratamiento de nuestros datos
- Reto de los sistemas jurídicos y de las autoridades: Conciliar las ventajas que ofrecen las TICs con la protección de los datos personales y la intimidad de los individuos.



Protección de datos personales en el sector de telecomunicaciones

Debate:

- La normativa de protección de datos personales aplica cuando se trata de información sobre una persona identificada o identificable,
- En el caso de las telecomunicaciones, diversa información que es tratada no permite la identificación, de forma razonable, de los titulares de la información.
- Sin embargo: la identificación de los titulares de los datos es posible cuando se combina la información de diversos agentes.
- Otros elementos que obligan a la protección de los datos en el sector:
 - ✓ Tratamiento masivo de la información a costos reducidos;
 - ✓ Oferta de información a un público masivo;
 - ✓ Diversidad de prestadores y usuarios, y
 - ✓ Posibilidad de la elaboración de perfiles de usuarios.



Medidas de seguridad en el tratamiento de datos personales

La seguridad de la información descansa en tres pilares básicos:

- 1. Confidencialidad:** accesible sólo para aquéllos que están autorizados.
- 2. Integridad:** exacta, correcta y completa.
- 3. Disponibilidad:** se puede utilizar cuando se necesite.



Regulación en telecomunicaciones

- Constitución (artículos 16 y 73, fracción XXIX-O)
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que regula datos personales de manera genérica:

“Artículo 40.- La presente Ley constituirá el marco normativo que las dependencias deberán observar, en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda, con la coadyuvancia del Instituto.”

- Ley Federal de Telecomunicaciones, que regula el tratamiento de datos personales de manera sectorial.



Principios y derechos de protección de datos personales

La legislación mexicana reconoce los siguientes principios y derechos :

Principios	Derechos
Licitud	Acceso
Consentimiento	Rectificación
Información	Cancelación
Calidad	Oposición
Finalidad	
Lealtad	
Proporcionalidad	
Responsabilidad	

Así como los deberes de **seguridad de la información y confidencialidad**.



El caso del Registro Nacional de Usuarios de Telefonía Móvil

Objetivo:

Identificar a los usuarios de líneas de servicio local móvil o de servicio móvil de radiocomunicación especializada de flotillas, y registrar las altas y bajas de sus líneas.

Este registro inscribe los siguientes datos:

- ✓ Número y modalidad de la línea telefónica;
- ✓ Nombre completo del usuario;
- ✓ Domicilio, con su respectivo comprobante;
- ✓ Nacionalidad;
- ✓ Datos contenidos en la identificación oficial vigente con fotografía, y/o CURP y/o pasaporte, y
- ✓ **Huella dactilar, en tinta o electrónica.**



La experiencia internacional

- **Chile:** Registro de teléfonos móviles reportados como robados.
- **Bolivia:** *Registro de Propiedad de Equipos Terminales Móviles*
- **Reino Unido:** el *National Mobile Property Register* es una base de datos de la policía nacional que inscribe los datos de las propiedades de las personas. Es un registro voluntario.
- **España:** registro en el que consta la identidad de los clientes de servicios de comunicaciones.

No se encontró evidencia de que algún caso internacional incluyera datos biométricos, como es el caso del mexicano.



El caso del Registro Nacional de Usuarios de Telefonía Móvil

Origen

- ***Acuerdo Nacional por la Seguridad, la Justicia y la Legalidad***, publicado por el Gobierno Federal el 25 de agosto de 2008, el cual tuvo por objeto establecer políticas específicas en materia de seguridad, justicia y legalidad.
- **Reformas a la Ley Federal de Telecomunicaciones** del 9 de febrero de 2009, que establece la obligación de los concesionarios de redes públicas de telecomunicaciones de llevar un **registro de usuarios de telefonía móvil y otro de comunicaciones**.



El caso del Registro Nacional de Usuarios de Telefonía Móvil

Regulación

- La autoridad competente para regular el Registro es la **Secretaría de Comunicaciones y Transportes**, a través de la **Comisión Federal de Telecomunicaciones**.
- **Reglas del Registro Nacional de Usuarios de Telefonía Móvil** del 15 de mayo de 2009, las cuales establecen los detalles operativos del registro.
- **Anteproyecto de Reglamento de la Ley Federal de Telecomunicaciones en Materia de Registro de Usuarios de Telefonía Móvil**, sometido a consulta pública el 29 de abril de 2010.



El caso del Registro Nacional de Usuarios de Telefonía Móvil

Características

- **Propósito fundamental:** propiciar cooperación entre las autoridades competentes en materia de prevención, investigación, detección y persecución de delitos cometidos por medio de telefonía móvil.
- Tres autoridades: SCT, SEGOB y PGR.
- Sujeto obligado: Concesionarios de redes públicas de telecomunicaciones.
- Dos registros:
 - Registro de usuarios de telefonía móvil
 - Registro de comunicaciones



Registro de Comunicaciones

Objetivo: Conservar datos de tráfico y localización de las llamadas telefónicas,

Este registro inscribe los siguientes datos:

1. Tipo de comunicación, servicios suplementarios, de mensajería o multimedia empleados;
2. Datos necesarios para rastrear origen y destino de las comunicaciones;
3. Datos necesarios para determinar fecha, hora y duración de la comunicación;
4. Fecha y hora de la primera activación del servicio, y etiqueta de localización desde la que se haya activado el servicio, y
5. Ubicación digital del posicionamiento geográfico de las líneas telefónicas.



El caso del Registro Nacional de Usuarios de Telefonía Móvil

En cuanto al registro de los datos...

- La **Ley Federal de Telecomunicaciones** estableció como obligación de los proveedores llevar el registro de la totalidad de los datos.
- Las **Reglas del Registro** modificaron lo anterior al señalar:
 - Los proveedores tendrían la obligación de conservar sólo los datos de modalidad de la línea telefónica,
 - La Secretaría de Gobernación sería la responsable de registrar y conservar el resto de los datos
- El **anteproyecto de reglamento** señala que
 - Los proveedores realizarán el registro.
 - También son responsables de mantener la información relativa a la modalidad de las líneas.
 - El proyecto de reglamento no hace mención alguna de la autoridad que será responsable de recabar y resguardar el resto de los datos personales.



Datos conservados actualmente por los proveedores

Operación: Los proveedores conservan de manera directa los siguientes datos:

1. Número telefónico del usuario que origina la llamada, mensaje o comunicación de datos;
2. Número telefónico del usuario hacia el cual se dirige la llamada o mensaje;
3. Fecha de llamada, de envío de mensaje o de inicio de sesión de datos;
4. Hora de inicio de la llamada, del envío del mensaje o de la sesión de datos;
5. Duración de la llamada u hora de terminación de la sesión de datos, y
6. Ubicación digital de posicionamiento geográfico.

○ Los proveedores deben conservar los datos de tráfico y localización por un plazo de doce meses, contados a partir de la fecha en que se realizó la comunicación.



Medidas de seguridad

- El anteproyecto de reglamento obliga a los proveedores de servicios a la implementación de una serie de medidas de seguridad aplicables para garantizar la confidencialidad, integridad y disponibilidad de los datos personales e información objeto de ambos registros, en materia de:
 - ✓ Resguardo de soportes físicos o electrónicos;
 - ✓ Control de acceso;
 - ✓ Funciones y obligaciones del personal autorizado;
 - ✓ Identificación y autenticación del personal autorizado;
 - ✓ Procedimientos de copias de respaldo y de recuperación de datos;
 - ✓ Continuidad en las operaciones, y
 - ✓ Auditoría y rastreabilidad de operaciones.



Observaciones del IFAI en materia de protección de datos personales

- La estructura general del Registro atiende los parámetros internacionales
- El IFAI ha detectado deficiencias y omisiones en temas torales, que podrían poner en riesgo la protección de los datos personales.
 - Principales observaciones:
 - ✓ La ausencia de disposiciones que establezcan con precisión las medidas de seguridad que deberán adoptar los sujetos involucrados para la transmisión de datos.
 - ✓ La falta de claridad en las obligaciones de cada actor respecto de los datos personales a recabar, conservar y transmitir.



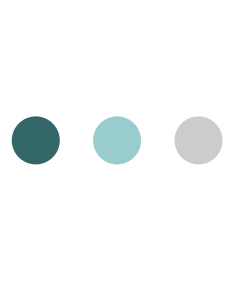
Observaciones del IFAI...

Respecto del **Registro de Usuarios o RENAUT:**

- La falta de definición del responsable del RENAUT, es decir ¿quién estará a cargo de su administración?
 - SCT, a través de la Cofetel, de conformidad con la LFT.
 - Secretaría de Gobernación, de conformidad con las Reglas de Operación del Registro.

En cuanto al **Registro de Comunicaciones:**

- Clarificar que los datos recabados **son específicamente de tráfico y localización** y no el contenido de las comunicaciones.



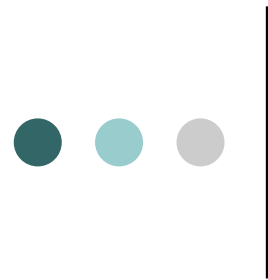
Observancia de los principios de protección de datos

- ✓ **Licitud:** el Registro es lícito.
- ✓ **Información:** se recomienda que incluya el aviso de privacidad.
- ✓ **Calidad:** la normatividad que regula el Registro no establecen con precisión mecanismos para llevar a cabo la corrección de los datos personales ante petición de su titular.



Observancia de los principios de protección de datos

- ✓ **Finalidad:** El Registro cumple de forma general con este principio.
- ✓ **Proporcionalidad:** No es posible evaluar el cumplimiento de este principio. Pero cabe señalar que no se tiene conocimiento de otro país que utilice huellas digitales en este tipo de registros.
- ✓ **Responsabilidad:** La normatividad sólo establece responsabilidades claras respecto de las medidas de seguridad, pero no con relación a otros aspectos.



Conclusiones:

1. Establecer con claridad la autoridad que estará a cargo del RENAUT, no sólo de su regulación;
2. Establecer medidas de seguridad adecuadas para la transmisión de datos, y
3. Señalar con precisión qué datos deberá recabar y conservar cada actor.