CAPÍTULO III

CASOS PARTICULARES

Los datos personales registrados en las bases de datos son altamente valiosos, se trata de aspectos que definen a la persona: nombre, domicilio, nacionalidad, educación, historial clínico, familia, historial crediticio, ideología, afiliación política, edad, antecedentes penales, religión, origen racial, preferencias sexuales, estado civil, etc. Si toda esta información circula sin ninguna restricción, con incumplimiento a las normas, leyes o tratados existentes, el cruce de información de las bases de datos puede crear perfiles completos que ponen en peligro la seguridad de las personas: podrían ser víctimas de secuestro, fraude, recibir ofertas de inversión que no solicitaron, ser víctimas de discriminación o chantaje, se les pueden negar ciertos servicios por su historial crediticio, recibir propaganda o publicidad no solicitada de acuerdo con sus hábitos de consumo, etc.

Es innegable que la información es una herramienta básica y necesaria para el desarrollo de toda actividad, tanto del sector público como privado, sin distinción alguna. En este capítulo se presenta un breve análisis del uso de la información que realizan diferentes sectores en nuestro país, con puntos de oportunidad y debilidades que hasta el momento ofrece la legislación y políticas públicas para su protección.

3.1 Sociedades de Información Crediticia

Las Sociedades de Información Crediticia (SIC), mejor conocidas como Burós de Crédito, son los referentes principales de los oferentes de crédito; se traducen en información de los usuarios que es necesaria para fomentar prácticas crediticias sanas que reduzcan el costo del crédito solicitado (Banco de México, 2009).

El objetivo principal para regular a las Sociedades de Información Crediticia es proteger los derechos de los deudores respecto a su historial de crédito. Existe un sinnúmero de bases de datos que contienen información de personas que en alguna ocasión han solicitado y recibido una tarjeta de crédito comercial o bancaria, algún préstamo o servicio. Dichos historiales

registran las operaciones realizadas por las personas, si realizan sus pagos correspondientes, etc. (Banco de México, 2009).

Las Sociedades de Información Crediticia o Burós de Crédito estandarizan esta información y la venden a los acreedores o empresas comerciales como un reporte de crédito. Dichos reportes sirven como referencia a las entidades financieras para determinar si las personas son sujetos de crédito o no y que les aprueben o rechacen sus solicitudes (Banco de México, 2009).

En México, el registro privado que constituye la fuente de información crediticia más importante es Buró de Crédito, se trata de una alianza entre Experian e inversionistas mexicanos interesados en recolectar y distribuir información crediticia de consumidores individuales, que cuenta con dos agencias que le proporcionan la información: Trans Union de México y Dun & Bradstreet. La misión declarada de este Buró de Crédito "*es apoyar al desarrollo de la economía mexicana al proveerle a las compañías la información que les permitirá extender el crédito a sus clientes sin comprometer la salud de sus organizaciones* (Credit & Loan Reporting, 2005)".

Para 2004, el Buró de crédito recibía información de mil 21 proveedores de datos. Para que las compañías reciban reportes de crédito, éstas deben aportar datos mensualmente, si no lo hacen durante dos meses consecutivos, el Buró deja de proporcionarles la información (Credit & Loan Reporting, 2005).

Los proveedores de datos son la mayoría de las Sofoles y compañías de arrendamiento no bancarias, compañías de telecomunicaciones a excepción de Telmex, ciertas empresas de micro financiamiento (uniones de crédito, cajas de ahorro popular, etc.) y diferentes comercios de menudeo, empresas comerciales y tiendas departamentales, de las que no está establecido un monto mínimo que deban reportar (entre éstas se encuentran Liverpool, Coppel, Salinas y Rocha, Palacio de Hierro, Sears, Elektra, Soriana, Suburbia) (Credit & Loan Reporting, 2005).

En 2005 la base de datos que le proporciona TransUnion provenía de 656 compañías no financieras y 141 compañías financieras, pertenecía a más de 29 millones de individuos que representaban 56 millones de relaciones crediticias, de éstas, alrededor de 30 millones estaban activas y eran actualizadas cada mes, guardan los datos durante 84 meses y hasta entonces los

borran. Por otro lado, la base de datos proporcionada por Dun & Bradstreet se alimentaba de 543 compañías no financieras y 148 compañías financieras, la base de datos era compuesta por 3.3 millones de cuentas, de las cuales 1.1 millones estaban activas y eran actualizadas mensualmente, pero a diferencia de la información proporcionada por TransUnion, lo datos los mantienen indefinidamente (Credit & Loan Reporting, 2005).

En 2007, Buró de Crédito anunció que el número de registros de créditos en su base de datos de personas físicas rebasó los cien millones, mismos que pertenecen a cerca de 42.3 millones de expedientes o personas físicas integradas. Los principales usuarios del Buró de Crédito son los bancos que registran el 56 por ciento del total de las solicitudes de reportes de clientes individuales y del 75 por ciento del total de las solicitudes de reportes de individuos con actividad empresarial o de empresas (Credit & Loan Reporting, 2005).

Además de los bancos, otros usuarios son instituciones financieras, Sofoles, agencias de bienes raíces, compañías de financiamiento automotriz, compañías de tarjetas de crédito, compañías de telecomunicaciones, arrendadoras, tiendas departamentales y otras empresas comerciales. De acuerdo con el Buró de Crédito, al año recibe 17 millones de solicitudes de reportes de crédito, y aproximadamente una tercera parte proviene de compañías no financieras (Credit & Loan Reporting, 2005).

Los reportes de crédito que dan a los Usuarios incluyen (Credit & Loan Reporting, 2005):

1. Datos generales del individuo o de la empresa.
2. Detalles con respecto al crédito adquirido por el individuo o negocio –que incluye el nivel total de endeudamiento-, sin señalar a los acreedores.
3. Historial de pagos, tanto positivo como negativo, incluye pagos atrasados, incumplimiento de pagos u otras irregularidades, y una calificación numérica del 1 al 9 que señala el grado de puntualidad del pago que realiza el individuo o la empresa.

Además de los reportes de crédito, el Buró también comercializa un producto de calificación crediticia y varios productos diseñados para detectar fraude, robo de identidad, delincuencia, clonación de tarjetas de crédito, etc. (Credit & Loan Reporting, 2005).

En enero de 2002 se promulgó la Ley para regular las Sociedades de Información Crediticia para reglamentar las actividades de los burós de crédito privados que hasta ese momento operaban apegados al reglamento general emitido en 1995. De acuerdo con su artículo 5º: "la recopilación, manejo y entrega o envío de información relativa al historial crediticio de las personas físicas y morales, así como de operaciones crediticias y otras de naturaleza análoga que éstas mantengan con Entidades Financieras, Empresas Comerciales o las Sofomes E. N. R., sólo podrá llevarse a cabo por Sociedades que obtengan autorización a que se refiere el artículo 6º. De la presente ley". Este último artículo mencionado declara que para operar como Sociedad de Información Crediticia es necesaria la autorización de la Secretaría de Hacienda y Crédito Público y deben estar sujetos a las normas establecidas por el Banco de México.

La ley manifiesta que la información contenida en cada base de datos de las SIC debe ser correcta, actualizada y únicamente puede ser usada por terceros siempre y cuando la persona dé su autorización. Toda la información que las personas dan a las entidades financieras como bancos, sofoles, etc., y a empresas comerciales como tiendas departamentales, telefonía móvil, empresas de financiamiento de autos, es recopilada por las SIC. En materia de privacidad, a fin de garantizar la seguridad la información de millones de usuarios, la Ley para regular las SIC establece que:

- Las sociedades tienen prohibido pedir y proporcionar información que no sea autorizada por esta ley (Art. 18, fracción I).

- El artículo 22 establece que la Sociedad debe adoptar las medidas de seguridad necesarias para evitar que se haga mal uso de la información, y se refiere a cualquier acto u omisión que dañe el patrimonio, a la persona de quien se posea la información, así como cualquier acción que beneficie a funcionarios o empleados de la sociedad.

- De acuerdo con el artículo 28, las Sociedades sólo podrán dar información a un usuario cuando tenga la autorización directa del Cliente, mediante su firma en donde conste que tiene total conocimiento de la naturaleza y alcance de la información que la Sociedad proporcionará al Usuario que la solicita, del uso que el Usuario hará de la información y de la facultad que tiene para consultar periódicamente su historial crediticio, mientras mantenga una relación con el Cliente.

- El artículo 33 habla sobre la obligación de la Sociedad de contar con sistemas y procesos para verificar la identidad del Usuario a fin de proteger la confidencialidad de la información en los términos de las disposiciones legales.

- Cuando un Cliente pide un servicio a un Usuario, el Cliente tiene derecho a conocer los datos que le otorgó la Sociedad para poder aclarar cualquier situación con respecto a la información que contenga el Reporte de Crédito (Art. 39).

- Los Clientes pueden solicitar a la Sociedad su Reporte de Crédito Especial, mediante unidades especializadas de la Sociedad, Entidades Financieras o a quien esté designado en Empresas Comerciales, de tal forma que le permita conocer de forma clara y exacta en qué condición (Art. 40).

- Los clientes tienen la facultad de reclamar cuando no estén conformes con la información contenida en su Reporte de Crédito (Art. 42).

Para 2007, en cumplimiento de esta Ley, el Buró de Crédito reporta haber eliminado más de 14.8 millones de registros en la base de datos de personas físicas que ya habían cumplido la antigüedad de 84 meses en la base de datos (e-consulta, 2007).

Las bases de datos son totalmente indispensables para el desarrollo de la actividad financiera y hasta 2002 no gozaban de muchas garantías. La Ley para regular las Sociedades de Información Crediticia es un ejemplo clave de la necesidad que había de proteger la información que las personas depositan en las diferentes instituciones o empresas, fue creada para fortalecer la credibilidad de los burós, establecer mecanismos que protegieran los derechos de los sujetos de los datos, tales como los requerimientos de consentimiento, y garantizar el acceso a los reportes de crédito y procedimientos para corregir información equivocada. Sin embargo, las Sociedades de Información Crediticia son la excepción explícita de la nueva Ley de Protección de Datos Personales en Propiedad de Particulares y no gozan de las mismas garantías legislativas, comenzando por los derechos de ARCO y los principios contenidos en la Ley de Particulares.

Para Ernesto Villanueva (2010), el hecho de no legislar específicamente en el sector de las Sociedades de Información Crediticia denota una negociación que privilegia una cuestión

política sobre una cuestión que debería ser estrictamente técnica, Esto es porque, si bien es cierto que ya tenían una legislación previa, la Ley de Particulares es más positiva y tiene mayores elementos garantistas por lo que, en todo caso, se debió haber reformado la Ley de Sociedades Información Crediticia para tenerla como una norma supletoria y no excluir a este sector del espíritu normativo de la nueva ley porque éste y los principios básicos de la legislación deben ser iguales para todos, puesto que no es posible distinguir y tener mayor protección en unos casos y menor protección en otros, por lo menos no se explica desde un punto de vista técnico.

Villanueva (2010) explica que, en el caso de México, esta diferencia obedece a razones políticas porque cuando la ley se elaboró ya había sectores establecidos, como el sector bancario o el sector comercial, que generaron tensión: "Cuando el comité de diseño está en la labor técnica ocurre que, al momento de la negociación en el Congreso, aparecen presiones de carácter político que provocan una legislación de aproximación sucesiva, lo cual es lamentable porque lo deseable es la existencia de una sola ley".

En este caso se hablaría de integrar en una a la Ley de Sociedades de Información Crediticia, la Ley de Protección de Datos en Posesión de Particulares y la Ley Pública. En cambio son tres leyes que regulan un mismo objeto y genera mayor burocracia, complicación y dificultad para el gobernado por tratar un mismo objeto y bien jurídico, que es precisamente la vida privada expresada mediante la protección de datos personales inherentes a las personas físicas y personas morales (Villanueva, 2010).

3.1.1 Políticas, contratos y convenios

Independientemente de lo establecido por la Ley para regular las Sociedades de Información Crediticia y otras reglamentaciones, las instituciones bancarias establecen cláusulas en sus contratos crediticios en las que marcan sus lineamientos con respecto al uso que otorgará a la información personal de sus clientes, ante los cuales los usuarios no han tenido más que declarar conformidad sin tener el recurso de oposición.

Los contratos bancarios, por ejemplo, incluyen cláusulas sobre el uso de la información que no proporcionan seguridad alguna para los usuarios y claramente establecen que la información

puede ser utilizada para diferentes fines, sin aclarar cuáles serán éstos, tal es el caso, por ejemplo, de Banamex:

- Banamex. Autorización para el uso de la información: "Autorizo a Tarjetas Banamex, S. A. de C. V., Sofom, E. R. y a Banco Nacional de México, S. A., a utilizar para cualquier fin, incluyendo la comercialización de otros productos o servicios, la información contenida en esta solicitud o en otros documentos que se deriven de la misma o de cualquier relación que mantenga con Tarjetas Banamex, S. A. de C. V., Sofom, E. R. o con Banco Nacional de México, S. A. así como a proporcionar dicha información y documentación, para tales efectos, a los integrantes de Grupo Financiero Banamex, sus afiliadas, controladoras, subsidiarias, asociadas, comisionistas o a cualquier empresa controlada directamente o indirectamente por Citigroup".

Dentro del sector privado, cabe citar como otra muestra un contrato de apertura de crédito Liverpool, identificado como DILISA, en cuya cláusula sobre la información establece que, en conformidad con el artículo 28 de la Ley para Regular las Sociedades de Información Crediticia, puede investigar sobre el historial crediticio del solicitante, con cualquier sociedad de información crediticia autorizada, cuantas veces sea necesario. Asimismo, el cliente, obligado solidario y los tarjetahabientes adicionales autorizan a DILISA a proporcionar y/o solicitar a las diferentes entidades financieras del país, los datos y documentos referentes a su identificación, así como información relacionada con su situación patrimonial y operaciones de crédito, dar información en relación con sus datos o respecto de sus operaciones relacionadas con la empresa, a otras con las que tiene relaciones de negocios, y que por sí misma o a través de cualquier tercero puede usar sus datos para contactarlo, por cualquier medio, con fines informativos, de cobranza o de publicidad. Finalmente, el contrato libera de cualquier responsabilidad a Liverpool por esta causa.

De manera similar, el Contrato de Financiamiento de El Palacio de Hierro, en su capítulo sobre Autorizaciones adicionales de "El Cliente", además de tener la atribución de evaluar el historial crediticio del cliente así como de investigar en su domicilio, declara que autoriza a El Palacio a proporcionar la información necesaria sobre sí, relacionada con su cuenta y sobre todas las operaciones de cualquier naturaleza que realice con El Palacio, a empresas operadoras o procesadoras de tarjetas de crédito, así como a los terceros que intervengan en el

otorgamiento y manejo de la tarjeta que El Palacio contrate para manejar la operatividad, con la frecuencia que sea necesaria. Otras dos cláusulas solicitan autorización del cliente para utilizar datos con fines publicitarios de El Palacio y para proporcionar sus datos a terceros con fines publicitarios. Es necesario mencionar que estas tres últimas cláusulas solicitan de manera adicional la autorización del cliente.

Será de esperarse que con la nueva legislación los titulares de los datos puedan hacer uso de sus derechos en la protección de los datos personales para garantizar que sus datos podrán ser usados únicamente para los fines para los que otorguen su consentimiento.

3.2 Instituto Federal Electoral

A partir de 1977 México inició una serie de reformas político-electorales que sirvieron como fundamento de la institucionalidad vigente. Entre estas reformas, una de las más solicitadas por los partidos de oposición al entonces partido hegemónico fue la conformación de un padrón electoral confiable, necesario para un procedimiento electoral democrático. La creación de este instrumento originó cierta tensión entre el derecho a la protección a la privacidad en su vertiente de protección de datos personales y la protección de los derechos políticos de los ciudadanos (Gómez y Ornelas, 2006).

El proceso de creación constó de varias etapas, involucró a ciudadanos, al Instituto Federal Electoral y a los partidos políticos. Los ciudadanos tuvieron que entregar su información personal necesaria para conformar el padrón electoral, que contiene todos los ciudadanos mexicanos que solicitaron su inscripción a fin de obtener su credencial para votar con fotografía para ejercer su derecho al voto (IFE, 2009), que incluyó: nombre completo, lugar y fecha de nacimiento, edad sexo, domicilio y tiempo de residencia, ocupación, firma, huella digital y su fotografía (Gómez y Ornelas, 2006).

A fin de que el padrón fuera lo más confiable posible y se eliminaran las inconsistencias, se involucraron los partidos políticos y los ciudadanos; esto supuso que los datos personales contenidos en las bases de datos se divulgaran para que tanto los institutos políticos como los votantes pudieran corroborar su veracidad (Gómez y Ornelas, 2006).

Para esto, las listas nominales con fotografía –relación que contiene a los ciudadanos que solicitaron su inscripción al Padrón y cuentan con su credencial para votar con fotografía vigente (IFE, 2009)-, son entregadas y el padrón electoral se pone a disposición de los partidos políticos para su consulta, revisión y, dependiendo del caso, elaboración de las observaciones que sean convenientes. Los artículos 145 y 156 del Código Federal Electoral establecen que la información que contiene es absolutamente confidencial, de uso exclusivo y no podrán destinarla a otros fines distintos al de revisión (Gómez y Ornelas, 2006).

Las listas nominales con fotografía, además de tener los datos de los ciudadanos, cuentan con su fotografía impresa, idéntica a la de su credencial para votar vigente, misma que es almacenada en una base de imágenes, a fin de garantizar mayor confiabilidad durante las jornadas electorales (IFE, 2009).

El Centro de Cómputo y Resguardo Documental (CECYRD) integra la base de imágenes de las fotografías que se toman a los ciudadanos que integran el padrón electoral, de acuerdo con información del IFE (2009), existen más de 200 millones de imágenes, entre fotografías, huellas digitales y firmas de los ciudadanos; si esta información se transformara en texto, su contenido sería equivalente a una biblioteca conformada por 1.3 millones de ejemplares, cada uno de 200 hojas tamaño carta, impresas por ambos lados.

Antes de la fecha de algunas elecciones, las listas nominales se exhiben en las diferentes secciones electorales para que los votantes del distrito correspondiente puedan verificar que estén incluidos en el padrón electoral para que puedan ejercer su derecho al voto. Al igual que los partidos políticos, los ciudadanos tienen la facultad de exigir a la autoridad electoral la aclaración de las inconsistencias que pueda presentar el padrón (Gómez y Ornelas, 2006).

En cumplimiento al artículo 161, párrafos 1 y 2 del Código Federal de Instituciones y Procedimientos Electorales, a partir de las elecciones federales de julio de 2003, la Dirección Ejecutiva imprimió las listas nominales de electores con fotografía que se distribuyeron entre los partidos políticos, distritos y casillas electorales y entre cada Vocalía Distrital del IFE como respaldo (IFE, 2009).

En este caso el derecho a la privacidad queda subordinado a un bien jurídicamente protegido distinto: "los derechos de la ciudadanía en la forma de un padrón electoral confiable y auténtico". La norma del Cofipe señala que (Gómez y Ornelas, 2006):

- Los documentos, datos e informes que los ciudadanos den al Registro Federal de Electores serán totalmente confidenciales y no podrán comunicarse o darse a conocer, a menos que haya algún caso de juicios, recursos o procedimientos en que el IFE sea parte.

- Los partidos políticos no pueden dar un uso distinto a la información que contienen las listas nominales y el padrón electoral que no sea revisión y formulación de observaciones.

- Las listas nominales que se exhiben en las secciones electorales son sólo una parte extraída del padrón electoral, no incluye toda la información, únicamente el nombre de los votantes.

Con todas estas acciones, el padrón electoral alcanzó un alto grado de consistencia, de tal manera que los elementos que lo conformaron coincidieron lo más posible con la realidad. Por ejemplo, en 1988 la elección federal se apegó a un padrón que tenía un 50% de inconsistencia, a diferencia de las elecciones de 1994 en las que los estudios le dieron un 94% de confiabilidad (Gómez y Ornelas, 2006). En las elecciones de 2003, el padrón estuvo conformado por 65 millones 337 mil 047 ciudadanos, de los cuales únicamente 64 millones 710 mil 596 contaron con credencial y aparecieron en las listas nominales, de los cuales 51.8 por ciento eran mujeres y 48.2 por ciento hombres (Saúl, 2003).

Para tener mayor conocimiento de la cantidad de información que contiene la base de datos del IFE en la actualidad, a continuación se presentan las estadísticas recuperadas de la página del IFE (2009):

Distribución de ciudadanos por sexo a nivel nacional (IFE, 2009)

Padrón Electoral		
Sexo	Ciudadanos	Porcentaje
Hombres	37 685 110	48.23%
Mujeres	40 454 737	51.77%
Total	78 139 847	100%

Lista Nominal		
Sexo	Ciudadanos	Porcentaje
Hombres	37 201 180	48.23%
Mujeres	39 924 117	51.77%
Total	77 125 297	100%

Tablas 4. Distribución de ciudadanos por sexo a nivel nacional

Distribución de ciudadanos por grupos de edad a nivel nacional (IFE, 2009)

Padrón Electoral		
Intervalo	Ciudadanos	Porcentaje
18	1 218 765	1.56%
19	1 799 089	2.3%
20 a 24	9 902 613	12.67%
25 a 29	10 094 600	12.92%
30 a 34	10 053 677	12.87%
35 a 39	10 053 677	12.87%
40 a 44	7 888 254	10.1%

45 a 49	6 668 523	8.53%
50 a 54	5 412 756	6.93%
55 a 59	4 188 157	5.36%
60 a 64	3 294 559	4.22%
65 o más	8 169 318	10.45%
Total	78 139 847	100%

Padrón Electoral		
Intervalo	Ciudadanos	Porcentaje
18	1 190 299	1.54%
19	1 768 972	2.29%
20 a 24	9 769 474	12.67%
25 a 29	9 979 300	12.94%
30 a 34	9 917 916	12.86%
35 a 39	9 322 282	12.09%
40 a 44	7 778 402	10.09%
45 a 49	6 576 226	8.53%
50 a 54	5 340 760	6.92%
55 a 59	4 136 436	5.39%
60 a 64	3 257 980	4.22%
65 o más	3 257 980	4.22%
Total	77 125 297	100%

Tabla 5. Distribución de ciudadanos por grupos de edad a nivel nacional

Así como se presentan estas estadísticas de acuerdo con la edad y el género, el IFE posee números de acuerdo con la entidad de origen, información de las bajas por duplicados, por situación ciudadana o por pérdida de vigencia. Se trata de millones de datos vertidos en una gran base de datos. Cabe preguntar en este punto qué garantías existían de que toda esta información era debidamente resguardada. Para responder, destaca el caso ocurrido con la empresa estadounidense Choice Point que incurrió en la compra de la base de datos del padrón electoral del IFE.

3.2.1 Choice Point

Fue en 2003 cuando se dio a conocer que la empresa Choice Point, dedicada a la recolección y venta de bases de datos (incluso de ADN) y a proporcionar "inteligencia para la toma de decisiones" de gobierno y empresas privadas, adquirió de una compañía mexicana el padrón electoral por 400 mil pesos. Chuck Jones, portavoz de Choice Point, aseguró que la compra fue dentro del marco legal, acorde con las leyes de ambos países, sin referir el nombre de la empresa con la que realizó la compra porque, según dijo, no podía identificarla sin su autorización, también afirmó que su principal cliente para este tipo de información era el Departamento de Seguridad Doméstica de Estados Unidos y el Servicio de Inmigración y Naturalización, que utilizaban las bases de datos obtenidas de México para corroborar la identidad y ciudadanía de personas que detenían ahí, es decir, el uso primario que daban a esa información era policiaco (Carreño, 2003).

De acuerdo con el IFE, los datos de 58 millones de ciudadanos mexicanos fueron sustraídos del Registro Nacional de Población e Identificación (Renapo), que depende de la Secretaría de Gobernación, mediante la triangulación en la que participaron empleados de una empresa de computación y una compañía que inmediatamente cambió su nombre, a la vez que aseguró que la Secretaría de Gobernación no tuvo algún trato con Choice Point durante esa administración (Herrera, Torres y Otero 2003).

Poco después, Choice Point devolvió la base de datos que había adquirido a la Procuraduría General de la República y se comprometió a suspender su uso y a borrarla de su sistema. El IFE, por su parte, responsabilizó a un Juan López Bedolla, trabajador de la empresa Vanguardia en Informática de haber vendido la información a Ismael Vaca Ramírez, gerente

de sistemas de la empresa Bases de Datos Especializada, que a su vez la vendió a Choice Point, mientras que la Fiscalía Especializada para Delitos Electorales aseguró que no los consideran presuntos responsables del delito (Fepade) y que podría haber varios responsables en cada etapa de la venta de la información (Otero, 2003).

Al continuar las averiguaciones, la Secretaría de Gobernación admitió que no encontraba 18 cartuchos que el IFE le entregó en 1999 y 2000 con todo el padrón electoral, mismos que tampoco fueron reportados en las actas de entrega-recepción por ex funcionarios del Renapo, por lo menos en dos relevos de sus directivos. Presuntamente, los archivos que contenía la información de los 58 millones de ciudadanos debían estar resguardados en Gobernación, pero hasta ese momento ignoraban su ubicación. Por esta razón, de confirmarse la teoría de que la sustracción de la base de datos del padrón electoral ocurrió en el Renapo, sería entonces ésta la información que contenían esos 18 cartuchos que el IFE entregó a Gobernación (Torres, 2003).

Por su parte, Vanguardia en Informática (Vinsa), negó haber participado en el robo del padrón y presentó una denuncia en contra de Ismael Vaca, Jorge López y Adriana López, personas involucradas en la compra-venta de la base de datos que obtuvo Choice Point por traición a la patria, robo equiparable y abuso de confianza, al haber sustraído de 1999 a 2000 los datos para la elaboración del Catálogo Nacional de Derechohabientes Canade que solicitó el Instituto Mexicano del Seguro Social (García, 2003). Según Vinsa, el robo ocurrió mientras los empleados trabajaban en Logística Externa (Logex), que coordinaba los trabajos de este proyecto en el que participaron seis empresas más especializadas, y presumía que esta información era la misma que posteriormente vendieron a Choice Point. Cabe señalar que para ese momento, Jorge López e Ismael Vaca eran director general y empleado, respectivamente, de Soluciones Mercadológicas en Bases de Datos (García, 2003).

Mientras realizaban todas las averiguaciones pertinentes, la PGR no había podido confirmar que Choice Point efectivamente borró la base de datos que contenía el padrón electoral mexicano, después de haber devuelto los discos con la información y asegurar que no conservaban ninguna copia, ya que necesitaban la colaboración del gobierno de Estados Unidos, razón por la cual solicitaron la intervención de la Subprocuraduría Jurídica y de Asuntos Internacionales (Otero, 2003).

Después de haber estado bajo arraigo domiciliario, los inculpados por la venta del padrón quedaron libres bajo una fianza de 96 mil pesos dado que el juez federal les concedió la suspensión definitiva por la orden de aprehensión girada en su contra por el delito de revelación de secreto, que fue el único por el que fueron procesados, ya que anteriormente otro juez determinó que no podían ser acusados por los delitos de carácter electoral y de traición a la patria, que les había consignado la PGR (Otero, 2004).

Esto se debió a que el juez de distrito en materia de procesos electorales con sede en México estimó que las leyes mexicanas únicamente protegen y castigan el mal uso que se haga de los documentos públicos electorales y, para sorpresa, el padrón electoral no es un documento, sino una base de datos; en otras palabras, la causa 141/2003 explica que el uso que se les da "a las actas de la jornada electoral, las relativas al escrutinio y cómputo de los consejos locales y distritales, y las de cómputos de circunscripción plurinominal y, en general todos los documentos y actas expedidos en ejercicio de sus funciones, por los órganos del Instituto Federal Electoral (Avilés, 2004)"; pero el juez explicó que en ningún momento se protege el mal uso que pueda darse al padrón electoral ya que éste constituye "un instrumento electoral con que cuenta el Estado para la elaboración de documentos electorales, sustentados en una base de datos, para garantizar el adecuado desarrollo del proceso electoral (Avilés, 2004)".

A pesar de que la Fepade apeló a esta resolución, el segundo tribunal unitario reafirmó que "cualquier hecho que no esté tipificado por la ley como delito, no lo será y, por ende, no es susceptible de acarrear la imposición de una pena". Finalmente, sólo pudieron castigar a cuatro ex funcionarios de la Secretaría de Gobernación, de quienes la Fepade no podía dar su nombre, por haber proporcionado el padrón electoral a Choice Point, delito distinto al electoral. Para esto tuvo que acusarlos de "ejercicio indebido de servicio público y de usurpación de funciones, porque estas personas tenían que custodiar, vigilar y proteger la información que fue usada indebidamente (Avilés, 2004)".

Christopher Hoofngale, Consejero Diputado del Centro para la Equidad de la Información (EPIC), con base en Washington, reveló que el gobierno americano llevaba más de 18 meses comprando información de uso privado de Estados en 10 países del hemisferio occidental a Choice Point. Después de que interpusieran una demanda a través del Acta para la Libertad de Información contra el Servicio de Inmigración y Naturalización para que desclasificara

documentos relacionados con Choice Point, salieron a la luz pública contratos por más de 11 millones de dólares entre el SIN y el departamento de Justicia para la adquisición de registros de votantes, registros nacionales, de conducir, y otras bases de datos en Argentina, Brasil, Colombia, Venezuela, México, Costa Rica, Guatemala, Honduras, El Salvador y Nicaragua (Gómez, 2003).

Según Hoofngale (Gómez, 2003), el gobierno de Estados Unidos impide dar precisiones sobre el uso que da a esa información bajo el supuesto de que se trata de "Asuntos de Seguridad Nacional". Irónicamente, el gobierno norteamericano adquirió información confidencial de otros países con total conocimiento de que en ese país es considerada "muy sensible", está protegida por la ley, castiga su venta con cárcel y, particularmente, si se diera el caso de la venta de los registros de los votantes, los ciudadanos no se registran para votar.

También afirmó que los países europeos son más estrictos con este tipo de información, por ejemplo, Choice Point no puede comprar bases de datos de europeos ni públicas ni privadas. A pesar de que en América Latina algunos países ya tenían leyes que protegían los datos personales la información fue vendida, lo que denota un problema serio de corrupción y no tanto de vacíos legales (Gómez, 2003).

El caso de Choice Point fue el detonador del problema del vacío legal que existía en México. Para 2004, la Fiscalía Especializada para la Atención de Delitos Electorales investigaba a tres empresas más que comercializaban los datos personales de millones de ciudadanos registrados en el padrón electoral. De acuerdo con la Fepade, las empresas que poseen el padrón lo venden a otras dedicadas a la publicidad o propaganda, con su determinada segmentación, o a despachos encargados de localizar a deudores para cobrarles (Avilés, 2004). Sin embargo, los usos que pueden hacerse de las bases de datos son múltiples, por esta razón era urgente que existiera una ley específica sobre la protección de los datos personales a fin de que la comercialización de esta información fuera condenable.

Cabe señalar que para las elecciones federales celebradas en 2005 todavía existió el riesgo de que los datos personales en poder del IFE fueran mal utilizados por empresas privadas, y aún por partidos políticos, a falta de una ley que los protegiera. Para esas fechas el derecho a la protección de datos personales apenas comenzaba a surgir en México de manera escueta y no

había mucho conocimiento generado en la materia ni una conciencia generalizada sobre la importancia de salvaguardar la información personal.

Es deseable que con las leyes establecidas a la fecha los datos personales en posesión de entes de gobierno, como el IFE, corran con mejor destino, sobre todo con la reforma de ley pública para que aplique verdaderamente las sanciones ante las faltas éticas.

3.3 Otras bases de datos

En una investigación periodística realizada por María de la Luz González de El Universal, en abril de 2010, advirtió sobre la venta de bases de datos con información personal de millones de mexicanos por doce mil dólares en Tepito. De acuerdo con la reportera, que lo comprobó en tres memorias externas, el comprador puede adquirir el padrón electoral del país, el registro vehicular y de las licencias de conducir, los números de los teléfonos públicos del país, los datos de los policías también de todo el país (con la fotografía, número de placa y el lugar donde están adscritos), el parque vehicular del Servicio Federal, que incluye el transporte de carga, etc.

Sumado a todo esto, destaca que esta información no sólo la utiliza el crimen organizado para extorsión, sino también agentes policíacos para "agilizar su trabajo" al rastrear llamadas relacionadas con secuestros o extorsiones realizadas desde teléfonos públicos, trámite que les tomaría aproximadamente cinco días si lo hacen conforme al procedimiento.

En entrevista, González (2010) declaró que los vendedores de las bases de datos le aseguraron que estaban actualizadas a 2009, y ella pudo encontrar sus datos, los de familiares y personas cercanas en el padrón que vendían para corroborar la información.

Sobre la manera ilícita en la que obtienen las bases de datos, agregó que: "Ellos compran las bases de datos a la gente que trabaja en las dependencias, a cualquier empleado que tenga acceso a las bases de datos, no tiene que ser el titular del área, con que sepa sustraer la información es suficiente porque no hay candados,… desafortunadamente en nuestro país no tenemos esta cultura de protección de datos". Y añadió que el caso del padrón resulta muy preocupante "no se sabe de dónde se filtró esa base de datos, el IFE dice que no fue de ahí y jura que el registro tiene candados, pero no conocemos cuáles son esos candados. Yo no sé

cómo resguardan la información que das para un simple trámite porque todas las bases de datos que puedas imaginar están al acceso del crimen organizado: tienen registros de bancos, de escuelas, etc. (González, 2010).

A pesar de que la Fepade inició una averiguación sobre el caso de Tepito, González (2010) afirma que no hay manera de controlar la venta y filtración de la información porque así como los policías compraron las bases de datos, ellos mismos las revendieron para "recuperar su inversión", y no hay manera de detener esto una vez que han sido desprotegidas. Por esto destaca la importancia de las sanciones para no continuar en la impunidad.

Otro caso que le parece preocupante son los partidos políticos porque cuando piden una copia del padrón se les da, "…y de ahí no sabes cuántos más la tienen, qué seguridad tiene el director del partido político, el director de elecciones, etc., sobre esas bases de datos que han sido tan cuidadosamente elaboradas, que han costado tanto trabajo integrar, qué pasa cuando se entregan las copias. ¿Por qué los partidos políticos deben tener nuestros datos? A mí me molesta, yo no soy militante de ningún partido político y pienso que no debería ser así González".

Estas averiguaciones dejan al descubierto la problemática que hay en México en cuanto a la falta de confiabilidad en las bases de datos almacenadas por el gobierno, que son tan vulnerables de robo y fugas de información. Es necesario cuestionar a las autoridades responsables de esa información para saber por qué se quebranta con tanta facilidad su seguridad y cómo es que no resultan responsables.

3.4 Sector Salud

En México, los prestadores de los servicios de salud están clasificados en tres rubros: seguridad social, servicios médicos privados y servicios de población abierta. De acuerdo con información arrojada por el Instituto Nacional de Estadística y Geografía en el censo nacional de 2000, los usuarios de los servicios de salud están distribuidos de la siguiente manera:

Sexo **Grupos de edad**	Población usuaria	Seguridad social	Servicios médicos privados	Servicios a población abierta
Mujeres	48 119 229	39.3	33.7	27.0
O a 4 años	5 080 100	35.5	32.6	31.9
6 a 14 años	10 632 394	35.1	31.5	33.4
15 a 64	29 785 096	40.9	34.6	24.4
65 y más años	29785 096	45.8	34.5	19.7
No especificado	124 517	32.4	37.3	30.3
Hombres	45 352 031	38.4	34.7	26.8
O a 4 años	5 256 931	35.6	32.6	31.8
6 a 14 años	10 898 810	35.4	31.2	33.4
15 a 64	26 925 920	39.6	36.7	24.4
65 y más años	2 140 382	46.4	36.9	19.7
No especificado	129 988	31.3	33.7	30.3

Tabla 6. Población usuaria de servicios de salud de acuerdo con el Censo de Población de 2000 (INEGI, 2000)

El grupo de seguridad social, 39 por ciento de los usuarios, correspondía a personas atendidas en el Instituto Mexicano del Seguro Social, Instituto de Seguridad, Servicios Sociales de los Trabajadores del Estado y demás instancias de seguridad social de gobiernos estatales; 34.2 por ciento comprendía a las personas atendidas por médicos particulares, ya fueran clínicas, consultorios u hospitales privados; mientras que el 26.9 por ciento acudía a servicios de población abierta.

Estos tipos de instancias médicas poseen información personal y sumamente confidencial puesto que se trata del historial clínico de cada paciente. Es necesario mencionar que la

información de todos los que son atendidos por instituciones particulares, es decir, más de la mitad, no está vinculada a los lineamientos establecidos por la Ley de Acceso a la Información y, por tanto, no quedaban protegidos por sus lineamientos referentes a la protección de datos personales.

Para 2003 el IFAI informó que las dependencias del gobierno federal tenían en su conjunto mil 589 sistemas de bases personales que hasta ese momento ya estaban registradas ante el organismo según lo establecido por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Marcelo Garza, ex director del IFAI, enlistó las 10 dependencias del Ejecutivo con más bases de datos personales: ISSSTE (29), Hospital General de México (140), Secretaría de Medio Ambiente y Recursos Naturales (105), Instituto Politécnico Nacional (77), Instituto Nacional de Bellas Artes (42), Secretaría de Salud (35), Seguro Social (31), Secretaría de la Función Pública (28), Instituto Mexicano de la Propiedad Industrial (27) y el Instituto Nacional de Ciencias Penales (26). Por ley, cada una de estas dependencias tiene la obligación de informar al público de las bases de datos personales que posean, a fin de que puedan conocer la información que tienen sobre los usuarios y, en un determinado caso, hacer las correcciones necesarias (Torres, 2003).

Según lo anterior, es necesario señalar que las instituciones de salud alineadas por la LAI como el ISSSTE, IMSS, Secretaría de Salud, entre otros, se encuentran entre las 10 dependencias de la administración pública federal con mayor número de bases de datos personales, cuestión por la que su regulación se hacía pertinente, y aún quedaba el sector de salud privado. Cabe aclarar que con la llegada de la nueva Ley de Protección de Datos Personales en Posesión de Particulares, los hospitales y clínicas privadas deberán registrar sus bases de datos para garantizar la seguridad de la información personal que poseen y cumplir con su reglamente, además de las normas existentes para este sector.

En este orden de ideas, de acuerdo con la Norma Oficial Mexicana NOM-168-SSA1-1998, se entiende por expediente clínico al "conjunto de documentos escritos, gráficos e imagenológicos o de cualquier otra índole, en los cuales el personal de salud, deberá hacer los registros, anotaciones y certificaciones correspondientes a su intervención, con arreglo a las disposiciones sanitarias"; también define un resumen clínico como un "documento elaborado por un médico, en el cual se registrarán los aspectos relevantes de la atención médica de un

paciente, contenidos en el expediente clínico. Deberá tener como mínimo: padecimiento actual, diagnósticos, tratamientos, evolución, pronóstico, estudios de laboratorio y gabinete". La norma establece que los prestadores de servicios médicos del sector público, social y privado deben elaborar y conservar el expediente clínico por un periodo mínimo de 5 años, mismo que debe contener los siguientes datos generales del usuario: nombre, sexo, edad y domicilio. Toda la información contenida pertenece a la institución prestadora del servicio médico y podrán otorgarla únicamente con una solicitud por escrito por el paciente, familiar, tutor, representante y autoridades sanitarias, ya que se trata de información confidencial (NOM-168-SSA1-1998).

A pesar de que la norma menciona que la información contenida en el expediente clínico debe ser manejada con discreción y confidencialidad, se atiene únicamente al cumplimiento de los principios científicos y éticos que orientan la práctica médica, mas no implica una sanción a quien haga un uso diferente o inapropiado de ella.

Por otro lado se encuentran los lineamientos establecidos por la Ley General de Salud en Materia de Prestación de Servicios de Atención Médica referentes al derecho a la información perteneciente a los usuarios de los servicios de salud, entre estos derechos se encuentran los mencionados los siguientes:

El artículo 29 habla sobre la obligación que tiene todo profesional de salud de proporcionar al usuario, familiares, tutor o representante legal, la información completa sobre el diagnóstico, pronóstico y el tratamiento que corresponda; al igual que la NOM 168, en su artículo 32 establece que deben conservar los expedientes clínicos de los usuarios por un periodo mínimo de cinco años.

En este mismo sentido, la Ley General de Salud, artículo 77 bis 37 establece ciertos derechos con respecto a la confidencialidad y a la información:

- Recibir información suficiente, clara, oportuna y veraz, así como la orientación que sea necesaria respecto de la atención de su salud y sobre los riesgos y alternativas de los procedimientos diagnósticos, terapéuticos y quirúrgicos que se le indiquen o apliquen;
- Contar con su expediente clínico;

- Ser tratado con confidencialidad.

Hay un caso específico en el que el prestador de salud debe subordinar el derecho de confidencialidad del paciente a fin de prevenir alguna enfermedad infecto-contagiosa, sobre este respecto, el artículo 35 señala que:

- Cuando en un establecimiento para la atención médica se presente algún demandante de servicios que padezca alguna enfermedad infecto-contagiosa será motivo de notificación obligatoria, deberá referirlo de inmediato al servicio correspondiente, a fin de que dicha persona tenga el mínimo contacto con los usuarios.

Es pertinente indicar que la Ley General de Salud no menciona en su contenido la definición de un expediente clínico y tampoco señala expresamente el libre acceso al contenido de éste y los términos de la titularidad, expresados únicamente por la norma 168. Sólo indica que la atención médica debe realizarse de acuerdo con los principios científicos y éticos que orientan la práctica médica, sin detallar específicamente cuáles son esos principios.

En entrevista, el Dr. Casas (2010), Director de la Comisión Estatal de Arbitraje Médico en Puebla, manifestó que el principal problema de la NOM 168 recae en que muchos médicos del sector público y privado no lo llevan como debe ser: “Por ejemplo, hace unos años hubo un caso muy comprometedor, cuando en el sur del estado de Puebla se cayó un cerro, vino el Presidente de la República y a cargo de la clínica de la región estaba un pasante, entonces el expediente de una persona que iba a ser trasladada decía: el paciente malo se pasa a México. Era todo lo que tenía”. Además de esto, los médicos tienen la obligación de guardar el expediente y tampoco lo hacen.

Se ha creado la controversia de quién es el dueño del expediente clínico si el paciente, el médico o la institución. El expediente clínico es una información que puede usarse para afianzar diagnósticos, en casos académicos para la enseñanza o para la investigación. Un expediente clínico bien llevado puede servir mucho. También es importante porque constituye la única defensa que el médico tiene ante cualquier demanda, ya que lo primero que pide el ministerio público es el expediente y no se le puede agregar ni quitar nada. Además de la historia clínica con antecedentes, notas de evolución, de laboratorio, el gabinete, etc., también debe llevar el consentimiento informado que es lo más importante. Si al paciente se le va a

hacer una operación se le debe explicar todo lo que se le va a hacer, efectos colaterales, qué le puede pasar, etc. y debe firmar de conformidad, lo que es el derecho de la corporeidad, que quiere decir que yo soy dueño de mi cuerpo y le da al médico la autorización para intervenir sobre él. Este derecho está basado en el consentimiento informado, explica Casas (2010).

En cuanto a los riesgos de la confidencialidad, el secreto médico y las excepciones, el Dr. Casas afirma que: "Yo no le veo riesgos a la información, claro que el expediente puede ser tergiversado, pero el acceso a la información debe ser confidencial. La confidencialidad del paciente en el tratamiento de la información es básica, los principios éticos obligan al médico a guardar la confidencialidad. Aunque claro que existen limitaciones, como casos que se salen de la ley, incluso debe dar aviso a las autoridades para establecer cercos sanitarios".

En este mismo orden de ideas, está pendiente el proyecto nacional del expediente clínico electrónico impulsado por la administración del Presidente Calderón. Este expediente es una plataforma de interoperatividad a la cual podrán ingresar las diferentes instituciones de salud que actualmente cuenten con sistemas de expediente clínico electrónico bajo determinados lineamientos tecnológicos y normativos (Ortiz, 2010).

Su intención es facilitar la atención de los pacientes en una institución diferente a la que originalmente ingresaron, con rápido acceso a su historial clínico, para evitar repetir estudios y aprovechar los recursos disponibles. Este tipo de información puede ser muy delicada si no se resguarda debidamente por la sensibilidad de su contenido, pero en septiembre de 2010 se publicó la Norma Oficial Mexicana 024SCA3 2003 del Expediente Clínico Electrónico que incluye la protección de los datos personales, avalada por el IFAI para la Plataforma Nacional de Interoperatividad (Ortiz, 2010), conocida como NOM 024 dentro del Sector Salud, que tiene como objetivo observar los sistemas de Expediente Clínico Electrónico para interoperar, procesar, interpretar, garantizar la confidencialidad, seguridad y el uso de estándares y catálogos de la información de registros electrónicos en salud.

El sector salud en nuestro país ha dado pasos para garantizar la seguridad de los datos personales, incluso Argentina señaló el avance que hay en México, sin embargo, el trato inicial de éstos recae en los médicos que realizan el expediente clínico y en su ética profesional para cumplir con lo establecido por las normas, leyes y reglamentos.

3.5 Sector Educativo

Otro sector en donde era urgente la protección de los datos personales era el educativo. De acuerdo con Ciscomani (2010), en México hay más de 26 mil escuelas privadas y más de 190 mil escuelas oficiales. El uso erróneo de datos personales en posesión de las instituciones educativas puede provocar marginación, discriminación y restricción del acceso de los estudiantes a mejores oportunidades formativas. Por esta razón, Francisco Ciscomani, durante su exposición dentro del marco del VIII Encuentro Iberoamericano de Protección de Datos Personales (2010), manifestó que la regulación y cooperación con el órgano garante era urgente.

El Registro Nacional de Alumnos concentra información de alrededor 25 millones de estudiantes, además del registro oficial de documentos académicos y de certificación, que constituyen un buró de documentos académicos con más de 30 millones de datos, constancias, certificados y títulos emitidos en los diferentes niveles educativos, mismos que, según Ciscomani (2010) fueron inscritos en 2009 en el Sistema Persona del IFAI.

Estas bases de datos, conformada por información de alumnos, familias y empleados, demandan una total protección puesto que abarca una tercera parte de la población nacional y se trata de un sector muy vulnerable que incluye menores de edad.

Entre las medidas que la Secretaría de Educación Pública toma para proteger los datos personales en posesión de las instituciones educativas está la elaboración de normas de control escolar, con criterios mínimos que deberán ser adoptados en los centros educativos por las autoridades escolares, así como una próxima creación de un Manual de Uso y Protección de Datos en centros escolares.

Es muy importante que, además de las leyes establecidas, las instituciones educativas se inclinen por proteger la información de sus alumnos y asimismo funjan como instructores en la materia para crear una cultura de autoprotección.

3.6 Sector de Telecomunicaciones

Hablar de las telecomunicaciones es hablar de las tecnologías de la información que han revolucionado el tratamiento de los datos personales. La Comisión Federal de

Telecomunicaciones supervisa todas las actividades de las telecomunicaciones y la radiodifusión en México, específicamente: telefonía local fija, telefonía celular-PCS, *paging*, T.V. restringida, provisión satelital, larga distancia nacional, larga distancia, larga distancia internacional de entrada, larga distancia internacional de salida y *trunking* (comunicación por radio).

Para el segundo trimestre de 2010, la Cofetel reporta en su diagnóstico e índices de producción del sector (2010): 19 millones 472 mil 888 usuarios de líneas de teléfono fijo, 86.9 millones de usuarios de telefonía celular, 393 mil usuarios de televisión vía microondas, cinco millones 223 mil de televisión por cable y 3.3 millones de vía satélite y 3 millones 251 mil usuarios de *trunkin.* Estos servicios son ofrecidos por diferentes empresas que almacenan información de sus clientes y manejan distintas políticas de privacidad.

Telmex, por ejemplo, declara en su Código de Ética que protege la privacidad de todas las formas de comunicación de sus clientes, ya sean de voz, datos o imágenes. Señala que: "ningún empleado puede obtener, ni usar o difundir información confidencial de un cliente, sin que exista una razón legítima para hacerlo; ningún trabajador debe difundir información alguna de las comunicaciones, transmisiones o tratos de los clientes, a menos que exista un requerimiento legal o que esté en riesgo la seguridad de clientes, trabajadores o bienes de la empresa; los tratos comerciales con los clientes y la información acerca de los estados de cuenta, equipos o circuitos, así como cualquier otra información de los clientes contenida en las bases de datos de la Compañía, sólo podrá ser utilizada por personas autorizadas". Los registros con datos de sus clientes o empleados son confidenciales. Deben ser resguardados y conservarlos actualizados y exactos.

Dentro del rango de la radiocomunicación también se encuentra Nextel, en cuyos estatutos del Convenio para el uso y privacidad del Sitio menciona que respeta la privacidad de sus usuarios, no difunde con propósitos comerciales la dirección electrónica y otra información personal, como su nombre, domicilio o edad, sin su consentimiento. Tampoco otorga permisos a terceros para realizar labores tendientes a identificarlos por medio de sus direcciones de correo electrónico. Sin embargo, el Usuario proporciona a Nextel la autorización para usar su información personal para crear contenido personalizado, servicios y anuncios que tengan que ver con la empresa, así como reportes agregados. De la misma manera, Nextel declara que

coopera con funcionarios estatales, locales o federales en cualquier investigación relacionada con cualquier contenido (Nextel, 2010).

Así como estos ejemplos, muchas empresas de distintos ámbitos dentro del sector privado de las telecomunicaciones manejan bases de datos con información de sus empleados y clientes y, a pesar de que están parcialmente protegidos por algunas leyes, cada una establece sus propios lineamientos con respecto al uso y fin de la información personal.

Un caso relacionado con las telecomunicaciones y el manejo de datos personales es el del Registro Nacional de Usuarios de Telefonía Móvil, mecanismo adoptado en el Acuerdo Nacional por la Seguridad, la Justicia y la Legalidad para contribuir con la prevención, investigación y persecución de delitos como secuestro y extorsión realizados con teléfonos celulares. Este registro contiene el nombre, número telefónico y la Clave Única de Registro de Población (CURP). Con apenas unos meses de existencia, de acuerdo con Víctor Solís (El Universal, 2010), la base de datos ya estaba disponible a la venta en Internet desde junio y el vendedor prometía entregar los datos de los más de 50 millones de usuarios de teléfonos celulares que se dieron de alta en el Renaut.

A pesar de que las intenciones originales de este registro podían ser aprobatorias, Miguel Calderón (2010) manifestó, durante su participación en el panel de telecomunicaciones en el VIII Encuentro Iberoamericano de Protección de Datos, que 40% de la población no creyó que Renaut ayudaría a la seguridad –a un año de su registro no se ha publicado ningún caso en el que haya impedido un secuestro o haya evitado y fraude o soborno- y veintisiete por ciento de la población no registró su teléfono por miedo a que tuvieran su información personal. Además, desde un inicio se trató de un esfuerzo infructuoso y obsoleto porque la relación entre el usuario móvil y la persona que realizó el registro es impredecible ya que no hay manera de garantizar que quien compre el teléfono celular lo conserve o que permanezca en el mismo domicilio que registró.

Un caso reciente e igual inexplicable ocurrió durante las campañas electorales de 2010 en Puebla, cuando usuarios del servicio de radiocomunicación Nextel, cuya política de privacidad sostiene que no difunde la información personal de sus clientes sin su consentimiento, recibieron mensajes de texto con contenido político sin que la empresa asumiera ninguna

responsabilidad y sin explicar cómo se autorizó el uso de la base de datos de sus usuarios para que recibieran los mensajes propagandísticos. En una entrevista realizada por la periodista Patricia Méndez (E-consulta, 2010), la titular de la Dirección de Relaciones Institucionales de la firma, Marisol Romero, sólo respondió que esta cuestión sólo podrían aclararla los altos directivos de la firma. Por otro lado, la Comisión Federal de Telecomunicaciones (Cofetel) indicó como respuesta que entre sus facultades no está regular los contenidos de las campañas publicitarias enviadas vía celular o Nextel, sino lo relacionado con los soportes tecnológicos de estos sistemas de comunicación.

Por estas razones es necesario regular, desde el marco jurídico, el uso que realizan estas empresas privadas con la información de millones de usuarios.

3.7 Internet

Por otro lado aparece un nuevo reto en el sector: Internet. Internet se ha convertido en una herramienta muy útil a la que se han trasladado actividades comerciales, sociales, trámites de gobierno, etc. que antes forzosamente se realizaban personalmente. Esta dinámica reciente ha originado gran preocupación por el riego que implica para la privacidad puesto que, como explicó De la Parra (2010) durante su participación en el VIII Encuentro Iberoamericano de Protección de Datos, la información proporcionada es muy detallada, individualizada y sujeta a procesamiento de forma masiva. También cuenta con información como el IP, que da información sobre el navegador, potencialidades, aplicaciones ejecutadas, tiempo y fecha de visita.

El comercio electrónico representa una de las inquietudes para la seguridad de la privacidad. Sin embargo, es una gran herramienta porque elimina las barreras geográficas y reduce la necesidad de intermediarios. Por esta razón, la protección en la red cobra vital importancia para incentivar la actividad económica dentro del mercado digital. Calderón (2010) expuso que según datos del Banco Mundial: “un incremento en la penetración de diez por ciento del mercado de banda ancha representa un incremento del uno por ciento del PIB, y México, desgraciadamente, hoy tiene una de las penetraciones más bajas de internet del mundo, más reducida que todos los países de la OCDE y de las más bajas si lo comparamos contra nuestros homólogos de otros países latinoamericanos”.

En este mismo orden de ideas, Julio César Vega (2010), dentro del marco del mismo Encuentro, dio a conocer que a pesar de su baja penetración, el comercio electrónico en México ha presentado un crecimiento sostenido de tasas aproximadas de 75 por ciento. De 2007 a 2008 aumentó 85 por ciento en el mercado interno, pero el internauta mexicano ya no compra únicamente en nuestro país, sino que también realiza operaciones en sitios web internacionales, lo que ocasiona que la cooperación internacional entre entidades privadas y públicas cobre mayor relevancia.

Así es que la protección de los datos en la red es un elemento clave para promover este sector porque, a opinión de Calderón (2010), si los usuarios se sienten seguros de hacer transacciones utilizarían más Internet. Sin embargo, también considera que una sobrerregulación tampoco es conveniente porque ocasiona la pérdida de competitividad en el mercado desarrollado mediante las tecnologías de la información. Por esta razón, Calderón (2010) se pronuncia a favor de "una regulación adecuada necesaria para consolidar la confianza de los usuarios en este ambiente digital e incrementar su uso y cantidad de servicios… con soluciones compatibles a regulaciones internacionales". Esto último es importante porque internet es una red global y podría ser problemático que la normativa mexicana difiriera mucho de la normativa de otros países.

El consentimiento del usuario debe ser indispensable, y para Calderón (2010) esto es una dicotomía porque muchas veces el usuario se preocupa por el uso de sus datos personales a la vez que, con gran facilidad, proporciona demasiada información sobre sí a las redes sociales.

Calderón (2010) también hace énfasis en la autorregulación puesto que Internet no es provisto por un solo operador, sino que existen proveedores de dispositivos, proveedores de aplicaciones, proveedores de soluciones, proveedores de contenidos y proveedores de acceso. Normalmente las regulaciones van dirigidas hacia los proveedores de las telecomunicaciones para quienes es técnicamente imposible vigilar todo el contenido de la red.

Otro elemento importante es la seguridad como un atributo de los servicios ofrecidos. Sin un servicio ofrece protección y seguridad gozará de mayor confianza para que sus clientes realicen operaciones, con el fin de crear un equilibrio entre el desarrollo del mercado y la seguridad de los usuarios.

Cada sitio web cuenta con políticas de privacidad en los que establecen cláusulas sobre el uso que harán de los datos personales, el fin para el que los recopilan y su transmisión a terceros, que los usuarios generalmente aceptan sin leer para poder registrarse y realizar alguna operación.

3.8 Redes sociales: *Facebook*

En la actualidad *Facebook* tiene alrededor de 500 millones de usuarios, se dice que si *Facebook* fuera un país sería el tercero más poblado del planeta. Por esta razón, la seguridad en la red social ha sido tema crucial para algunos países y México también comienza a entrar en el debate.

Canadá fue uno de los primeros países en prever el riesgo que *Facebook* representaba para sus usuarios. Entre esas amenazas, Chantal Bernier (2010) destacó algunos puntos durante su ponencia en el VIII Encuentro Iberoamericano de Protección de Datos Personales: 1)los parámetros de confidencialidad de *Facebook* no eran suficientemente robustos, 2)obtenía y utilizaba datos personales con fines publicitarios en exceso de los fines por los cuales los había recibido, 3) comunicaba los datos personales de los usuarios a terceros que desarrollaban aplicaciones, y 4) no cercioraba el uso de los datos personales de nuevos usuarios por personas que no estaban inscritas en la red social.

Otras de las preocupaciones que manifestó la Universidad de Ottawa fueron las cuestiones de la notificación y del consentimiento, deseaban saber si la información que *Facebook* ofrecía a sus usuarios era suficientemente clara para que pudieran dar un consentimiento que fuera válido para la obtención, utilización y divulgación de los datos personales. Los mecanismos de seguridad también eran un tema de riesgo por el millón de terceros dedicados a elaborar aplicaciones. En resumen, las negociaciones que Canadá inició con *Facebook* giraron en torno a las aplicaciones elaboradas por terceros, la desactivación y anulación de cuentas que no eran claramente distinguidas, las cuentas de usuarios fallecidos y los datos personales de los no usuarios (Bernier, 2010).

España, por otra parte, también se ha ocupado por la privacidad de los usuarios en *Facebook* y en 2009 logró que se estableciera que el mínimo de edad para ser usuario fueran catorce años.

México, por su parte, de acuerdo con Ornelas (2010), directora general de Clasificación y Datos Personales del IFAI, las empresas que administran redes sociales en Internet deberán cambiar sus políticas para proteger la integridad física y moral de niños y adolescentes mexicanos, si no lo hacen serán sujeto de las sanciones de la nueva ley de particulares, que es una herramienta útil para obligar a la industria a que establezcan mecanismos para avisar a los niños que la información que suban a las redes sociales sólo van a usarla en esos espacios y no en buscadores como *Google* o *Yahoo* si no existe un consentimiento expreso de los usuarios.

Además de esto, Ornelas (2010) señaló que, de acuerdo con pronunciamientos del VIII Encuentro Iberoamericano de Protección de Datos, es necesario que gobiernos, sociedad e industria se comprometan para:

- Sensibilizar sobre los riesgos que las redes sociales pueden representar para los menores de edad.
- Prevenir mediante la educación de los menores. Esto conlleva la capacitación de docentes.
- Concientizar a los padres de familia para que adopten medidas preventivas en los hogares.
- Propiciar que los gobiernos establezcan políticas públicas con injerencia en el tema.

Finalmente, Ornelas (2010) señala que la principal misión del IFAI es trabajar en una cultura de la prevención y no en una cultura sancionadora y, en este mismo sentido, Vélez (2010) se pronuncia a favor de la actividad de las universidades en este tema para crear responsabilidad, tal como es el caso de Canadá.

3.9 Aspectos generales

Como se ha leído en este capítulo que explica el trato que algunos sectores dan a los datos personales, tanto el sector público como el sector privado cuentan ya con leyes y políticas públicas que protegen su seguridad, además de normas u otras leyes complementarias. Sin embargo, hay sectores que pertenecen tanto al ámbito público como al privado, tal es el caso de las instituciones de salud o educación, que evidencian que el hecho de que existan dos leyes que diferencien desde esta perspectiva (público y privado) está de más porque bien podría ser una misma ley que simplifique la labor del legislador y del órgano garante que, por tratarse del mismo que garantiza a su vez el acceso a la información, es bastante complicada.