INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN PÚBLICA – IFAI
DIRECCIÓN GENERAL DE CLASIFICACIÓN Y DATOS PERSONALES

INFORME SOBRE CAPACITACIÓN RECIBIDA POR LA OFICINA DE PRIVACIDAD DE CANADÁ A UNA DELEGACIÓN DE FUNCIONARIOS DEL IFAI, DE DISTINTAS DEPENDENCIAS DEL GOBIERNO FEDERAL Y ENTIDADES FEDERATIVAS

DEPENDENCIA: Privacy Office, Ottawa.

ASISTENTES: Por parte del IFAI, María Marván Laborde y Horacio Aguilar Alvarez de Alba, Comisionados del IFAI, y Lina Ornelas Directora General de Clasificación y Datos Personales. También asistieron Consejeros de los Institutos de Acceso a la Información de los Estados de Coahuila, Guanajuato, México y Querétaro; un representante del Banco de México y otro de la Concamín; así como funcionarios de las Secretarías de Gobernación, de Economía, de la Comisión Federal de Mejora Regulatoria y del Servicio de Administración Tributaria.

LUGAR: Ottawa, CANADÁ.

FECHA: 1 al 3 de mayo de 2006

DESARROLLO:

La Oficina de Privacidad de Canadá, a través de la Comisionada Jennifer Stoddart, organizó una capacitación a servidores públicos mexicanos, tanto del ámbito federal como estatal, con la participación de una amplia gama de funcionarios de dicha oficina y diversas actividades conexas, como una visita a la oficina del Comisionado de Acceso a la Información Sr. John Reid, a la sesión de preguntas del Parlamento en la que participa el Primer Ministro, y un encuentro con el Sr. Peter Boehm, Vice Ministro Adjunto para América del Norte, Departamento de Relaciones Exteriores y Comercio Internacional de Canadá.

A continuación se resumen los aspectos sustantivos de las reuniones con el personal de la Oficina de Privacidad Canadiense (OPC) y con el Comisionado de acceso a la información. Se anexan al presente informe, las presentaciones electrónicas que fueron proporcionadas por la OPC, durante la capacitación.

Lunes 1 de mayo de 2006

- **Primera sesión.**

Impartida por: Heather Black, Comisionada Asistente de la Privacidad de Canadá, y Pat Kosseim, Consejero General de la OPC.
Temática: Promoción y Protección de la Privacidad a Nivel Federal – Un examen general del mandato y la legislación de la OPC.

En esta sesión introductoria, se explicó en qué consiste la legislación canadiense en materia de privacidad y protección de datos personales. Se analizaron el objeto y alcances tanto del acta de privacidad *"Privacy Act"*, como de la nueva regulación sobre Protección de Información Personal y Documentos Electrónicos *"Pipeda"*. En el primer caso, el objeto del acta de privacidad es proteger la privacidad de los individuos respecto a la información que de sí mismos obre en alguna institución gubernamental Canadiense, mientras que la *Pipeda* se limita a apoyar y promover el comercio electrónico al tiempo de proteger información personal que sea recabada, usada o divulgada en actividades comerciales. A nivel provincial existen marcos normativos sustancialmente similares, como lo es en los casos de Alberta y Ontario, asimismo, dichas provincias también regulan la protección de otro tipo de datos personales, no solo de aquellos involucrados en transacciones comerciales, sino también los datos de salud o de educación.

La Oficina de Privacidad de Canadá se encarga de vigilar el cumplimiento de ambos ordenamientos jurídicos (Privacy Act y Pipeda). La OPC, realiza investigaciones sobre demandas particulares y también puede iniciar procedimientos de oficio, en ambos casos protegen a los denunciantes; emite recomendaciones por lo que sus resoluciones no tienen fuerza obligatoria; también presenta recursos ante el Tribunal Federal; realiza verificaciones; promueve la educación del público, y el respeto de los datos personales. En los casos que involucran temas de acceso a la información personal, por ejemplo, relativa a servidores públicos, se coordinan con la Oficina de Acceso a la Información.

En el caso del Acta de Privacidad, la cual está en vigor desde 1985, se considera que es necesario revisarla para hacerle adecuaciones para robustecerla y actualizarla. Dicha normatividad prevé el derecho de acceso y corrección de datos personales, define a los datos personales como la información relativa a un individuo identificable que se encuentre bajo cualquier forma, proporcionando una lista genérica, aclarando que no es restrictiva. A esta ley se le ha dado la

categoría de cuasi constitucional, ya que sus principios se encuentran recogidos en la Carta Canadiense de Derechos y Libertades. Se abordó también aquellos casos de acceso a la información personal por parte de terceros, en los cuales se aplican los principios de consentimiento y revisión del interés público, como es el caso de cierta información de servidores públicos que la misma ley establece que puede divulgarse, señalando que se trata únicamente de aquella información relativa al cargo y las funciones de dicho empleado.[1]

La puesta en marcha de la *Pipeda* se ha efectuado a partir de año 2000, a través de la aplicación de 10 principios fundamentales entre los que destacan, el de rendición de cuentas, identificación de los fines, consentimiento y limitación de la recolección, uso, divulgación y retención de los datos. La regulación para circulación de información personal en el ámbito comercial descansa sobre el sistema denominado *opt-out*, que consiste en que a través de un aviso de privacidad, se le informa al titular de los datos la finalidad para la cual serán utilizados y la manera de oponerse expresamente al tratamiento de su información, por lo que ante el silencio, se considera que se cuenta en todos los casos con su consentimiento tácito o también denominado implícito. La *Pipeda* será revisada por el Parlamento, ya que dicho ejercicio debe llevarse a cabo cada 5 años.

- **Segunda sesión.**

Impartida por:
Stephanie Perrin, Directora, Departamento de Investigación y Políticas
Anne Marie Hayden, Directora, Departamento de Educación Pública y Comunicaciones OPC.
Temática:
Creando Conciencia—Investigación, Políticas y Educación Pública en la OPC

La primera parte de la sesión fue impartida por la Directora del Departamento de Investigación y Políticas, la cual explicó cómo se llevan a cabo las investigaciones dentro de la OPC, en particular, se mencionaron los casos sobre Investigación sobre cuestiones de actualidad como el uso extensivo de dispositivos de radio frecuencia para la localización de objetos o personas y su potencial amenaza a la privacidad (RFID); los caso sobre correos electrónicos no deseados (SPAM); investigaciones sobre cuestiones ante el Parlamento como la puesta en marcha de la lista de personas que no quieren recibir llamadas de promoción comercial

[1] La información personal que se puede divulgar de servidores públicos se encuentra definida en el apartado 3, inciso j): (i) El hecho de que el individuo es o fue oficial o empleado de una institución gubernamental; (ii) el cargo y domicilio gubernamental, incluyendo el teléfono; (iii) el rango salarial al que pertenece (no se entregan sueldos exactos), las responsabilidades del cargo desempeñado, (iv) el nombre del individuo en un documento preparado por el individuo en el curso de su empleo y, (v) sus opiniones personales o puntos de vista del individuo durante el curso de su empleo.

(*"do not call list"* o listas Robinson); cuestiones sobre auditorias y autentificación de personas.

También, el área de investigaciones lleva a cabo análisis para el Parlamento sobre nueva legislación que puede resultar invasiva a la privacidad (v.g. *Ley antiterrorista*); sobre cuestiones políticas y administrativas que los ministerios someten a su consideración como lo son los casos de personas desaparecidas, circulación de los datos a través de las fronteras, la tarjeta de identidad nacional, y realizan una labor relevante al elaborar análisis de riesgo e impacto de nuevas tecnologías y ofertas de servicios (v.g. puntos de acceso inalámbrico, informática omnipresente).

Otra labor relevante que realiza el área de investigaciones, es la de hacer propuestas para tratar de armonizar la normatividad federal con las provinciales, por ejemplo, actualmente analizan directrices sobre la utilización de RIDF o sobre video vigilancia de las policías.

Finalmente, participan en los foros internacionales de discusión como lo son, la Conferencia Internacional de Comisarios de Privacidad y de Protección de Datos; el grupo de trabajo en protección de datos personales en las telecomunicaciones (IWGDPT), la OCDE, y APEC.

La segunda parte de la sesión se centró en explicar la labor educativa y de comunicación social de la OPC, en donde buscan tener un papel pro activo y estratégico, abarcando sectores relevantes de la población para generar conciencia, por lo que centran sus esfuerzos en sensibilizar a la opinión pública.

La OPC lleva a cabo ciclos de conferencias, talleres y eventos en relación con las dos leyes federales y han creado una "marca" de la OPC. Se impulsa el conocimiento generalizado del sitio en Internet de la OPC, el cual tiene información relevante y es amigable con los usuarios ya que responde a las preguntas mas frecuentes. Llevan a cabo la publicación anual del informe de la OPC y hacen seguimiento en medios de comunicación.

Finalmente, derivado del aumento de recursos financieros que le han sido aportados a la OPC, en los próximos años, el énfasis será puesto en nuevas actividades como lo son, la elaboración de un plan de comunicaciones estratégico, la creación y fomento de comités editoriales, la publicación de artículos en la página de tribuna libre, más productos/actividades para los parlamentarios, aumento de las iniciativas de colaboración, publicaciones, módulo de aprendizaje electrónico para las empresas, y la coordinación de eventos, entre los que destaca el hospedaje de la conferencia de Comisionados de Privacidad y protección de datos personales del 2007.

- **Tercera sesión.**

Impartida por: Anne Rooke, Directora General Asistente, Departamento de Investigaciones, y Trevor Shaw, Director General, Departamento de Auditorias.
Temática: La OPC en materia de cumplimiento

Esta sesión abordó el procedimiento de investigaciones seguido por la OPC, el cual se estructura como a continuación se describe.

La Dirección de Investigaciones y Solicitudes de Información recibe las solicitudes por carta, teléfono y personalmente. Luego de un análisis inicial se determina la admisión y a partir de ese momento, empiezan a correr los plazos de ley. Posteriormente, se analizan los derechos correspondientes en temas sobre Denegación del acceso, recogida, uso y divulgación de datos, retención, consentimiento y salvaguardias. Existe un procedimiento de resolución rápida.

En la fase de investigación se llevan a cabo las tareas siguientes: establecimiento de los hechos; entrevista a los testigos; examen de la documentación, y ya en ejercicio del poder de investigación, se ordenan comparecencias; se exigen pruebas testimoniales; se puede ordenar la inspección in situ para obtener evidencias y documentos que se analizan posteriormente, y se realizan entrevistas en privado.

Una vez terminado el análisis, éste se presenta con recomendaciones particulares, con lo cual se puede llegar a un arreglo luego de una revisión del comisionado o del sub comisionado del expediente, quienes toman una decisión adecuada, la cual se notifica a las partes. Los resultados de una solicitud pueden encontrar que la misma no estuvo bien fundada, o si esta contaba con los fundamentos adecuados, por lo cual se procedió a resolverla emitiendo las recomendaciones correspondientes, mismas a las que se les da seguimiento para verificar su correcta implementación. Un demandante o la misma comisionada pueden acudir al Tribunal Federal tanto por cuestiones relacionadas con el Acta de Privacidad, como por la *Pipeda*, el tribunal puede denegar el acceso, o bien, ordenar a la organización que corrija las malas prácticas y otorgue una compensación al titular de los datos[2]. Algunos casos relevantes resueltos por la

[2] Estadísticas del 1 de enero al 31 de diciembre de 2005.

- **Solicitudes de información personal:**

Privacy Act		***Pipeda***	
Recibidas:	2.670	Recibidas:	5.685
Cerradas:	2.798	Cerradas:	6.210

- **Demandas:**

Privacy Act		***Pipeda***	
Recibidas:	1.209	Recibidas :	400
Terminadas:	886	Terminadas :	401

OPC se refieren a la venta de máquinas de fax, asuntos de video vigilancia en lugares de trabajo, intercambio de información para la comercialización de productos, faxes mal dirigidos, robo de computadoras, y políticas de protección de datos en hoteles.

En la segunda parte de la sesión se habló de la importante y delicada labor de Auditoria que lleva a cabo la OPC, a través de la cual se llevan a cabo los llamados Privacy Impact Assessment (PIA's). El área de auditoria es muy activa ya que tiene a su cargo la inspección de 156 instituciones federales, mas todo el sector privado en el ámbito comercial. Es un área estratégica porque las auditorias son una herramienta esencial para promover la privacidad, ya que una auditoria puede cambiar comportamientos. A través de las auditorías se lleva a cabo una protección pragmática de los datos personales, ya que las organizaciones "no hacen lo que esperas, sino lo que inspeccionas". Con el aumento presupuestal que autorizó el Parlamento para la OPC, una de las áreas que se verán mas fortalecidas con recursos humanos y materiales, es la de auditorias.

Martes 2 de mayo de 2006

- **Cuarta sesión.**

Temática: Privacidad en el Sector Salud en Canadá — Retos y Oportunidades

Ponentes:

Anne Cavoukian, Comisionada de la Privacidad e Información en Ontario.
Marcel Nouvet, Viceministro Adjunto para la Salud en Canadá

En Ontario, es una sola autoridad la encargada del acceso a la información pública gubernamental y la protección de la privacidad. La Comisionada de información y privacidad, la Doctora Cavoukian, abordó en esta ocasión, el delicado e importante tema de la protección a la intimidad y privacidad de las personas, cuando se trata información relativa a su salud por profesionales de la medicina, con especial énfasis en los expedientes clínicos electrónicos.

La Dra. Cavoukian señaló que la necesidad de privacidad nunca había sido mas importante como en la actualidad, debido a la extrema sensibilidad de la información personal relativa la salud, la insuficiente y atomizada regulación a lo largo del sector; el incremento de los intercambios electrónicos de información sobre la salud, y los múltiples actores involucrados en este tema.

A diferencia del nivel federal, la provincia de Ontario si cuenta con una regulación especial en materia de protección de la información personal relativa

a la salud *The Personal Health Information Protection Act, (PHIPA).*[3] Esta regulación entró en vigor en noviembre de 2004, y se basa en los principios sobre prácticas leales para el tratamiento de información personal como el principio del consentimiento y finalidad, entre otros. La PHIPA define quienes son los actores involucrados con el tratamiento de información personal, así como las formas en que puede otorgarse el consentimiento por parte de los titulares, los cuales deben ser informados acerca de los alcances de su decisión.

La Oficina de Información y Privacidad de Ontario es muy activa y ha elaborado diversos folletos informativos para diseminar el conocimiento acerca de la importancia de la protección de los datos personales, y en particular, en el ámbito de los hospitales, han elaborado folletos y carteles, de los cuales el IFAI obtuvo ejemplares.

Respecto al expediente clínico electrónico, se hizo énfasis en las ventajas de la automatización de la información ya que se mejora la calidad y los costos de los servicios de salud, así como la investigación médica, a través de un rápido acceso a una gran cantidad de datos; asimismo, se puede lograr una mayor seguridad a través de controles y auditorias, y también se puede mejorar la protección de la privacidad limitando el acceso, solo a aquellos actores que tengan "la necesidad de conocer" dicha información.

Los retos en esta asignatura se centran en lograr un adecuado control del intercambio de información; de accesos no autorizados o no autorizados, los cuales pueden catastróficos debido al volumen, cantidad y calidad de los datos, así como a su utilización.

A consulta expresa del IFAI se aconsejó que antes de dar inicio a políticas públicas de digitalización y/o automatización electrónica de expedientes y datos clínicos, es necesario llevar a cabo una análisis del impacto en la privacidad que dichas políticas pueden conllevar, de modo que deben contemplarse con el sector salud, los aspectos siguientes:

- ¿Qué tipo de datos deben contemplarse en el expediente clínico electrónico, solo los clínicos u otros más sensibles?
- ¿Los datos deben ser almacenados en un servidor central o en el punto de generación?
- ¿Cómo debe administrarse el consentimiento del paciente (expreso o implícito), particularmente cuando se interactúa con sistemas que no contemplan el consentimiento?

[3] Otras regulaciones en la materia se han expedido en **Alberta (***Health Information Act);* **Manitoba, (P***ersonal Health Information Act;* **Québec,** *Act respecting access to documents held by public bodies and the protection of personal information, Act respecting the protection of personal information in the private sector, y* **Saskatchewan,** *Health Information Protection Act.*

- ¿Cuáles son los niveles de seguridad que constituyen "medidas razonables" para cada caso concreto?
- ¿Quién accede a qué tipo de información y con qué propósitos?
- ¿Quién da seguimiento a las fallas en las medidas de seguridad o de protección de la privacidad y notifica a los titulares dichos aspectos?

Finalmente, se dio un panorama de la situación a nivel internacional, en la cual, los EUA planean que en 2010, todos los americanos tendrán un expediente clínico electrónico. Los países miembros de la Unión Europea también planean un programa similar. Ante los vertiginosos avances tecnológicos en este campo, lo más recomendable es realizar evaluaciones preliminares acerca de los impactos a la privacidad de los pacientes.

- **Quinta sesión.**

Impartida por: Alain Jolicoeur, Presidente, Agencia de Servicios Fronterizos de Canadá.
Temática:
Seguridad en la Frontera y Privacidad en Canadá.

La Agencia de Servicios Fronterizos de Canadá (ASFC), fue creada en diciembre de 2003. Depende del ministerio de Seguridad Pública de Canadá y tiene por misión, contribuir a implementar las prioridades de seguridad nacional; ofrecer servicios fronterizos integrados, y facilitar la circulación transfronteriza de bienes y personas que entran y salen del país.

La ASFC es una institución que conjunta las atribuciones en materia de aduanas, migración e información fronteriza. Dicha institución da seguimiento a las leyes que regulan la admisibilidad de personas y bienes en territorio Canadiense y son los encargados de establecer las políticas de movimientos transfronterizos. Cuentan con el algoritmo de análisis de riesgo mas avanzado del mundo ya que pueden obtener información sobre los contenedores que arriban a territorio Canadiense con 24 horas de anticipación, esto se logra mediante el trabajo de agentes de inteligencia Canadienses que inspeccionan los contenedores en los puertos extranjeros para asegurar embarques seguros. La ASFC también trabaja con el Centro Nacional de Evaluación de Riesgos (CNER), el cual cuenta con la tecnología mas avanzada en un laboratorio científico donde se llevan a cabo pruebas sobre detección de radio actividad, reconocimiento de iris del ojo, rayos x, espectro de movilidad de iones para detectar explosivos etc.

Como la ASFC controla un sinnúmero de bases de datos personales[4], en materia de privacidad, la circulación transfronteriza de la información personal, plantea desafíos únicos relacionados con la protección de la información privada. Por lo anterior, la ASFC busca encontrar un equilibrio entre la seguridad y protección de las fronteras Canadienses y los límites en la comunicación de la información privada de sus clientes. Para lograr este objetivo, la ASFC se sirve del mandato que tiene por ley; los programas de información de inteligencia y análisis de riesgos; las relaciones bilaterales con países clave, y las leyes canadienses, todo lo anterior para crear una frontera inteligente, basada en una organización inteligente, con valores como la integridad, el respeto y el profesionalismo.

La ASFC cumple con la normatividad en materia de protección a la privacidad y actualmente hospeda actividades de auditoria de la OPC en curso, en particular en temas sobre los intercambios de información con EUA y la publicación de un informe previsto para el verano de 2006.

Un aspecto interesante mencionado por el ponente, es que las expectativas de los viajeros con relación a su privacidad, no son las mismas que las de los canadienses en su vida cotidiana, es decir, que un ciudadano canadiense admitiría un mayor control sobre su información y la de personas que ingresan a su territorio, por razones de seguridad. Es ese rubro, la ASFC es cuidadosa al capacitar a los agentes migratorios, para llevar a cabo cuestionarios por niveles, y dado que por el cruce de bases de datos antes de que las personas ingresen a territorio canadiense, ya se tiene un "pre-clearance" o perfil mínimo del pasajero, solo en caso de ser necesario se realizan preguntas mas sensibles sobre información patrimonial, familiar y la vida personal del mismo[5].

Finalmente, se hizo mención a la Alianza para la Seguridad y la Prosperidad de América del Norte, firmada en marzo de 2005 por Canadá, México y Estados Unidos, la cual tiene como objetivo aumentar la seguridad y protección de América del Norte; facilitar el crecimiento económico de los tres países, y mejorar la calidad de vida en la región. Asimismo, entre 2003 y 2004, Canadá y México discutieron un Memorandum de Entendimiento para el intercambio de información relacionada con el TLCAN, en el cual, es necesario revisar cuestiones

[4] La ASFC cuenta con varios programas de obtención de información previa que le permiten gestionar la frontera de forma más eficaz:

- Sistema de Información Previa sobre Pasajeros (SIPP)
- Registro del Nombre de Pasajeros (RNP)
- Información Anticipada sobre Expediciones Comerciales (IAEC)
- Iniciativa de Seguridad de Contenedores (ISC)

[5] Mediante la autorización previa de los viajeros, la ASFC facilita la circulación transfronteriza de los bienes y personas, ya que cuenta con las siguientes bases de datos: NEXUS, Programa de Expediciones Rápidas y Seguras (EXPRES), y CANPASS, a través de los cuales, se puede saber si un pasajero se encuentra en listas de delincuentes buscados e información de diversa índole.

relacionadas con la seguridad de las bases de datos y la protección de la privacidad.

- **Sexta sesión.**

Impartida por: Linda Routledge, Directora, Asuntos del Consumidor, Asociación Canadiense de Banqueros; Louise Cannon, Vice Presidente Superior, División de Cumplimiento, Bank of Nova Scotia, y Robin Gould-Soil, Gerente General, Asuntos de Privacidad, TD Bank Financial Group.

Temática: Protección de la Privacidad en el Sector de Servicios Financieros

La privacidad ha sido piedra angular para el sector financiero, dado que la confidencialidad en el manejo de la información por parte de este sector, en particular el bancario, es consustancial a las operaciones que realizan y porque solo sus titulares pueden tener acceso a la misma. La privacidad ha sido parte de los códigos de conducta financieros desde 1900.

En Canadá, el sector de servicios financieros queda sujeto a la regulación de la PIPEDA, aunque con anterioridad ya contaban con medidas para la protección de la privacidad. El sector financiero ya cumplía con los principios de la OCDE de 1980, en materia de privacidad y movimientos transfronterizos de datos, por lo que en 1985, la Asociación Canadiense de Banqueros (ACB) publicó sus principios de privacidad para proteger la información de sus clientes. A partir de ese año y hasta el 2000, el sector financiero jugó un papel muy activo creando conciencia y aplicando los principios de protección de información personal, que ayudaron a la conformación de una legislación que ahora es obligatoria a todo el sector comercial a través de la PIPEDA.

Los diez principios aplicables a la privacidad en el sector financiero son:

1. Principio de **responsabilidad**: Los bancos son responsables y rinden cuentas acerca de la información que controlan;
2. Principio de **proporcionalidad**: Los bancos identifican los propósitos para los cuales será utilizada la información;
3. Principio del **consentimiento**: Los bancos obtienen el consentimiento para recabar, usar y divulgar información;
4. Principio de **finalidad**: Los bancos limitan la recolección y el uso de información a aquella únicamente requerida para los fines de otorgamiento de servicios;
5. Principio de finalidad: Los bancos limitan el uso y en su caso, divulgación y retención a los fines consentidos y para ciertos fines;
6. Principio de **calidad** de los datos: Los bancos mantienen la información actualizada;

7. Principio de **seguridad**: Los bancos protegen la información de acuerdo con su sensibilidad;
8. Principio de **información**: Los bancos informan a sus clientes acerca de sus políticas de privacidad;
9. Principio de **acceso y corrección** de datos: Los bancos proveen a sus clientes el acceso necesario a su información para que puedan verificarla, y
10. Los bancos atienden las quejas de los clientes en temas de privacidad.

El sector de servicios financieros en Canadá apoya la regulación en materia de protección a la privacidad y proponen algunas enmiendas a la PIPEDA para que no se convierta en un obstáculo en la efectiva prevención de fraudes; el conocimiento generalizado de cierta información que podría ser de interés público; clarificar los derechos de acceso y evitar abusos, y finalmente, lograr facilitar investigaciones a través de la armonización a nivel federal y provincial en temas como recuperación de cartera vencida y pago de deudas, adquisiciones y fusiones, etc.

El Banco Scotiabank cuenta con un programa de privacidad exhaustivo que establece reglas estrictas en el manejo de la información de sus clientes y que exige de sus funcionarios en todas sus subsidiarias, el apego al código de privacidad; para ello, otorgan la capacitación correspondiente a todos los empleados. También se llevan a cabo auditorias de control, hay una intensa campaña de información a los clientes acerca del uso que dan a sus datos, otorgando no solo avisos de privacidad[6], sino folletos informativos y otra información en línea de cómo salvaguardar su información[7]. También cuentan con las más altas medidas de seguridad para asegurar la integridad de la información.

Finalmente, se hizo una presentación de las políticas de privacidad por parte del encargado de la oficina de asuntos de privacidad del grupo TD Bank Financial

[6] Los avisos de privacidad deben incluir qué datos se recaban, para que finalidad, por quiénes (responsables de las bases de datos), las opciones para el titular (opt-in opt out) y cómo contactar a la organización. Los avisos deben ser completos, pero al mismo tiempo muy fáciles de entender ya que aquellos con demasiada información en ocasiones no son fácilmente comprensibles. Dado que muchos formatos no cuentan con demasiado espacio, se pueden incluir resúmenes del aviso de privacidad en tres líneas y a petición de los titulares se entrega el aviso completo. Si la finalidad para la cual fueron recabados los datos va a modificarse, siempre se notifica al titular de los datos para obtener su consentimiento. Estos avisos de privacidad, equivalen a nuestra leyenda de información al titular de los datos a que se refieren el Décimo séptimo y Décimo octavo de los Lineamientos de protección de datos personales.

[7] Los clientes del banco pueden conocer mas acerca de las políticas de privacidad aplicables, a través de un folleto informativo denominado "El grupo Sotiabank y tu: Una cuestión de privacidad" ("*The Scotiabank Group and You: A Question of Privacy")* el cual puede obtenerse, así como otra información relacionada, a través del sitio: www.scotiabank.com

Group, el cual también considera que la PIPEDA es un ordenamiento relevante y al igual que Scotiabank, lleva a cabo estrategias internas para asegurar la privacidad de sus clientes.

- **Séptima sesión.**

Impartida por: Sue Lajoie, Políticas de Información, Privacidad y Seguridad, Consejo del Tesoro.
Temática: Un enfoque interno- Casos de estudio en la implementación de políticas de privacidad.

Se analizaron varios casos recientes que involucran temas de rendición de cuentas y privacidad.[8]

La funcionaria abordó la problemática que enfrentan las autoridades en los casos de apertura de información confidencial y señaló que existen maneras de aproximar este tipo de situaciones a través de un balance entre el interés público contra la amenaza a la privacidad de un individuo.

En estos casos, remarcó que no por el hecho de que el público tenga un interés en algún caso en particular, ello significa que existe un "interés público" en conocer la información. El balance debe basarse entonces en una prueba denominada prueba de la invasión a la privacidad *"invasión of privacy test",* la cual sopesa:

1. Las expectativas de privacidad del individuo;
2. La naturaleza de la información persona involucrada, y
3. Las posibles consecuencias para el titular de la información en caso de que se ordene la divulgación de la misma, contra el interés público. En otras palabras, que el bien público a generar sea mayor, que el daño al particular.

Ante solicitudes de esta naturaleza, las oficinas gubernamentales dan vista a la Comisión de Privacidad, la cual decide si notificar al individuo o individuos concernientes, o iniciar una queja contra las acciones de una oficina en particular.

Miércoles 3 de mayo de 2006

[8] Además de la presentación en power point, se tiene copia de la presentación más detallada de cada caso, los cuales aportan elementos valiosos a ser considerados por el IFAI, en caso de ser necesario.

Reunión con el Comisionado John Reid, de la Oficina de Acceso a la Información de Canadá.

El Comisionado Reid expuso que con el gobierno del nuevo Primer Ministro Harper, el derecho de acceso a la información atraviesa por una situación de riesgo, al poder verse disminuido, ya que se ha presentado una propuesta de reformas al Acta de Acceso a la Información (Access to Information Act) a través de una nueva Acta denominada Acta Federal de Rendición de Cuentas (Federal Accountability Act).

Derivado de lo anterior, el Comisionado de la Información presento al Parlamento Canadiense, un reporte especial en respuesta a dicha nueva propuesta de acta y un documento a discusión sobre lo que el considera debe ser una verdadera y profunda reforma al Acta de Acceso a la Información, que entre otras cosas, amplía los sujetos obligados y el alcance de diversas disposiciones, por ejemplo, en materia de documentación de procesos deliberativos. Dicho documento fue entregado al IFAI.

Respecto a la operación diaria de la Comisión, se compartieron experiencias relevantes en temas como apelaciones, costos de acceso, tiempos de respuesta y cumplimiento de las resoluciones. En Canadá, si una agencia gubernamental federal no acata la resolución del Comisionado y el ciudadano no acude a la Corte por sí mismo, la Comisión, previo acuerdo con el ciudadano, presenta una demanda ante los tribunales y cubre todas las costas.

Se hizo énfasis en la importancia que reviste el hecho de que la Comisión emita resoluciones consistentes, por lo que se sugiere resolver con estricto apego a lo que la Ley establece. También se habló de la importancia del área de investigaciones, misma que es neurálgica ya que es en ésta área donde se resuelven la mayoría de los casos, junto con la de Auditoria General. El Comisionado de la Información solo interviene en casos de difícil resolución o donde no existe claridad o criterios específicos para resolver. Comentaron que en el área de investigaciones se recluta personal con alta integridad que es sometido a exámenes especializados de confiabilidad (clearence), a efecto de demostrar su idoneidad para el cargo y con una educación sólida.

En materia de su relación con la Comisión de Privacidad y la manera en que resuelven casos que involucran tanto al Acta de Acceso a la Información, como al Acta de Privacidad, el Comisionado Reid mencionó que la Corte en Canadá ha dicho que ambas leyes son una sola pieza, por lo que actúan de manera coordinada con la Comisión de Privacidad para conocer los precedentes y criterios de dicha institución.[9]

[9] La Suprema Corte en recientes resoluciones –por ejemplo en el caso de Joan Van Den Bergh v. Nacional Research Council Canada- el Juez O'Reilly dijo: "El Acta de Acceso a la Información y el Acta de

Respecto a casos de tensión entre acceso a la información y protección de privacidad, por ejemplo, cuando se abordan cuestiones sobre acceso a información personal de servidores públicos, el Comisionado mencionó que además de atender las disposiciones legales aplicables que señalan la publicidad de aquella información relacionada con la función pública, los Tribunales Canadienses han clarificado la cuestión, a través de una resolución a un asunto de la Policía Montada.[10]

Sobre la aplicación diferenciada de una prueba de daño con los elementos presente, probable y específico, el Comisionado señaló que cuando se trata de excepciones discrecionales en su ley (Discretionary Exemptions), se aplica la prueba con los tres elementos, y en el caso de aquellas excepciones obligatorias (Mandatory Exemptions), no aplican la prueba. Lo anterior, correspondería en nuestra ley a aplicar la prueba en los casos de la fracción 13 y no en aquellos de la 14.

Finalmente, es relevante mencionar que el Acta de Acceso a la Información Canadiense, contiene una prueba de interés público en su apartado 20 (6). A través de dicha prueba, se puede dar acceso a información confidencial de los particulares (financiera, comercial, científica o técnica, secreto industrial u otra), de modo que es posible la apertura de dicha información aún sin el consentimiento de los titulares de la misma, si se dan dos condiciones:

1. Si existe un interés público relacionado con salud pública, seguridad pública, o protección del medio ambiente, y
2. Si el interés público en la apertura claramente es mayor en importancia, que la pérdida financiera o ganancia no recibida por los particulares, su pérdida de competitividad o interferencia con otras negociaciones frente a terceros.

Conclusiones:

Privacidad son dos caras de una misma moneda. Juntas establecen las reglas que gobiernan la apertura y la protección de la información que posee el Gobierno. Ambos son estatutos de igual importancia y, cuando se apliquen, los jueves las debe leer de manera conjunta. Tal y como lo estableció el Juez Gonthier, estos estatutos contienen un código uniforme con provisiones complementarias que pueden y deben interpretarse de manera armónica."

[10] Caso RCMP. http://www.lexum.umontreal.ca/csc-scc/cgi-bin/disp.pl/en/pub/2003/vol1/html/2003scr1_0066.html?query=repertorie(information%20commissioner)%20AND%20dates(2003)&langue=en&selection=&database=en/jug&method=all&retour=/csc-scc/cgi-bin/srch.pl?method=all~~rep

La participación del IFAI en esta capacitación resultó relevante, dado que se conoció de cerca el funcionamiento de una institución con años de experiencia en materia de protección de datos personales y derecho a la privacidad. Aunado a lo anterior, se resolvieron dudas concretas a efecto de poder aprovechar al máximo los criterios aplicados en dicho país, en las resoluciones y regulación que se expida.
Finalmente, la interacción con dependencias de la APF, resultaba necesaria para encontrar puntos de contacto y comunicación con los propios sujetos obligados, en un tema en el cual el IFAI es la autoridad, de modo que se pueda valorar y dimensionar el tema y la labor institucional. En el mismo sentido y compartiendo experiencias, se pudo entablar una mejor relación con las instituciones espejo al IFAI en las Entidades Federativas y otros actores.

Actualmente se cuenta con una estrecha relación y un canal expedito de comunicación tanto con la OPC como con la Oficina de Acceso a la Información, para darle continuidad y contenido a temas como el tratamiento de datos de salud, las medidas de seguridad para sistemas de datos personales y el seguimiento a las resoluciones y criterios jurisprudenciales en temas de tensión y alcance de derechos, tanto de acceso a la información, como de privacidad.