REPORTE DE PARTICIPACIÓN EN PASANTÍA INTERNACIONAL

NOMBRE DE LA ACTIVIDAD	Pasantía en la Comisión Federal de Comercio (en inglés: *Federal Trade Commission),* en adelante FTC.
LUGAR Y FECHA DE LA PASANTÍA	Washington D.C. Desde el 4 al 6 de febrero de 2020, en la Comisión Federal de Comercio. Adicionalmente, se realizaron reuniones con otras instituciones públicas y privadas, el día 3 y 7 de febrero de 2020.
OBJETIVO GENERAL DE LA PASANTÍA PARA LA INSTITUCIÓN	El objetivo general del viaje era conocer directamente el trabajo en materia de privacidad que realiza la FTC. Exponerse a buenas prácticas, entender sus desafíos y las complejidades propias de su rol. Junto a las autoridades de la FTC, la visita aprovechó de agendar reuniones con autoridades de otros organismos públicos de Estados Unidos y organizaciones privadas que aportaran en materia de protección de los datos personales. En particular, el objetivo en la FTC era conocer la manera en que esta institución hace cumplir las regulaciones sobre privacidad y protección de datos, cómo desarrolla e implementa las políticas públicas sobre dichas materias, cómo entiende los estándares de seguridad de datos que los encargados de datos deben seguir, entre otros asuntos.

DESCRIPCIÓN DE LA PASANTÍA
(PROGRAMA DE ACTIVIDADES, AGENDA PARALELA, REUNIONES BILATERALES REALIZADAS)

Programa de actividades ejecutado:

Lunes 3 de febrero			
Horario	**Actividad**	**Representantes de la Institución**	**Tema**
11:30 – 12:30	**1. Reunión en Microsoft**	1. Laura Gardner, Directora de Política de Privacidad de Microsoft (vía remota); 2. Alex Pessó, Director Legal y de Asuntos Corporativos de Microsoft Chile (vía remota); 3. Sebastián Palacios, Abogado en Asuntos de Transformación Digital en Microsoft (vía remota); y 4. Daniel Korn, Director de Asuntos Corporativos de Microsoft Latinoamérica.	El enfoque de Microsoft frente al Reglamento General de Protección de Datos de la Unión Europea (GDPR) y los principios sobre privacidad de Microsoft.
14:00 – 16:00	**2. Reunión en el Departamento de Estado *(Department of State)***	Equipo de Programa de gestión de los registros e información del Departamento de Estado: 1. Federico Klein 2. Mary Suzanne Archuleta Jeannie Miller	Programa de gestión de los registros e información del Departamento de Estado.
17:00 – 18:00	**3. Reunión en el Archivo Nacional de Seguridad *(National Security Archive)***	1. Peter Kornbluh , Director de Chile del Archivo Nacional de Seguridad 2. Carlos Osorio, Director de Proyectos	Uso del acceso a la información y privacidad de los datos para dar a conocer hechos históricos que han sido reservados y posteriormente desclasificados.

Martes 4 de febrero			
4. Programa de Pasantía en la Comisión Federal de Comercio (*Federal Trade Commission -FTC*)			
10:30 – 11:15	**4.1. Privacidad y seguridad de datos: el marco legislativo y estructura institucional**	1. Hugh Stevenson/ Director Adjunto/ Protección Internacional al Consumidor / Oficina de Asuntos Internacionales; 2. Michael Panzera/ Asesor en Protección Internacional al Consumidor/ Oficina de Asuntos Internacionales; y 3. Andrea Arias/ Abogada/ División de Protección a la Privacidad e Identidad.	Seguridad y privacidad de los datos: el marco legislativo/ Estructura institucional.
11:15 – 12:30	**4.2. Privacidad y seguridad de datos: aplicación de la ley y sanciones**	Andrea Arias/Abogada/División de Protección a la Privacidad e Identidad	Seguridad y privacidad de los datos: cumplimiento y sanciones
1:45 – 3:00	**4.3. Seguridad y privacidad de los datos: herramientas y técnicas de investigación**	Phillip Miyo / División Tecnología y Análisis para Litigios	Seguridad y privacidad de los datos: herramientas y técnicas de investigación.
3:15 – 4:00	**4.4. Educación en privacidad para consumidores y empresas**	Lesley Fair / Abogada Senior / Oficina de Protección al Consumidor.	Educación para consumidores y empresas sobre cuestiones de privacidad / seguridad.
Miércoles 5 de febrero			
10:15 – 11:00	**4.5. Mecanismos de Transferencia Transfronteriza de Datos**	Peder Magee/ Abogado/ División de Protección a la Privacidad e Identidad.	Mecanismos de transferencia de datos transfronterizos.
11:00 – 11:45	**4.6. Ley de protección de datos infantil en internet (*Children's online privacy protection act*- COPPA)**	1. Alison Lefrak/ Asesora en Protección Internacional al Consumidor/ Oficina de Asuntos Internacionales; y 2. Peder Magee/ Abogado/ División de Protección a la Privacidad e Identidad.	Reglas especiales: privacidad de los niños.
11:45 – 12:30	**4.7. Ley WEB SEGURA *(Safe Web Act):* Cooperación internacional e intercambio de información**	Hugh Stevenson/ Director Adjunto/ Protección Internacional al Consumidor / Oficina de Asuntos Internacionales.	Ley sobre seguridad en la Web: Cooperación internacional e intercambio de información.
14:00 – 15:00	**4.8. Reunión Comisionado Noah Joshua Phillips**	Comisionado Noah Joshua Phillips.	Protección de datos personales
Jueves 6 de febrero			
10:30 – 11:30	**4.9. Dispositivos conectados y Big Data**	Andrea Arias/Abogada / División de Protección a la Privacidad e Identidad	Seguridad de datos y privacidad: Internet de las cosas y Big Data.
11:30 – 12:30	**4.10.Inteligencia Artificial (IA)**	Ellen Connelly/ Abogada/ División de Protección a la Privacidad e Identidad.	Inteligencia Artificial
2:00 – 3:30	**4.11. *FinTech* y datos financieros**	1. Deon Woods-Bell/ Oficina de Asuntos Internacionales; Christopher Leach/ División de Prácticas Financieras.	FinTech y datos financieros
3:30 – 4:15	**4.12. Seguimiento de Dispositivos cruzados *(Cross-Device Tracking)***	Megan Cox / División de Protección a la Privacidad e Identidad.	Dispositivos de localización

Viernes 7 de febrero			
09:30 – 11:00	**5. Reunión en el Departamento de Seguridad Nacional *(Department of Homeland Security- DHS)***	Amy Bennett, Acting Director, FOIA Policy, Compliance and Training DHS Privacy Office	Política de privacidad en el Departamento de Seguridad Nacional
		Shannon Ballard/ Directora de Programas Internacionales de Privacidad/ Oficina de Privacidad.	Implementación de la Ley sobre libertad de información (FOIA) en el Departamento de Seguridad Nacional
12:30 – 14:00	**6. Reunión en Facebook**	1. Laura Juanes, Directora Global de Política de Privacidad; 2. Melinda Claybaugh/ Directora de Política de Privacidad en Washington D.C.	La política de privacidad de Facebook.

PONENCIAS/PRESENTACIONES EFECTUADAS

1. Reunión en Microsoft

El enfoque dado por la empresa Microsoft en materia de protección de datos personales considera la legislación de distintos países, incluido el Reglamento General de Protección de Datos de la Unión Europea (conocido por su sigla en inglés, GDPR) y los estándares de certificación.

Microsoft considera importante enfocarse en tres temas:

- Realizar inversiones de ingeniería para empoderar a los consumidores, lograr el cumplimiento y ayudar a los clientes de Microsoft a lograr el cumplimiento.
- Evaluación de riesgos en tiempo real.
- A través de una plataforma de administración del cumplimiento, Microsoft permitiría a las empresas administrar sus políticas de cumplimiento de manera centralizada.

Recomiendan cuatro pasos para la implementación del GDPR:

1. Descubrir: Identificar los datos personales que se tienen y conocer donde residen.
2. Administrar: Regular como se acceden y como son usados los datos personales.
3. Proteger: Establecer controles de seguridad que permitan prevenir, detectar y responder a brechas de vulnerabilidades y de datos.
4. Reportar: Mantener un estado actualizado, documentado, administrar adecuadamente las notificaciones de brecha de seguridad y solicitudes de datos.

Adicionalmente, entrega las siguientes recomendaciones:

- Simplificar todo el proceso a través del gobierno de datos, configurando o asignando etiquetas a los datos sensibles.
- Uso de herramientas inteligentes para descubrir y controlar los datos.
- Implementar controles de conformidad, clasificando los datos. Distinguir entre datos del cliente que son confidenciales y/o que contienen datos personales

Los principios de privacidad de Microsoft son:

- Beneficio al usuario: Cuando recopilan datos, los utilizan para beneficiar y mejorar las experiencias del usuario.
- Control: respecto de su privacidad.
- Transparencia: Entregarán información respecto a lo que se hace con los datos en un lenguaje claro y claro.
- Seguridad: Implementarán fuertes medidas de seguridad para proteger los datos.

- Protección Legal: Respetarán las leyes de privacidad de cada país/región y fomentarán la protección legal de su privacidad como un derecho humano fundamental.
- No realizar orientación por contenido: No utilizarán el correo electrónico, chat, archivos u otro contenido personal para enviar anuncios.

Para ello, existen tres principios claves que garantizan:

Seguridad: Todos los datos respecto del cual realizan tratamiento están seguros.

- Invierten sobre 1 billón de dólares al año en CiberSeguridad
- Tienen más de 3500 profesionales de seguridad que trabajan para asegurar que sus *datacenter* no sufran de ataques.
- Bloquean más de 5 mil millones de ataques de distintos *malware* por mes.

Transparencia: En la recopilación y los usos de los datos.

- Proporcionan las ubicaciones geográficas dónde se almacenan los datos del cliente.
- Publican la cantidad de demandas legales de datos de clientes que reciben de las agencias de aplicación de la ley.
- Brindan visibilidad de lo que hacen con los datos del cliente, cómo lo protegen y cómo tienen el control.

Conformidad: Se gestionan los datos de sus clientes de acuerdo con la legislación vigente en el país donde provean los servicios.

- Tienen la cobertura de cumplimiento más completa de la industria.
- Se comprometen a compartir sus experiencias en el cumplimiento de regulaciones complejas.
- Ponen a disposición varios recursos para ayudar a nuestros clientes en su viaje de cumplimiento.

La empresa brinda herramientas para la gestión de riesgo, manejo de casos y demostrar cumplimiento.

Existen aspectos del GDPR que para Microsoft han sido difíciles de implementar:

- Lo más esencial para las empresas es realizar un correcto "Mapeo de los datos" (*Data Mapping).* Generalmente, las empresas no entienden, desconocen los datos que se encuentran recopilando, o a qué categorías o elementos de estos datos tienen accesos. Es fundamental realizar el mapeo de los datos e identificar su trazabilidad *(mapping and tracking data*) suele ser una labor difícil para las empresas. Esta labor es incluso más relevante que registrar bases de datos, por cuanto el principal problema es saber qué la empresa recopila ese dato, más que documentar lo que tiene.
- Se deben identificar procesos en los cuales se recopila, identifican y clasifican datos. Ejemplo: procesos de clasificación de datos; proceso de uso correcto de autorización. Es un desafío para las empresas entender en etapas primarias la necesidad de recopilar datos y qué requisitos deben tener estos datos, no sólo para su trabajo, sino que también pensando en temáticas como la ciberseguridad. Esto ultima es una exigencia mayor para las PYMES en las cuales el impacto de implementar el DGPR es mayor. Microsoft elaboró una herramienta denominada "*Compliance Manager"* que permite cumplir la normativa.

2. Reunión con el Programa de Gestión de los Registros e Información del Departamento de Estado

El Departamento de Estado mantiene registros relacionados con:

- La formulación y ejecución de la política exterior de EE.UU.
- La administración y las operaciones del Departamento de Estado y las Misiones de EE.UU. en el extranjero
- Solicitudes de ciudadanos estadounidenses para pasaportes estadounidenses.
- Solicitudes de visa de no ciudadanos para ingresar a los EE.UU.
- Asistencia consular a ciudadanos estadounidenses en el extranjero.
- Empleados actuales y anteriores del Departamento de Estado.

Las etapas en el ciclo de vida de los registros del Departamento de Estado:

- Se crea un registro para documentar la organización, funciones, decisiones, procedimientos, operaciones u otras actividades del Departamento.
- El registro es revisado por la Administración Nacional de Archivos y Registros (NARA por sus siglas en inglés) para determinar su valor y, por lo tanto, su disposición final, temporal o permanente.
- Los registros temporales son registros tasados y aprobados para su eliminación después de un período de tiempo específico de acuerdo con un cronograma de eliminación de registros aprobado por NARA.
- Los registros que NARA determina que tienen un valor permanente se revisan para desclasificarlos cuando alcanzan los 25 años de edad (revisión sistemática) y se transfieren a los Archivos Nacionales.
- Después de 25 años, un registro puede permanecer sin divulgación. Las preocupaciones que influyen en esta decisión incluyen la seguridad nacional, las prohibiciones legales y la privacidad personal. Si bien un registro puede retenerse por más de 25 años, la decisión de retener está sujeta a una nueva revisión previa solicitud.
- Una vez que los registros del Departamento de Estado se han ingresado a los Archivos Nacionales, ya no están bajo el control legal del Departamento de Estado.

El marco legal relevante que regula el manejo de archivos, según los expositores del Departamento de Estado, es:

a) La Orden Ejecutiva N° 13.526, de diciembre de 2009, titulada “Información clasificada de seguridad nacional”.

   Esta norma establece que la información puede ser clasificada en los siguientes 3 niveles: "altamente secreta", "secreta" o "confidencial", dependiendo si la divulgación no autorizada de la misma razonablemente podría causar daños “extremadamente graves”, “graves” o sin gravedad, respectivamente, a la seguridad nacional que la autoridad de clasificación original puede identificar o describir.

   Adicionalmente, para ser clasificada en alguno de esos niveles la información debe pertenecer a uno o más de los siguientes asuntos:

   i. planes militares, sistemas de armas u operaciones;
   ii. información del gobierno extranjero;
   iii. actividades de inteligencia (incluidas acciones encubiertas), fuentes o métodos de inteligencia, o criptología;
   iv. relaciones exteriores o actividades extranjeras de los Estados Unidos, incluidas fuentes confidenciales;
   v. asuntos científicos, tecnológicos o económicos relacionados con la seguridad nacional;

vi. Programas del Gobierno de los Estados Unidos para salvaguardar materiales o instalaciones nucleares;
vii. vulnerabilidades o capacidades de sistemas, instalaciones, infraestructuras, proyectos, planes o servicios de protección relacionados con la seguridad nacional; o
viii. el desarrollo, producción o uso de armas de destrucción masiva.

Esta regulación estableció el "*Mandatory Declassification Review*", que permite a cualquier persona solicitar la "revisión de desclasificación" de un documento clasificado con el fin de obtener la versión liberada de dicha información.

Igualmente, esta normativa establece la *"Automatic Declassification*", donde aquella información que tiene valor histórico permanente se desclasifica automáticamente una vez que alcanza los 25 años archivada, a menos que el jefe de una agencia haya determinado que se encuentra dentro de una exención limitada que permite la clasificación continua y ha sido aprobada adecuadamente. Esto se realiza a través de un procedimiento no automatizado. Pueden ser archivos físicos (papel) o electrónicos.

b) La Orden Ejecutiva N° 13556, titulada: "información no clasificada controlada" (*Controlled Unclassified Information-CUI),* dictada en noviembre de 2010.

Esta Orden establece un programa para administrar la información sensible no clasificada bajo la Orden Ejecutiva N° 13.526 y otras normas, en el Poder Ejecutivo. Las categorías y subcategorías fijadas bajo esta Orden pretenden servir como designaciones exclusivas para identificar información no clasificada que requiera controles de protección o difusión. Algunas de dichas categorías son: infraestructura crítica, acuerdos internacionales, recursos naturales, privacidad, etc.

Internamente, el Departamento de Estado ha fijado "Programas de disposición de registros" que documentan las principales series de registros (incluidos los registros electrónicos) relacionados con las actividades de cada oficina, identifica los registros temporales y permanentes, y proporciona instrucciones obligatorias para la retención y disposición (retiro o destrucción) de cada serie de registros en función de su carácter temporal o permanente. Todos los programas de disposición de registros deben estar aprobados por el NARA.

Para el Departamento de Estado ha sido especialmente importante el "Programa General de Registros 6.1: Correo electrónico administrado bajo un enfoque *Capstone*", emitido por el NARA (*National Archives o Archivos Nacionales y Administración de Documentos)*, que orienta a las agencias federales sobre el manejo y disposición de sus correos electrónicos, según la jerarquía o posición del funcionario que interviene en la comunicación, obligando a no borrarlos y a enviarlos al NARA en cierto plazo.

Por último, señalan que han aprendido que es necesario aplicar desde el inicio de la cadena de vida de un registro, la clasificación del mismo, determinando su nivel de sensibilidad, ya que hacerlo después es muy difícil. Para ello se obliga a clasificar el mensaje, impidiendo su envío, si no ha sido etiquetado.

Los expositores destacan que es importante crear una cultura institucional donde los funcionarios entiendan que la información que manejan no es propia, sino que pertenece al Estado. Por ejemplo, los mensajes de WhatsApp referidos a asuntos labores deben ser reenviados a los correos electrónicos para su posterior archivo y disposición.

3. Reunión en el Archivo Nacional de Seguridad (*National Security Archive)*

Este equipo ha colaborado con la Comisión Interamericana de Derechos Humanos y el Archivo del Terror en Guatemala. Han participado en la discusión de la privacidad y el enfoque de apertura de información para esclarecer estados de excepción en periodos de dictaduras militares. En este aspecto, la privacidad aparece en dos sentidos: privacidad de víctimas y privacidad de perpetradores.

Su objetivo es esclarecer episodios históricos que tienen impacto hasta el día de hoy. Se han acercado a temas importantes como: bitácoras de entrada y salidas de la Casa Blanca. Destacan también, la existencia de deudas históricas de transparencia como la decisión de Estados Unidos de invadir Irak y Kuwait.

Algunos aspectos interesantes referidos a la privacidad de las personas:

- La privacidad en Estados Unidos se extingue con el fallecimiento de la persona.
- La reserva de la información es por 25 años, luego de este período los documentos se desclasifican por rutina y no por requerimiento de las personas (*Sunset clause Executive Orden 13526).*

Sin embargo, se menciona la decisión del Buró Federal de Investigaciones (FBI) de revelar sus fuentes cuando sus agentes han fallecido. Esta decisión fue una decisión voluntaria y de corte político, ya que por otro lado, quedó a criterio de la Agencia Central de Inteligencia (CIA) proteger sus fuentes.

4. Programa de Pasantía en la Comisión Federal de Comercio (FTC)

4.1. Privacidad y seguridad de datos: el marco legislativo y estructura institucional

a) Privacidad y Seguridad de Datos en los Estados Unidos

En Estados Unidos no existe ninguna ley federal integral que regule de forma comprensiva la privacidad ni la seguridad de los datos. En cambio, cuentan con un mosaico de leyes federales promulgadas en diferentes momentos que regulan ciertas industrias y tipos de datos, por ejemplo:

- Ley sobre privacidad de los conductores
- Ley sobre no discriminación en información genética
- Ley sobre privacidad en las comunicaciones electrónicas
- Ley sobre informes de crédito justos o imparciales
- Ley de prevención de abuso en ventas telefónicas y fraude al consumidor.
- Ley de protección de la privacidad infantil en internet

b) Antecedentes de la FTC

La Comisión Federal de Comercio (FTC, por sus siglas en inglés) es una agencia federal independiente, que posee un doble mandato: proteger a los consumidores y fomentar la competencia.

Su misión es prevenir las prácticas comerciales anticompetitivas, engañosas o desleales_hacia los consumidores; mejorar el nivel de información de las opciones disponibles para los consumidores y aumentar el grado de comprensión del proceso competitivo por parte del público; y cumplir con estos objetivos sin imponer una carga indebida sobre la actividad comercial legítima.

La privacidad y la seguridad de los datos se consideran dentro de la protección del consumidor. Se efectúa a través de: perseguir el cumplimiento de la ley, iniciativas de política y educación al consumidor y concientización al sector comercial.

c) Marco legal y competencias de la FTC

- La ley orgánica de la FTC establece que “Las conductas o prácticas injustas o engañosas en el comercio (o que afectan este) se declaran ilegales" (Sección 5 (15 U.S.C. §45). Entonces, las acciones pueden ser “desleales” o “engañosas”.

- Para la ley de FTC, la “deslealtad” es una conducta o práctica que causa (o es probable que cause) un daño sustancial a los consumidores que éstos no pueden evitar razonablemente y que no genera beneficios compensatorios para los consumidores o la competencia.

- Por su parte, en la misma ley, el” engaño” es una representación, omisión o práctica sustancial que pueda inducir a error al consumidor que actúa razonablemente bajo las circunstancias.

- En este sentido, la FTC vigila que las empresas cumplan las promesas que efectúan a los consumidores y que cuenten con procedimientos razonables para protegerlos.

- *Safeguards Rule (implements Gramm-Leach-Bliley Act):* Las "instituciones financieras" (excluyendo a los bancos) deben garantizar la seguridad y confidencialidad de la información del cliente. Los obliga a establecer procesos de almacenamiento de la información, designar un empleado

responsable, identificar riesgos, evaluar la efectividad de los procesos, a través de una empresa externa de tecnología, entre otros asuntos. Además, los consumidores tienen derecho a consultar por su información y verificar que sea correcta.

- *Fair Credit Reporting Act (FCRA)* Requiere manejo particular e informes específicos cuando se usan datos para ciertos fines (p. ej., crédito o contratación).

- *Red Flags Rule*: Las instituciones financieras deben implementar un programa para detectar "señales de alarma" de robo de identidad.

- *Children's Online Privacy Protection Act (COPPA*): Requiere seguridad razonable para la información recopilada de niños en línea. Se consideran niños, los menores de 13 años. Requiere el permiso de los padres para el tratamiento de los datos de menores.

d) Transferencia de datos con la Unión Europea

"*Privacy Shield Framework"* establece un método para permitir que las empresas transfieran datos personales a los Estados Unidos desde la Unión Europea (U.E.) de manera coherente con la legislación de la UE.

Para unirse al "Marco de Protección de Privacidad", una empresa debe certificar ante el Departamento de Comercio, que cumple con los Principios de Protección de Privacidad.
El incumplimiento por parte de una empresa de los principios es sancionable en virtud de la Sección 5 de la Ley FTC que prohíbe las conductas desleales y engañosas.

e) Mirada a nivel estatal

Existen sólo tres Estados que cuentan con una regulación específica sobre protección de datos personales, a saber: California, Nevada y Maine. Resulta especialmente importante la ley del primero de ellos, denominada "*California Consumer Privacy Act" (CCPA*), la cual fijó nuevos derechos del consumidor:

- El derecho a saber si su información personal se recopila.
- El derecho a solicitar las categorías específicas de información que una empresa recopila al presentar una solicitud verificable.
- El derecho a saber qué clase de información personal se recopila sobre ellos.
- El derecho a oponer la venta de información personal.
- El derecho a eliminar su información personal.
- El derecho al servicio y precio igualitario, incluso si ejercen sus derechos de privacidad.

Por otra parte, sólo nueve Estados poseen leyes de notificación de fallos de seguridad en los datos, estos son: Washington D.C., Maryland, Delaware, New Jersey, Connecticut, Rhode Island, Massachusetts, New Hampshire y Vermont.

4.2. Privacidad y seguridad de datos: aplicación de la ley y sanciones

La FTC realiza investigaciones para determinar la existencia de conductas "desleales" y/o "engañosas", que se relacionen con la privacidad y seguridad de los datos. Estas investigaciones pueden surgir a partir de denuncias de particulares, o bien, de oficio por la FTC, según criterios de priorización institucional.

Por lo general, no se divulga la existencia o inexistencia de investigaciones. Se inician de manera secreta. Luego, la información recabada durante una investigación también tendrá el carácter de confidencial, para proteger de futuros ataques o brechas de seguridad a las empresas.

Dentro de las investigaciones, la FTC emite las "*Civil Investigative Demands" (CIDs*) o "citaciones civiles" que consisten en solicitudes de información de tipo interrogatorio, solicitudes de producción de documentos o solicitudes de testimonio para las empresas investigadas. Para esto, revisan las "promesas" efectuadas por las compañías a sus clientes, sus políticas de privacidad, la descarga de aplicaciones asociadas, etc. Piden copia del examen forense que la propia empresa haya contratado.

En lugar de enviar una CID, la FTC puede enviar una carta a la empresa preguntando por una situación particular. Esta comunicación no es obligatoria de ser respondida, pero la mayoría responde. Muchos casos terminan con esta respuesta, al no detectarse ninguna infracción.

En el marco de las CID, FTC cuenta con 30 a 45 días para llegar a un acuerdo con la compañía, que evitará el juicio ante la Corte. Con todo, si llegan a acuerdo, éste debe ser aprobado por la Corte respectiva.

a) Aplicación en el contexto de seguridad de datos, cuatro principios claves:

i. La seguridad de los datos se considera un proceso continuo, y por lo tanto las investigaciones de la FTC se enfocan en el proceso.
ii. Las prácticas de seguridad de una empresa deben ser razonables y apropiadas a la luz de las circunstancias.
iii. Una filtración de datos no indica necesariamente que una empresa no haya utilizado medidas de seguridad razonables, dado que no existe la seguridad perfecta.
iv. Puede que las prácticas de seguridad no sean razonables, y como consecuencia, estar sujetas a la aplicación de la Ley FTC, aunque no se haya experimentado ninguna filtración.

b) Recursos típicos:

i. Generalmente, las órdenes de la FTC tienen una duración de 20 años.
ii. Prohibición de tergiversaciones en el futuro.
iii. Programa integral de privacidad y/o seguridad de datos.
iv. Evaluaciones bienales llevadas a cabo por terceros.
v. Otros requisitos específicos, como: divulgaciones o actualizaciones de software.
vi. Sanciones civiles por infracciones de normas y órdenes de la FTC.

c) Casos de seguridad de información:

UBER. Prácticas engañosas (en contravención de Sección 5):

- Se afirmó que la empresa había monitoreado atentamente el acceso interno a los datos personales de los consumidores y que se había sometido a auditoría efectuada por especialistas en seguridad de datos de forma continua.
- Se afirmó que se proporciona una seguridad razonable para los datos personales de los consumidores almacenada en sus bases de datos.
- Como consecuencia:
  - ✓ Bajo la orden, se debe implementar un programa integral de seguridad de datos y de privacidad durante 20 años con auditorías bienales.
  - ✓ Se debe someter a la FTC informes de incidentes pertinentes.

d) Casos de privacidad:

FACEBOOK

- El año 2012, la FTC detectó 8 violaciones a la privacidad de los clientes de Facebook. A raíz de ello, se emitió la orden que prohibía a esa empresa realizar conductas engañosas en relación con la privacidad, seguridad de la información y compartir información con terceros. Además, obligó a la compañía a generar un programa de protección de la privacidad.
- Sin embargo, en 2019, repitió infracciones y cometió otras nuevas. Específicamente, tuvo las siguientes conductas:
  - ✓ FB informó a los usuarios que se podía limitar el intercambio de datos a ciertos grupos (p.ej., amigos), pero en realidad se compartió la información con los desarrolladores de aplicaciones.
  - ✓ No se evaluó ni abordó adecuadamente los riesgos de privacidad planteados por terceros (desarrolladores de aplicaciones).
  - ✓ Tergiversó que los usuarios tendrían que "activar" la tecnología de reconocimiento facial, pero en realidad, para muchos usuarios, era ya una configuración predeterminada.
  - ✓ Vulneró la Ley FTC cuando afirmó que recopilaría números de teléfono sólo por motivos de seguridad, pero en realidad reveló los números por motivos de publicidad.
- Como consecuencia, la empresa fue se sometió a una multa de $US 5 mil millones y se acordaron nuevos requisitos de privacidad:
  - ✓ Mayor supervisión de los desarrolladores de aplicaciones de terceros (p.ej., terminar aquellos que no certifiquen el cumplimiento de las políticas de la plataforma)
  - ✓ Consentimiento para usar / compartir información de reconocimiento facial de manera que exceda las divulgaciones anteriores.
- Para fijar los montos de las multas se considera el número de personas afectadas, las utilidades de la empresa involucrada y otros criterios a discreción de la FTC.

Se destacó la siguiente publicación de la FTC: "*Start with security*: Mejores prácticas", con las siguientes recomendaciones:

- Integrar la seguridad desde el inicio
- Controlar el acceso a los datos de manera razonable
- Requerir contraseñas seguras y autenticación
- Almacenar información personal confidencial de forma segura y protegerla durante la transmisión
- Segmentar la red y monitorear quién está tratando de acceder y salir
- Asegurar el acceso remoto a la red
- Aplicar buenas prácticas de seguridad al desarrollar nuevos productos
- Asegurarse de que los proveedores implementen medidas de seguridad razonables
- Establecer procedimientos para mantener actualizada su seguridad y abordar las vulnerabilidades que puedan surgir
- Asegurar los documentos, los medios físicos y los dispositivos

Para mayor información, link de acceso al informe "*Start with security*" elaborado por la FTC.

4.3. Seguridad y privacidad de los datos: herramientas y técnicas de investigación

El Laboratorio Tecnológico *(Tech Lab)*, están bajo la División de Litigación Tecnológica y Análisis (*Division of Litigation Technology and Analysis* (DLTA)) del *Bureau of Consumer Protection* (BCP). Tienen un equipo de 6 personas que son responsables del laboratorio y entre sus usuarios se encuentra el equipo de 8 investigadores *(data scientists).*

El objetivo del laboratorio es tener un entorno de tecnología de la información (TI) que simule a la experiencia de los consumidores en línea, interactuando con la tecnología, y que permita al personal de la FTC, realizar investigaciones y estudios.

Tienen diferentes usuarios del laboratorio, abogados, tecnólogos, paralegales, investigadores, becarios, economistas, estudiantes de pasantías de secundaria, universidad y facultades de derecho, oficiales administrativos.

Tienen definidas las reglas de conducta para utilizar el laboratorio de parte del personal:

- Los recursos del laboratorio son para uso oficial.
- Todos los usuarios del laboratorio deben firmar anualmente las "Reglas de Conducta" para obtener acceso a los recursos del laboratorio.
- Tienen un procedimiento para realizar préstamos de instrumentos de investigación a usuarios y que puedan utilizarlos fuera de la oficina.

Respecto al entorno informático:

- El entorno informático ha sido diseñado y estructurado para tratar con complejidades de investigaciones, con el fin de soportar diversas investigaciones y estudios.
- Todos los usuarios del laboratorio tienen una amplia experiencia en informática y poseen conocimiento especializado en sus respectivas áreas tecnológicas.

Respecto al personal del laboratorio y conocimientos:

- Para algunos temas específicos, buscan experiencia y conocimientos en expertos y/o especialistas externos.
- El diseño e implementación del laboratorio fue liderado por profesional que había diseñado el *DataCenter* de la FTC, siendo su área de especialización la infraestructura tecnológica y *networking.*
- El equipo del laboratorio se entrena respecto de la actualización de tecnologías y conocimientos. Se especializa una persona, quien transfiere el resto del conocimiento a los demás integrantes del equipo.
- Respecto a la renta del equipo del laboratorio, tienen una remuneración menor que la del mercado, de acuerdo con su grado de especialización, pero apelan a la retención de talento, pues la FTC es uno de los mejores lugares para trabajar, y los temas son desafiantes y de punta.
- Se encargan de mantener la integridad de la data de las investigaciones.
- El equipo del laboratorio (6 personas), transfieren habilidades y entrenan a los investigadores (soporte de alto nivel), para usar las herramientas en el marco de la investigación. Es decir, ellos no realizan la investigación, sino que transfieren habilidades, participan desde sus conocimientos tecnológicos y proporcionan el soporte para que los investigadores puedan utilizarlas adecuadamente.

Con respecto a sus técnicas de investigación, tienen como objetivo recabar evidencia de prácticas comerciales injustas, engañosas o fraudulentas, para ello:

- Acceden a Internet e interactúan con la tecnología de la misma manera que los consumidores.
- Evitan alertar sobre la investigación.
- Protegen la agencia, tanto de datos maliciosos como de la divulgación de métodos y capacidades de investigación.

Con respecto a sus técnicas de investigación, tienen como objetivo recabar evidencia de prácticas comerciales injustas, engañosas o fraudulentas, para ello:

- Acceden a Internet e interactúan con la tecnología de la misma manera que los consumidores.
- Evitan alertar sobre la investigación.

- Protegen la agencia, tanto de datos maliciosos como de la divulgación de métodos y capacidades de investigación.

4.4. Educación en privacidad para consumidores y empresas

El rol de educación en la FTC es continuo y permanente. Generalmente, los errores, estafas, engaños de parte de las empresas a los consumidores suelen repetirse año a año, independiente de si se trata de una empresa grande o una empresa pequeña.

Asimismo, la persona mal intencionada- el ladrón de información- no roba solamente a empresas grandes, sino que, a cualquier persona, estando toda la población susceptible de recibir una estafa o engaño.

La preocupación de la FTC en el rol de educación y del cumplimiento de las demás labores no es solamente con Microsoft u Oracle, sino que también con los pequeños empresarios y los consumidores individuales.

El equipo está integrado por aproximadamente 20 personas y entre ellos, destacan personas formadas en seguridad de la información, reclamos, anuncios de alimentos; redes sociales. Existen dentro del equipo: escritores, expertos en percepción y cognición del consumidor, abogados; quienes que tratan de traducir la información jurídica exacta al contenido de mensaje que requiere recibir el consumidor. Los mensajes deben ser cortos, concisos y precisos, tanto para empresas como para consumidores.

La información debe estar en un formato factible de compartir y respecto del cual no se vea el logo de la FTC. Desde su experiencia, se ha logrado penetrar mucho más en los consumidores sin necesidad de poner créditos (logo) en la información a difundir (el uso de logos es limitado y cuando se hace, se utiliza un logo pequeño al final de cada material). En este sentido, no importa que la información venga de la FTC, lo que importa es que se conozca y que cualquier otra entidad, pública o privada, pueda reutilizar esa información. Se comenta el ejemplo de la policía de Nueva York, la NYPD, que adaptó los videos de la FTC y esto permitió llegar a 100 millones de personas adicionales.

El sitio web de la FTC cuenta con una versión en español, así como mucho de los materiales de difusión. También cuentan con un canal de *youtube* con información en videos, en inglés y en español.

En la sección: "*Consumer Blog*" es posible encontrar información de artículos y casos. Además, cuenta con blogs de suscriptores orientados al consumidor, el cual logra más de 10 mil suscripciones nuevas por mes. Para suscribirse sólo se pide un correo electrónico. Los artículos del blog son generalmente, casos con los cuales se escribe máximo 5.000 palabras, concentrándose en el mensaje que se quiere dar al consumidor. También cuentan con un blog para empresas, llamado *"Business Blog*" en el cual existen 82 mil empresas, la mayoría de sus suscriptores son abogados.

Se comentan casos exitosos de difusión como lo fueron las campañas:

- "Hang up": mediante gráficas atractivas se hace un llamado a los consumidores a disminuir la recepción de llamadas no deseadas solicitando que colgaran el teléfono. Esto permitió que las empresas de carriles telefónicos tomaran medidas en el tema de llamadas indeseadas.

- Robo de identidad: campaña que invita a personas que fueron víctimas de robo de información a denunciar esta situación ante la FTC. Generalmente, son personas a las que les da vergüenza asumir que sufrieron este tipo de estafa. Se les invita a visitar un sitio y generar cartas para realizar la denuncia ante la FTC.

- Ciberseguridad para PYMES: Otra campaña destacada es la implementación de la ciberseguridad en empresas pequeñas. Esta campaña fue en terreno y ellos priorizaron ir justamente a ciudades pequeñas en la cual consultaron primero que es lo que la FTC podría hacer por ellos. Participaban de estas reuniones pequeños empresas: peluqueros, dueños de negocios y ellos les señalaron que no querían tener que contratar consultores para implementar la ciberseguridad en las empresas, pues no tienen los recursos para eso. Se terminó desarrollando una guía especial para este segmento en materia de ciberseguridad (10 lecciones para empresas, disponible en *ftc.gov/cybersecurity).*

4.5. Mecanismos de transferencia transfronteriza de datos

Respecto de la regulación vigente en materia de mecanismos de transferencia o flujo transfronterizo de datos personales, se destacó en primer término, la importancia de facilitar la transferencia internacional de datos personales, reconociendo los beneficios que esta actividad representa para la economía global y local, los gobiernos, las organizaciones y las personas; manifestando, sin embargo, la relevancia de establecer marcos regulatorios que otorguen efectiva protección a los datos en estas circunstancias, resguardando la privacidad de los titulares de esto, con el objeto de que se mantenga la confianza de las personas en la economía digital.

Así, en lo que respecta a la posición de Estados Unidos frente a esta materia, dicho país interactúa con regulaciones regionales, con la finalidad de facilitar los flujos transfronterizos de datos. De dicho modo, participa en el sistema de las Reglas de Privacidad Transfronteriza (*Cross Border Privacy Rules System o CBPR*, por sus siglas en inglés) del Foro de Cooperación Económica Asia-Pacífico (APEC) y en el acuerdo *Privacy Shield* con la UE.

Las principales características del CBPR, cuyas reglas establecen cómo deben operar las transferencias internacionales de datos entre los países participantes (a la fecha, Estados Unidos, México, Japón, Canadá, Singapur, la República de Corea, Australia y Taipei Chino):

a) Adopción de principios compartidos en el tratamiento de los datos personales;
b) Creación de mecanismos de aplicación donde la transferencia de los datos se realiza entre economías de los países miembros; y
c) Responsabilidad de las organizaciones, que deben poder demostrar que cuentan con ciertas protecciones antes de recibir un permiso general para transferir datos.

Con todo, la participación en el Sistema CBPR se encuentra supeditada a las disposiciones legales -locales - en materia de protección de datos personales. Dicho principio se reconoce explícitamente en el párrafo 44 de las Políticas, Reglas y Directrices de APEC, que estipulan que “la participación en el sistema CBPR no reemplaza las obligaciones legales de una organización participante”.

En particular, se señaló que el objetivo del sistema de protección de datos de APEC consiste en incentivar a las organizaciones responsables del tratamiento de datos, a que desarrollen sus propias reglas de privacidad que regulen el flujo de información personal internacional. Para dichos efectos, se desarrolló un sistema de certificación voluntaria al cual las empresas tratadoras de datos adhieren voluntariamente a un conjunto de reglas de privacidad comúnmente acordadas basadas en el Marco de Privacidad de APEC. En la práctica, señaló que un agente de responsabilidad evalúa a las empresas y otorga la certificación en caso de cumplimiento; solo las organizaciones certificadas pueden mostrar un sello, una marca de confianza o una participación en el CBPR.

En resumen, a través del Sistema CBPR las compañías certificadas y los gobiernos trabajan en conjunto para asegurar que el flujo transfronterizo de datos entre las economías participantes se lleva a efecto bajo un marco de protección, de acuerdo con los estándares prescritos.

El sistema CBPR protege los datos personales, de la siguiente manera:

a) Estándares ejecutables: de forma previa a la incorporación al sistema, se debe demostrar que los requerimientos del CBPR serán ejecutables por la autoridad reguladora correspondiente del país en el que se encuentra.
b) *Accountability*: Para obtener la certificación, una compañía debe demostrar ante un *"Accountability Agent"* (entidad pública o privada independiente) que dan cumplimiento a los requerimientos del CBPR, y que la compañía en cuestión está llevando a cabo sistemas de monitoreo y ejecución.
c) Protección basada en riesgo: las compañías certificadas deben implementar medidas de seguridad que resulten proporcionales a las probabilidades y entidad de las eventuales amenazas de vulneraciones, la naturaleza confidencial, o la calificación de sensible de la información.
d) Reclamaciones por parte de los consumidores ante infracciones: Los *"Accountability Agents*" recibirán, investigarán y resolverán las disputas entre consumidores y compañías certificadas, cuando se alegue el incumplimiento de los requerimientos del CBPR.
e) Empoderamiento de los consumidores: las compañías certificadas deben otorgar a los consumidores el acceso y la corrección de sus datos personales.
f) Coherencia regulatoria: aun cuando los gobiernos podrán imponer requerimientos adicionales a las compañías certificadas en materia de protección de datos personales, las economías participantes acuerdan acatar los 50 requerimientos que contempla el programa CBPR, facilitando su implementación a través de sus regímenes legales locales.
g) Cooperación transfronteriza ejecutable: El Sistema CBPR provee un mecanismo para las autoridades regulatorias en orden a cooperar en la ejecución de los requerimientos del programa.

4.6. Ley de protección de datos infantil en internet (*Children's online privacy protection act- COPPA*)

La ley de protección de datos infantil en internet (*Children's online privacy protection act* o ley COPPA, por sus siglas en inglés) contiene el marco legal de protección de los datos de los menores de edad en su actividad en la red.

La Ley COPPA aplica a los siguientes operadores:

- Operadores de sitios web comerciales y servicios en línea "dirigidos a niños", que recopilan, mantienen u ofrecen la posibilidad de divulgar información de identificación personal (PII, por sus siglas en inglés).
- Operadores de sitios y servicios de "audiencia general" (incluyendo sitios para adolescentes) que tienen conocimiento real de la recopilación de PII de menores de 13 años.

a) Aviso y consentimiento de los padres o responsables:

La regla principal de esta normativa consiste en que los operadores de sitios web comerciales dirigidos a menores de 13 años deben proporcionar un aviso a los padres y obtener su consentimiento, de forma previa a la recopilación de información personal de dichos menores.

b) Aspectos principales de la regulación:

i. Aviso de política de privacidad: se deben publicar enlaces destacados en sus sitios web a un aviso en que se disponga la forma en que se recopila, usa y/o divulga la información de menores de 13 años.
ii. Aviso y consentimiento verificable de los padres: salvo ciertas excepciones, se deberá poner en conocimiento de los padres que el sitio web recopila información de menores de edad,

obteniendo su consentimiento de forma previa a la recopilación, uso y/o divulgación de dicha información, y de modo verificable.

iii. Recopilación limitada: no se debe condicionar la participación de un niño en actividades en línea para recabar información personal adicional a la razonablemente necesaria.

iv. Derecho a la eliminación: se debe permitir a los padres la revisión y /o eliminación de la información de sus hijos de las bases de datos respectivas y prohibir que se recopile más información.

v. Seguridad de los datos: se deben establecer procedimientos para proteger la confidencialidad, seguridad e integridad de la información personal que se recopila.

c) Elementos distintivos de sitios web comerciales cuya audiencia está constituida principalmente por menores de edad:

- Diseño/contenido del sitio.
- Tipo de publicidad en el sitio.
- Composición de la audiencia.
- Público objetivo.
- Utilización de dibujos animados.
- Música y artistas atractivos para los niños y niñas.

d) Algunos elementos interesantes de destacar en la aplicación de esta ley:

- A la fecha, la FTC ha llevado a cabo diversos procedimientos en el marco de la aplicación de la Ley COPPA. Así, por ejemplo, lo hizo con la aplicación *Tik Tok (Musical.ly*), a cuyos operadores sancionaron con la suma de 5.7 millones de dólares, por infracciones a la referida regulación.
- La sanción más alta impuesta a la fecha por la FTC en el marco de esta ley fue en el caso FTC y NY *Attorney General vs. Google y YouTube*, por la suma de 170 millones de dólares.

e) Extraterritorialidad de la Ley COPPA:

- La Ley COPPA rige también respecto de los operadores de sitios web que se encuentren localizados fuera de Estados Unidos, pero cuya audiencia consiste en menores de 13 años en dicho país; y,
- Recopilen a sabiendas información personal de menores de 13 años.

4.7. Ley WEB SEGURA *(Safe Web Act):* Cooperación internacional e intercambio de información

En Estados Unidos existe la Ley web segura (*Safe Web Act*) desde el año 2006, esta legislación entrega a la FTC la facultad de ejercer la Ley ante "actos o prácticas desleales o engañosas", en especial, en el ámbito internacional.

En específico, esta ley otorga una serie de herramientas para mejorar la aplicación de la ley con respecto a los asuntos de protección del consumidor, particularmente aquellos con una dimensión internacional, incluida una mayor cooperación con las autoridades policiales extranjeras a través del intercambio de información confidencial y la prestación de asistencia de investigación. La Ley también permite intercambios de personal y otros esfuerzos de cooperación internacional.

Las atribuciones de la FTC en esta materia son:

- Aplicar la *"FTC Act"* en una amplia gama de contextos, la mayoría de los cuales tiene características transfronterizas (p.ej. Protección y seguridad de datos, robo de identidad, estafas en comercio electrónico, servicios financieros, prácticas engañosas en aplicaciones móviles, etc.).
- Aplicar estatutos sobre sectores o prácticas específicas (ej: telemarketing, spam, protección de la privacidad online de niños).
- Se excluyen actividades de instituciones financieros, seguros y servicio público de telecomunicaciones y de transporte.

Las fronteras se abren cada vez más para todo el mundo en cuanto a comercio electrónico, transferencia de los datos, etc; y también las estafas, pero el límite de jurisdicción de las autoridades que ejecutan la ley se mantenía, , para solucionar esta problemática se creó la Ley *US Safe Web Act* (2006), en la cual la FTC dispone de varios mecanismos para combatir el fraude fronterizo.

a) La Ley *US Safe Web Act*

Bajo la Ley U.S. *Safe Web Act*, la FTC dispone de varios mecanismos para combatir el fraude transfronterizo, el cual se realiza principalmente a través de la colaboración con "Agencias extranjeras de aplicación de la ley" *("Foreign Law Enforcement Agencies"),* es decir, puede generar colaboración con:

- Un organismo administrativo o autoridad judicial de un gobierno extranjero que tengan atribuciones de generar oficios de ejecución de la Ley u de organismos que realicen investigaciones en materia de asuntos civiles, penales o administrativos
- Cualquier organización multinacional, que sea en representación de algún país en materias relacionadas con la misión de la FTC.

La colaboración se brinda un ámbito de aplicación muy amplio que refleja el rango de las agencias con los cuales se colabora habitualmente. Ejemplos: agencias de protección al consumidor, policía, telecomunicaciones.

b) Mecanismos de la ley:

Se implementan dos mecanismos principales:

i. Intercambio de información:

La FTC puede compartir información de manera confidencial con otros organismos de ejecución de la ley en el extranjero. La Ley autoriza el intercambio de información relacionada con la protección de los consumidores obtenida a través de procesos legales obligatorios.

ii) Acuerdo/Certificación:

Se precisa un acuerdo previo u otro certificado por escrito que la agencia solicitante se compromete a:

- Proteger la confidencialidad de la información; y
- Usarla solamente con fines oficiales de ejecución de la Ley.

c) Limitaciones importantes:

- Se permite el uso de la información en conexión con procesos judiciales y administrativos, a condición de que antes de cualquier uso público en tal proceso, se notifique al titular de la información, de modo que pueda tomar medidas cautelares.
- No se permite "*onward sharing,"* es decir, la transferencia a terceros sin aprobación previa.
- Hay requisitos específicos relacionados con el tratamiento de datos personales que se consideran "sensibles".

d) Tipos de asistencia en materia de investigaciones

La FTC puede proporcionar asistencia en forma de recopilación de información/pruebas por medio de sus facultades vigentes de investigación, aún si la FTC no está realizando su propia investigación.

Se le otorga a la FTC la posibilidad de llevar a cabo "*civil discovery*" (obligación de exhibición documental) de parte de las autoridades civiles o de las autoridades penales en aquellos casos remitidos por el Fiscal General.

e) Petición "*Foreign Law Enforcement Agency Request"*

En la petición por asistencia, se precisa afirmar que se efectúa una investigación o un proceso de ejecución en el rubro de infracciones de leyes que prohíben.

- Las prácticas fraudulentas o engañosas;
- Prácticas que son "sustancialmente parecidas" a las que se prohíben por la Ley FTC.

f) Criterios para proveer asistencia entre una agencia y la FTC:

- Se acuerda entre la FTC y la agencia que se proveerá asistencia de forma recíproca.
- En el caso que se esté gestionando una solicitud o petición por parte de la FTC que pueda perjudicar el interés público de los Estados Unidos.
- En caso de que la práctica relacionada a la solicitud, podría generar un perjuicio a un número considerable de consumidores.

La asistencia en materia de investigaciones se trata de información de todo rango: proveedores de servicios de Internet, bancos, empresas de telefonía, etc.

Para proveer esta asistencia, tienen que cumplir con la "Ley de privacidad de comunicaciones electrónicas" ("*Electronic Communications Privacy Act"- ECPA*). La ECPA prohíbe la interceptación no autorizada de llamadas de teléfonos celulares y transmisiones entre ordenadores. La protección se extiende también al acceso no autorizado a comunicaciones electrónicas almacenadas, o su revelación.

El 2015 se lanza "Alertas de la Red de Global de Cumplimiento de Privacidad Alertas" "*GPEN Alerts*" (GPEN es la sigla de la "*Global Privacy Enforcement Network")* , plataforma online para intercambiar información de las investigaciones (prueba de investigaciones) que transfieran las fronteras, de forma segura y confidencial.

La FTC creó, junto a otras siete organizaciones internacionales, la GPEN. En la actualidad, esta red se expandió a 65 organismos miembros y representando a 47 países y 300 usuarios.

Adicionalmente, la FTC, bajo la *"US safe web act"* tiene un programa de intercambio de personal con agencias de protección de datos personales y agencias de protección al consumidor.

4.8. Reunión Comisionado Noah Joshua Phillips

El Comisionado Phillips comentó, en términos generales, sobre el trabajo que lleva a efecto la Comisión Federal de Comercio, en el ámbito de sus competencias. Indicó a dicho respecto que, en su opinión, resulta conveniente revisar el proyecto de ley chileno en que se encuentra actualmente en tramitación en el Congreso Nacional, que actualiza la legislación en materia de protección de datos personales en Chile, con el objeto de que la nueva regulación no afecte el correcto desenvolvimiento de los acuerdos comerciales suscritos entre Chile y otras economías.

4.9. Dispositivos conectados y *Big Data*

El Internet de las cosas (*Internet of Things, IOT)*), tiene distintos beneficios al consumidor, entre ellos:

- Salud
- Automatización del hogar
- Transporte
- Beneficios a la sociedad

El IOT también trae consigo riesgos, en el ámbito de la privacidad y de la seguridad:

Riesgos a la privacidad:

- Problemas en la precisión de los datos.
- Recopilación directa de información personal sensible.
- Recopilación de información personal, hábitos, ubicaciones y condiciones físicas a lo largo del tiempo. Todo esto puede terminar en inferencias o consecuencias imprevistas.
- Falta de conocimiento o consentimiento del consumidor.
- Falta de precisión de los datos.

Riesgos a la seguridad:

- Permitir el acceso no autorizado y el mal uso de la información personal
- Facilitar los ataques a la red del consumidor u otros sistemas
- Riesgos para la seguridad personal y física

a) Internet de las cosas *(Internet of Things, IOT)*

Muchos dispositivos conectados no tienen una interfaz de usuario tradicional, por lo que las empresas deben pensar de manera integral sobre la información y las expectativas que se transmiten a través de una experiencia del usuario más amplia:

- Elecciones a punto de venta
- Tutoriales
- códigos en los dispositivos
- Elecciones durante la configuración
- Portales de gestión
- Iconos
- Comunicaciones “fuera de banda” solicitadas por los consumidores
- Menús generales de privacidad
- Enfoque de experiencia del usuario

Hay distintas preguntas de seguridad que preocupan en los dispositivos IOT, por ejemplo:

- "¿Cuál será el nivel de seguridad y soporte (que reciben los dispositivos IOT) mientras están bajo garantía?
- Si se descubre una vulnerabilidad crítica, ¿se proporcionará una actualización?
- ¿Qué sucede después de que expira la garantía?
- ¿Deberían los refrigeradores modernos tener una vida útil, como la comida contenida dentro?"

La FTC ha tenido distintos casos en el que se procesaban datos personales sin consentimiento del usuario/a:

- Caso SmartTv de la marca VIZIO: Capturaban imágenes cada vez que se prendía el TV y enviaba la información. Esta información la vendían.
- Otros casos comentados fuero el de la empresa Vtech; Blu Bold like US.

Para mayor información, link de acceso al informe de IOT elaborado por la FTC.

b) Big Data:

Es la capacidad de recoger datos de los consumidores de una variedad de fuentes y el uso de algoritmos para:

- Extraer información oculta
- Identificar correlaciones
- Hacer predicciones
- Deducir inferencias
- Descubrir nuevas ideas

Según la definición de la FTC, *Big Data* se puede definir a través de las "3 V", que significan:

- Volumen: gran cantidad de información a analizar, en las que los costos para almacenar y acceder a los puntos de datos son asequibles.
- Velocidad: para recopilar, acumular y analizar datos. Eso se ve incrementado por los avances tecnológicos.
- Variedad: amplitud de datos a analizar y que permite realizar combinaciones de datos que pareciera que no tienen relación entre sí.

Lo productos del *big data* se utilizan en las áreas de marketing, mitigación de riesgos y búsqueda de personas. Sus clientes son infinitos: abogados; investigadores; industrias (automotriz, financiera, marketing y publicidad, energía, hospitales, viajes, entretenimiento, educación, manufactureras, farmacéuticas, inmobiliarias, tecnologías); medios de comunicación, campañas políticas, Gobierno e intermediarios de datos, por nombrar algunos.

Intermediarios de Datos *(Data Brokers)*

Los *data brokers* son agentes que recolectan información, entre ellos datos personales, sobre individuos de registros públicos y fuentes privadas, incluidos registros de censos y cambios de domicilio , vehículos automotores y registros de manejo , material aportado por el usuario a sitios de redes sociales , informes de medios y tribunales, registro de votantes listas, historiales de compras de consumidores, listas de buscados y listas de vigilancia de terroristas, registros de transacciones de tarjetas bancarias , autoridades de atención médica e historiales de navegación web. Esta información en muchos casos es vendida a externos, como personas, compañías u otros *data brokers.*

La FTC generó un informe sobre los Intermediarios de datos. La Sección 6 (b) faculta a la Comisión para requerir que una entidad presente "de forma anual o especial", un informe o responda por escrito a preguntas específicas "para proporcionar información sobre la" organización, negocio, conducta, prácticas, administración y relación de la entidad con otras corporaciones, sociedades e individuos ".

- En el informe se solicitó información de nueve intermediarios de datos:
  - ¿Naturaleza y fuentes de datos?
  - ¿Cuál fue el uso, mantenimiento y diseminación de los datos utilizados?
  - ¿Les dan acceso a los consumidores, y la capacidad de corregir y/o optar por no participar?

- La FTC generó un informe con recomendaciones sobre los d*ata brokers:*
  - Resume los resultados de la investigación.
  - Propone legislación.
  - Recomienda las mejores prácticas.

Dentro de las conclusiones de este reporte, se destacan por ámbitos:

a) <u>Fuentes de información:</u>

- Existían 9 fuentes de datos (empresas). Es decir, una fuente por cada empresa.
- La mayoría de estas empresas compran información en los mismos lugares.
- Utilizan múltiples fuentes para los mismos datos.
- Siete de los nueve intermediarios de datos compran o venden información entre ellos mismos.

b) <u>Tipos de datos adquiridos:</u>

- Datos *Raw* (Brutos): Por ejemplo, nombre, dirección, edad, origen étnico;
- Elementos de Datos: Derivan Inferencias de los datos *Raw;*
- Segmentos de Datos: A partir de la información comprada y desconociendo su origen, se generan "fichas" de consumidores que consideran:
  - Características similares
  - Pronostican comportamientos de los consumidores

c) <u>Operaciones que realizan los *data brokers:*</u>

- Los intermediarios de datos coleccionan datos de consumidores de numerosas fuentes, en gran medida, sin el conocimiento de los consumidores.
- La industria de datos es compleja, con múltiples intermediarios de datos que están vendiendo datos entre ellos mismos.
- Los intermediarios de datos recogen y almacenan miles de millones de elementos de datos que cubren casi todos los consumidores estadounidenses.
- Los intermediarios de datos combinan y analizan datos sobre consumidores para hacer inferencias sobre ellos, incluyendo información potencialmente delicada.
- Los intermediarios de datos combinan datos en línea y datos obtenidos fuera de línea para ofrecer productos a los consumidores en línea.

d) Beneficios y riesgos de los *data brokers:*

- Los consumidores se benefician de muchos de los propósitos para los cuales los intermediarios de datos coleccionan y usan datos:
  - Ayudan a prevenir el fraude.
  - Mejoran las ofertas de productos.
  - Ayudan a ofrecer anuncios más personalizados.

- Muchos de los propósitos para los cuales los intermediarios de datos coleccionan y usan datos presentan riesgos a los consumidores.
- El almacenamiento de los datos sobre consumidores de manera indefinida puede crear riesgos de seguridad.

Para mayor información, link de acceso al informe de *Data Brokers* elaborado por la FTC.

La FTC genero un informe sobre *Big Data*. Como parte del informe se menciona el ciclo de vida de *Big Data*, el cual está basado en 4 subprocesos:

- Colección de datos
- Compilación y consolidación de los datos
- Extracción de datos y análisis de estos
- Uso de los datos

Para mayor información, link de acceso al informe de *Big Data* elaborado por la FTC.

4.10. Inteligencia Artificial (IA)

No existe una definición singular de inteligencia artificial, pero en términos generales, son técnicas automatizadas para procesar y tomar decisiones con información.

El aprendizaje automatizado (*machine learning*) es un subconjunto de la IA e involucra el uso de sistemas automatizados que son entrenados con datos en tiempo real para aprender como generar resultados sin ser codificados explícitamente.

- Puede ser: supervisado, sin supervisión o refuerzo.
  - Supervisado: usar datos etiquetados para aprender una regla.
  - Sin supervisión: detectar patrones ocultos en los datos.
  - Refuerzo: se lleva a cabo mediante prueba y error y tiene el objetivo de aprender cómo hacer una tarea en particular (por ejemplo, conducir un automóvil).

- Dónde se emplean técnicas de Inteligencia Artificial:
  - Creatividad digital.
  - Aplicaciones financieras.
  - Salud y asistencia sanitaria.
  - Transporte / vehículos autónomos.
  - Reconocimiento de voz.
  - Traducción de idiomas.
  - Juego de azar.
  - Productividad del trabajador.
  - Predicción del tiempo.
  - Sector energético.
  - Problemas sociales (contaminación, vigilancia, violencia, etc.)

a) Audiencia en Inteligencia Artificial:

Entre el 2018 y 2019, en un periodo de 12 meses, la FTC efectúo audiencias denominadas: "*Hearings on Competition and Costumer Protection in the 21st Century*", en las que convocó a expertos

tecnológicos, la academia, industria, y sociedad civil para discutir tópicos de competencia y protección del consumidor, incluyendo Inteligencia Artificial. Cualquier persona podía presentar un tema en las audiencias.

Los panelistas discutieron algunas preocupaciones de la IA, tales como:

- Problemas de privacidad que surgen de la capacidad mejorada para derivar información confidencial de grandes compilaciones de datos ordinarios. Por ejemplo, ejemplos destacados en los informes del Proyecto de Privacidad del New York Times y otros informes en la prensa popular.

- Falta de transparencia: ¿son explicables las decisiones basadas en IA?
  - ¿Explicable a quién?
  - ¿Qué significa que se pueda explicar las decisiones de IA para diferentes partes interesadas?
  - ¿Deberían los sistemas de IA ser externamente responsables o comprobables?

- Capacidad para evadir medidas de seguridad explotando vulnerabilidades en algoritmos de aprendizaje automático.
  - Aprendizaje automático adverso: diseñado para intentar engañar a los modelos de aprendizaje automático (por ejemplo, autos sin conductor y ejemplo de señal de stop)

- Preguntas sobre quién es responsable de los daños al consumidor.

Los panelistas explicaron que otras preocupaciones también surgen en la toma de decisiones, pero pueden amplificarse mediante el uso de IA:

- Decisiones sesgadas o injustas.
- Decisiones poco confiables o inexactas.
- Asimetrías de información y poder entre consumidores y empresas.
- Discriminación de precios mejorada.
- Limitaciones en la información y la elección derivadas del sesgo determinista algorítmico/confirmación.

b) <u>Privacidad e Inteligencia Artificial:</u>

Algunos expertos han distinguido los métodos de procesamiento de datos antiguos de los métodos habilitados para IA:

- La Inteligencia Artificial permite una capacidad mucho mayor para recopilar, almacenar y procesar enormes cantidades de datos.
- Permite detectar conexiones que no necesariamente serían evidentes a través de otras formas de análisis.
- Habilita la predicción e imputación.
  - Con suficientes datos sobre lo qué he hecho y lo qué han hecho personas similares a mí, puedo predecir mejor lo que haré.
  - Con suficientes datos sobre lo qué he hecho, y lo qué han hecho personas similares a mí, pueden inferir mejor los datos (¿sensibles?).
- Los comentaristas expresaron su preocupación acerca de cómo se representan los datos confidenciales, la enorme cantidad de datos recopilados y la falta de previsibilidad que los consumidores pueden tener sobre cómo se utilizan los datos.

c) <u>Transparencia e Inteligibilidad:</u>

Los panelistas describieron un debate considerable en los círculos científicos y políticos sobre lo que significan estos términos para la Inteligencia Artificial.

Por ejemplo, pueden significar:

- ¿Entendemos cómo funciona la IA?
- ¿Entendemos cómo se usa la IA?
- ¿Podemos explicar un resultado particular?

Algunos panelistas señalaron que la incapacidad para explicar la tecnología o su producción puede aumentar las preocupaciones sobre el sesgo o la equidad.

¿Los implementadores de IA están identificando y abordando cualquier sesgo o injusticia en los resultados que impactan significativamente a los consumidores? Incluso para los algoritmos de "caja negra", puede ser posible mejorar la equidad de los resultados.

Los panelistas también debatieron la medida en que puede haber un intercambio entre transparencia y precisión.

d) Políticas:

Los panelistas debatieron si las leyes actuales son suficientes para manejar los posibles desafíos que plantea la Inteligencia Artificial:

- Algunos señalaron que la IA tiene aplicaciones tan diversas que una "ley de IA" integral podría ser difícil.
- En lugar de una ley general, sugirieron que los formuladores de políticas se centren en aplicaciones de alto impacto (biometría, crédito, salud, etc.).
- Otros señalaron que la FTC ya tiene una autoridad amplia y flexible, en virtud de la Sección 5 y una autoridad más específica, en virtud de estatutos como el FCRA y ECOA (por ejemplo, los requisitos de máxima precisión posibles de FCRA requieren informes de crédito precisos independientemente de la tecnología utilizada).
- Algunos advirtieron que la regulación podría sofocar la innovación de IA.

Los marcos *(frameworks*) emergentes se centran en: "Equidad, responsabilidad, transparencia y ética".

En Estados Unidos, existen organismos que han desarrollado estos marcos emergentes asociados a la Inteligencia Artificial, entre esos organismos podemos mencionar a los siguientes:

- Fundación Nacional de Ciencia.
- la Agencia de Proyectos de Investigación Avanzada de Defensa
- El Instituto Nacional de Estándares y Tecnología.
- Empresas como Google y Microsoft tienen declaraciones similares de sus principios de IA.

Otros marcos éticos para la IA se basan en la igualdad de oportunidades o la ética en la investigación de sujetos humanos.

Los principios éticos de la Asociación de la Industria del Software y la Información para IA buscan defender los derechos humanos, la justicia, el bienestar y la virtud.

e) Algoritmos de Colusión: sin ponerse de acuerdo con sus competidores, los sistemas informáticos que contienen algoritmos pueden llegar a coludirse, por ej. Pueden modificar los precios automáticamente.

- ¿Se pueden usar los algoritmos como herramientas para ejecutar acuerdos de precios entre competidores?
- Algunos panelistas consideraron que este tipo de conducta es capturada por el marco antimonopolio tradicional.
- Hubo desacuerdo, sin embargo, entre los panelistas en la medida de qué algoritmos podrían facilitar colusión tácita o podría coludir independientemente, sin humanos intervención.
- Algunos panelistas sugirieron que colusión tácita algorítmica requiere un reexamen de lo tradicional marco antimonopolio, mientras que otro sugirió que el peso de la económica y técnica actual la literatura no apoya estas preocupaciones más amplias sobre colusión tácita algorítmica o autocontrol algoritmos.

f) Efecto de la IA en el análisis anti fiduciario:

Un panelista hizo los siguientes puntos relacionados con la competencia sobre estas tecnologías:

- El movimiento hacia el análisis predictivo permite precios más observables y un procesamiento de datos más eficiente, lo que puede tener implicaciones para la teoría de la colusión;
- Con la mayor dependencia de tecnologías como los asistentes digitales, los encargados de hacer cumplir la ley antimonopolio pueden necesitar pensar más sobre "datos cautivos" que pueden no ser observables para los competidores en la forma en que Internet era cuando se lanzaron compañías como Google; y
- Aunque el avance de estas tecnologías puede no requerir un cambio en la ley antimonopolio, puede ser necesario cambiar la forma en que se aplica la ley existente.

Para acceder a información complementaria de este tema, se informan algunos informes de interés:

- Facial Recognition Technology
- AI and Blockchain
- Competition and Consumer Protection Hearings AI
- Big data, privacy and competition
- Data security
- FTC's Approach to Consumer Privacy

4.11. *FinTech* y Datos Financieros

El término *Fintech* resulta de la unión de las primeras sílabas de *Finance y Technology*, y representa a las empresas que ofrecen servicios financieros utilizando la tecnología existente para ofrecer productos y servicios financieros innovadores.

Las empresas *Fintech* son empresas que intermedian en todos los ámbitos del mundo de las finanzas actuando como *brokers,* como mediadores de pago, como emisores y receptores de transferencias o como asesores financieros. Son empresas de *Crowdlending;* de transferencias de fondos; de asesoramiento financiero y en inversiones; de pagos y cobros a través de dispositivos móviles, entre otras.

En los últimos años, la industria financiera ha tenido que adoptar nuevas tecnologías financieras *(Fintech*), que implica un cambio en la mentalidad de las instituciones financieras tradicionales y ha tenido un impacto directo en la forma en que los reguladores del sector financiero visualizan el mercado en el futuro.

El marco jurídico que regula las transacciones de *FinTech* son:

- Ley Federal de la Comisión Federal de Comercio (*FTC Act)*
- Ley de veracidad en los préstamos *(Truth in lending Act)*
- Ley de transferencia de fondos electrónicos *(Electronics funds transfer Act)*
- Ley de informes de crédito justos *(Fair Credit Reporting Act- FCRA)*
- Ley de igualdad de oportunidades de crédito *(Equal Credit Opportunity Act-ECOA)*
- Ley Gramm-Leach Billey *(Gramm-Leach Billey Act- GLBA*)
- Ley de confianza del comprador en línea *(Restore Online Shopper's Confidence Act- ROSCA*
- Ley de protección de la privacidad en línea para niños *(Children´s Online Privacy Protection Act-COPPA*)
- Además, de leyes de aplicación a nivel estatal.

Además, se establecen "memorándums de entendimientos" (*memorandum of understanding-MOU*) que determinan la jurisdicción en ciertos ámbitos de competencias de organismos, con la finalidad de no entorpecer una investigación. Los memorándums son comunicaciones formales para coordinar de manera sistemática entre instituciones cuando se está investigando una temática con la finalidad de coordinar el trabajo entre agencias y evitar ir en ámbitos contrarios.

Las agencias que interactúan en este ámbito son: Comisión Federal de Comercio (*Federal Trade Commission-FTC)*; Departamento del Tesoro (*Department of the Treasury)*; Corporación Federal de Seguro de Depósitos (*Federal Deposit Insurance Corporation- FDIC)*; Oficina de Protección Financiera del Consumidor (*Consumer Financial Protection Bureau- CFPB*); Comisión de Bolsa y Valores (*Securities & Exchange Commission- SEC);* Junta de Gobernadores del Sistema de la Reserva Federal (*The Federal Reserve System Board of Governors)*; Oficina del Contralor de la Moneda (*Office of the Comptroller of the Currency).*

A nivel internacional, existe consenso en que a los consumidores se les deben brindar el mismo nivel de protección de sus datos en el comercio electrónico del comercio físico. En este aspecto, existen directrices, tanto de la OCDE, ONU y de la FTC para la protección de consumidores en el ámbito de la FinTech, por ejemplo:

- *Consumer Protection in E-commerce de la OCDE (link)*
- *United Nations guidelines for consumer protection (link)*

La OCDE ha identificado una guía de 6 pasos para abordar las denuncias de parte de los consumidores en el marco de las transacciones de *FinTech*. El enfoque apunta a la interacción con las partes interesadas:

- Paso 1: identificar y definir el problema y su fuente
- Paso 2: Medir el daño al consumidor (detrimento al consumidor)
- Paso 3: Determinar si requiere una acción política (*policy action)*
- Paso 4: Evaluar las opciones disponibles de acciones política (*policy action)*
- Paso 5: Seleccionar la mejor opción de acción política (*policy action)*
- Paso 6: Revisar la efectividad de la opción implementada

Se utiliza la herramienta de los 6 pasos para analizar las políticas de *FinTech* y su ámbito de aplicación:
Para determinar si existe detrimento, se requiere contar con la evidencia del detrimento. La FTC actúa en base a denuncias; estudios (encuestas; grupos de enfoques; *"sweeps*" y/o compras encubiertas; experimentos

económicos); informes de organizaciones externas (asociaciones de consumidores; académicos; medios de comunicación); indicadores.

Para determinar el alcance del problema y detrimento, la FTC realiza una serie de audiencias y talleres relacionados con *FinTech.* Una vez que se define la política, se aplican los principios de protección del consumidor a acciones particulares de aplicación de la ley; se emiten las ordenes de ejecución y se publica la información con enfoque hacia el consumidor y empresas comerciales.

Ejemplo de talleres, audiencias y estudios realizados:

a) Talleres:

- *Marketplaces lending*
- *Crowdfunding and peer-to-peer payments*
- *Artificial intelligence and blockchain*
- *Cryptocurrency scams*

b) Estudios:

- *Data brokers: A call for transparency and accountability*
- *Big data: a tool for inclusion or exclusion*

c) Audiencias Públicas:

- Protección del consumidor
- Rol de la FTC en un mundo cambiante 1 y 2

La FTC realiza investigaciones; cita a los involucrados; solicita ordenes al Juez y opta por llegar a un acuerdo con la empresa infractora antes de la demanda. De no obtenerse el acuerdo, la Corte resuelve el caso. De obtener el acuerdo, se emite una orden ejecutiva con acciones de cumplimiento *(enforcement actions*) que son verificadas por la entidad.

Se comentan algunos ejemplos de casos en los que se ha exigido el cumplimiento de la ley:

- *Venmo:* Aplicación tecnológica conocida por organizar "vaquitas" de dinero. Esta aplicación retenía datos de consumo de sus usuarios y comunicó la información de con quién cada persona realizaba transacciones y en qué tipo de comercio consumía.
- *Blue Global:* Esta empresa conectada a los consumidores con prestamistas de menor costo, entregando sus datos a prestamistas legítimos. Sin embargo, sólo el 2% de los compradores de datos de esta aplicación eran prestamistas.
- *Career Education Corp (CEC*): Empresa proveedora de préstamos estudiantiles que informaba que estaba afiliadas a ciertos empleados y las FFAA. Esta empresa vendía datos de visitantes a empresas de educación mintiendo as las empresas durante la afiliación de las personas.
- *Credit Bureau Center (CBC);* Empresa que proporcionaba historial crediticio, obtuvo los datos de sus consumidores a través de tergiversaciones, haciéndose pasar por propietarios y pidió que los solicitantes obtuvieran informes de crédito de su stio web, haciendo que los consumidores se inscribieran en sus planes y sin informarles que tenían derecho al menos a un informe gratuito al año.
- Otros casos: *Gran Teton; Realpage; Uber; Pact inc.;*

La FTC no regula el sector financiero pero la proliferación de nuevos servicios por las vías tecnológicas (apps y dispositivos móviles) en este sector han determinado que la FTC se involucre en la protección de la privacidad de los consumidores, a través del engaño o la acción desleal de parte de las empresas.

4.12. Seguimiento de Dispositivos cruzados *(Cross-Device Tracking)*

Consiste en el análisis de la experiencia del consumo posible a partir de la existencia de una gran cantidad de dispositivos tecnológicos que permiten efectuar ese seguimiento del consumidor: aplicaciones en los celulares; Netflix; Facebook; entre otros.

Es un concepto relativamente nuevo y para informarse de las nuevas tecnologías existentes, la FTC realiza audiencias con las empresas para enterarse de las nuevas tecnologías que se están empleando. Además, se informan a través de las asociaciones de consumidores y publicistas. Complementariamente, FTC efectúa talleres con consumidores para recibir sus comentarios sobre la experiencia de consumo de este tipo de tecnologías y esta información se registran en los blogs de la FTC.

Los beneficios del *cross-device tracking* está asociada en conocer la experiencia ininterrumpida del consumidor a través del uso de estos dispositivos, lo que permite orientar la publicidad de una manera más dirigida a las necesidades del usuario y les permite ser más competitiva.

En el ámbito de la privacidad, este tipo de dispositivos debe efectuar la recopilación de la información del consumidor con su conocimiento y consentimiento. En consecuencia, aspectos como la transferencia y consentimiento, en distintos momentos del uso, permiten operar de forma segura para la privacidad y seguridad del consumidor.

Se comentan los casos de *cross-device tracking* en los cuales la FTC ha intervenido: Caso Visio; Silver Bush y Stalker wear.

5. Reunión en el Departamento de Seguridad Nacional (*Department of Homeland Security- DHS)*

a) Política de privacidad en el Departamento de Seguridad Nacional:

La definición de privacidad no es la misma que utilizan los países de la Unión Europea, porque tienen en cuenta datos con alguna conexión personal: información personal identificable. El marco de leyes que regula es distinto para el sector público y sector privado.

En el caso del sector público el marco de leyes esta dado por:

- Constitución
- *Privacy Act 1974*: establece qué información se recopila y para qué; con qué autoridad se obtiene la información; cuándo se destruye o archiva la información.
- *E-Goverment Act*: Evaluación de riesgos de recabar cierta información y compartirla.
- *Fredom Of Information Act (FOIA)*
- FIPPS marco común de privacidad internacional
- *Homeland Security Act* (2002): crea el Jefe de seguridad en DHS con responsabilidades para garantizar temas de privacidad y transparencia.

El sistema tiene equilibrio de responsabilidades para los poderes ejecutivo, legislativo y judicial:

Ejecutivo	Legislativo	Judicial
• *Office of Management and Budget* • Emite pautas y directivas. • Revisa informes de agencias federales • *Inspectors General* • Reportes semestrales al congreso que incluyen informes sobre privacidad. • Participación en el reporte de la Federal *Information Security Management Act.* • Auditorias Bienales de Privacidad. • Auditorías, Investigaciones e Inspecciones a agencias estatales.	• *Government Accountability Office* ○ Apoya al Congreso ○ Mejora el rendimiento y asegura la rendición de cuentas del Gobierno Federal. ○ Realiza investigaciones y auditorías según lo ordenado por la ley o a solicitud de comités del Congreso. ○ Informa sobre el cumplimiento de los objetivos del programa gubernamental. • *Congressional Commites* ○ Supervisan el desempeño del poder ejecutivo e investigan las denuncias de irregularidades. Investiga y supervisa la financiación para agencias y programas y promueve el *Accountability.*	• Hacen cumplir diversos estatutos y leyes.

El Departamento de Seguridad Nacional tiene responsabilidades en torno a:

- Asegurar que el uso de tecnologías no afecte la protección de la privacidad en el uso, la recopilación y la divulgación de información personal.
- Proporcionar una reparación imparcial y efectiva para todos los reclamantes

Principios de las Buenas Prácticas del Departamento de Seguridad Nacional:

- Transparencia
- Participación
- Especificación de propósito
- Minimización de datos
- Uso limitado de datos
- Calidad e Integridad de los datos
- Seguridad
- Rendición de cuentas y vigilancia.

Actividades internacionales del Departamento de Seguridad Nacional:

- Cuando se desarrollan o actualizan nuevos sistemas para recopilar información de identificación personal, realizan una reunión con el gerente del proyecto, al inicio del proceso de diseño, para revisar si los principios que promueve el Departamento de Seguridad Nacional son parte del proceso de documentación de cumplimiento.
- Se coordinan esfuerzos para asegurar que los incidentes de privacidad sean reportados, abordados, investigados y mitigados.
- Intercambio de información e Inteligencia:
    - Revisan todos los acuerdos de intercambio de información del Departamento.
    - Son parte de juntas y grupos de trabajo nacionales e internacionales de intercambio de información.
    - Promueven la consistencia y transparencia en todos los ámbitos.
    - Realizan revisiones de privacidad de los productos y reportes de inteligencia.

Instrumentos Internacionales en privacidad de los que EEUU es parte:

- Guías de seguimiento de dispositivos cruzados sobre la protección de la privacidad y los flujos transfronterizos de datos personales (*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data).* OECD, 1980.
- Marco de privacidad (*Privacy Framework*). APEC, 2004.
- Plan de acción Más allá de la frontera: Declaración de principios de privacidad de los Estados Unidos y Canadá (*Beyond the Border Action Plan: Statement of Privacy principles by the Unites States and Canada),* 2012.

Elementos a considerar sobre la privacidad en asuntos internacionales:

- El intercambio de información es fundamental para combatir el terrorismo y la seguridad.
- Cada país tiene una historia, cultura y contexto político particular.
- Los países soberanos y democráticos tienen sus propias leyes y deberes para proteger a sus ciudadanos.
- Las leyes de privacidad y su aplicación siempre variarán entre los países.
- La Transparencia es una solución.

b) <u>Implementación de la Ley sobre libertad de información (*Freedom of information Acta, FOIA)* en el Departamento de Seguridad Nacional</u>

Freedom of Información Act (FOIA)

- Promulgada por el Congreso en 1966.
- Creada para garantizar el acceso a la información pública y prevenir el secretismo.
- Las agencias deben responder todas las solicitudes de información, excepto la información reservada.

- La última modificación de FOIA fue en el 2016.
- Aplica solo al poder ejecutivo. No aplica al poder legislativo, judicial ni a la Casa Blanca.

Qué Información es pública:

- Todos los documentos que se elaboran o que mantienen las agencias en el desarrollo de sus deberes.
- Documentos tanto impresos como digitales.
- Incluye información de los mensajes de texto, fotos, videos de celulares y otros servicios de mensajería.
- Temas públicos realizados a través de emails personales también son considerados información pública.

Excepciones:

- Material clasificado.
- Reglamentos de personal internos.
- Información reservada por otras leyes.
- Información comercial o financiera confidencial.
- Documentos intra o inter agencias.
- Información personal.
- Registros o información compilada para la aplicación de la ley.
- Registros relacionados con la supervisión de instituciones financieras
- Información geológica y Geofísica.

Supervisión Federal de la *FOIA:*

Ejecutivo:	Legislativo:	Judicial:
• *Departament of Justice office information policy*: Emite guías y orientaciones • *National Archives and Record Administration Office of Government Information (Ombudsman FOIA):* Resuelve discrepancias, monitorea cumplimientos y emite opiniones de carácter consultiva.	• *Congressional Commites*: realiza supervisión y aprueba legislación. • *Government Accountability Office*: realiza auditorías de cumplimiento.	• Tribunal de distrito dictamina sobre litigios FOIA. Los casos pueden ser resueltos donde reside el solicitante o donde opera la agencia.

Las solicitudes más recurrentes en la FOIA del Departamento de Seguridad Nacional versan sobre los siguientes aspectos:

- Archivos sobre extranjeros.
- Deportaciones y Aprehensiones.
- Registros de entrada y salida.
- Investigaciones criminales.
- Registros Médicos.
- Registros de empleados.

El Departamento recibió 400.245 solicitudes en el año 2019, 5.000 solicitudes más que el 2018. Es la agencia del Estado que más solicitudes recibió el año 2019.

6. Reunión en Facebook

La Dirección con la cual se sostiene la reunión se encarga de velar por los compromisos de privacidad *(privacy engagement)* de Facebook, esto significa establecer relaciones de confianza con los *stakeholders:* reguladores; tomadores de decisiones; sociedad civil, académicos, entre otros.

Producto del acuerdo con la FTC (la que, a esa fecha, estaba pendiente de ratificación de los Tribunales), Facebook se ha preocupado de escuchar y recibir f*eedback* para internalizarlo en el proceso de toma de decisiones.

A partir de este acuerdo es la dedicación del equipo denominado Consejo de Privacidad (*Privacy Council*) a la "privacidad por diseño", esto es velar por la privacidad en todas las etapas de generación de sus servicios: ideación, diseño, implementación, entre otros. Los equipos deben hacer certificaciones regulares para verificar el cumplimiento de los cambios.

Otro compromiso del acuerdo es la publicación de un "*White Paper*" en temas de transparencia; información al titular del dato; consentimiento, entre otros. Su idea es proporcionar solución a los dilemas de privacidad.

La empresa trata de equilibrar la privacidad con las posibilidades de innovación a través de los datos en la economía digital, considerando la legislación global y el correcto flujo de la protección de los datos.

En el marco de la privacidad de los datos, Facebook nos comentan los temas relevantes en esta materia:

- Consideran el Reglamento General de Protección de Datos de Europa (GDPR), y los países que lo adoptan, como muy positivo. Lo que les preocupa es que se haga una copia textual al implementar esta legislación en cada país, sin un análisis local. Facebook está pendiente de la revisión del GDPR prevista para mayo del 2020, en especial, considerando que sus principales clientes y su publicidad provienen de pequeñas y medianas empresas.

- Otro tema que están revisando con interés, es la regulación de tecnologías específicas, como el reconocimiento facial y la Inteligencia Artificial. Para esto, creen que debe existir una discusión más holística, de largo plazo, pues al llegar las definiciones normativas, la tecnología ya habrá evolucionado. También, está dentro de sus preocupaciones los temas de sesgos al trabajar con Inteligencia Artificial.

- Están preocupados por el flujo transfronterizo de datos. Mencionan el caso de India, país que decidió restringir el flujo transfronterizo, exigiendo almacenamiento local.

- Un aspecto que encuentran positivo tanto para compañías como órganos reguladores, es el intercambio de opiniones e ideas. Han hecho colaboraciones con la autoridad de Singapur en materias de Inteligencia Artificial, y su forma de regulación. La ley de India incluye explícitamente la posibilidad de hacer estos trabajos. Con la OCDE también están viendo este tema.

- En el caso de Estados Unidos, Facebook está a favor de una Ley Federal. Consideran positivo la coordinación entre privados y reguladores. El GDPR es una posibilidad de crear códigos de conducta, de tener buenas prácticas desde el principio. Hasta el día de hoy no hay un código conducta del GDPR. En cambio, Colombia y México si lo tienen.

- Consideran de importancia tener un periodo de implementación de las leyes. Se debe considerar que el GDPR un trabajo de 30 o 40 años, no es copiar un modelo externo, hay que adaptarlos a las realidades locales, aún hay que aprender y está en construcción. Un tema que han visto en Europa es la cantidad de reclamos que tienen que recibir y tramitar. Lo que se da en países de tradición civil. Por ejemplo, en España tienen que responder a todos los requerimientos. Esto no permite enfocarse en los fenómenos, pues hay que ver todos los casos.

- El CBPR (*Cross-Border Privacy Rules,* de APEC) es un tema interesante, en el contexto del nuevo NAFTA. Se le ve mucho potencial, hay varios países interesados en incorporar el protocolo. En Chile, la ley no está incluyendo explícitamente que el ente regulador pueda certificar a certificadores, lo que haría no poder cumplir con la mirada del CBPR, que es práctico y libera tiempos a la entidad reguladora.

- Respecto a los desarrolladores externos que operan en la plataforma de Facebook, indican que deben aceptar las condiciones de Facebook para estos efectos. Sus condiciones son muy restrictivas para usar sus API (interfases con las cuales los desarrolladores acceden a información). Si necesitan más que la foto, nombre o email, pasa por un proceso manual para justificar porque necesitan los datos. Además, esto se hace con el consentimiento del usuario.

- Respecto a la estrategia de gestión de software (plataforma Facebook) utilizan el enfoque *Sandboxing*, que permite aislar las aplicaciones desarrolladas, de los recursos críticos de la plataforma (versión de Facebook en uso por sus usuarios). Más información, se puede ver en: https://developers.facebook.com/ads/blog/post/2016/10/19/sandbox-ad-accounts/.

RESULTADOS PARA LA INSTITUCIÓN (NUEVOS PROYECTOS, OPORTUNIDADES O DESAFÍOS IDENTIFICADOS PARA LA INSTITUCIÓN)	Además de la elaboración de este informe final consolidado. Se programó la ejecución de una actividad de transferencia de conocimientos de esta pasantía al equipo interno del CPLT, cuyos contenidos se informan a continuación: **I. Charla de Protección de Datos Personales y el rol del CPLT** **Objetivo:** Dar a conocer las modificaciones al proyecto de ley de Protección de Datos Personales y sus implicaciones al rol del Consejo para la Transparencia. **Contenidos:** 1. Introducción a la legislación de protección de datos personales 2. Propuesta de perfeccionamiento legal en tramitación Conceptos generales Principios de la Protección de Datos Personales Derechos ARCOP 3. Órgano garante de protección de datos personales • Atribuciones legales • Gobierno Corporativo **II. Charla la experiencia norteamericana en protección de datos personales** **Objetivo:** Dar a conocer el modelo de protección de datos personales de Estados Unidos, a partir del rol de la *Federal Trade Commission (FTC*). **Contenidos:** 1. Características del modelo norteamericano de protección de datos personales

	2. Federal Trade Commission como órgano garante de protección de datos personales: a. Definición b. Marco legal y competencias c. Procedimiento y sanciones d. Casos emblemáticos 3. Los avances tecnológicos y la protección de datos personales 4. Promoción y educación de consumidores en datos personales
OBSERVACIONES	Informe elaborado a partir de los apuntes de proporcionados por integrantes de la delegación.
FECHA: **ELABORADO POR:**	Carolina Andrade, Gastón Avendaño, Marisol Contreras, Ana María Muñoz, Daniel Pefaur y Emerson Suárez. Marzo 2020