Conferencia Anual Latinoamericana Sobre Delitos Financieros de la ACFCS

13-14 de Octubre, 2016 | Hard Rock Panamá Megapolis

Panel General 3: El enorme riesgo que corre la PRIVACIDAD de la información en los delitos TRANSNACIONALES y cómo mitigarlo

Rolf Stern

Presidente Ejecutivo

BDO Consulting

Ecuador

ACFCS | ASOCIACIÓN DE ESPECIALISTAS CERTIFICADOS EN DELITOS FINANCIEROS

Indice

I. Introducción
II. Contexto
III. Situación global en LATAM
IV. Status en países selectos
V. Conclusiones

Indice

I. Introducción

- Visión global a la privacidad relacionada con investigaciones de delitos financieros
- Énfasis en la región LATAM
  - Visión global
  - Particularidades de países selectos
- Algunas conclusiones basadas en lecciones aprendidas

Indice

I. Introducción

II. Contexto

III. Situación global en LATAM

IV. Status en países selectos

V. Conclusiones

II. Contexto

- El resultado deseado de la investigación sobre delitos financieros transnacionales ha cambiado
  - Antes, el foco estaba en identificar culpables y su castigo: ***punición*** (autores intelectuales y materiales, encubridores, ejecutores): **P**
  - Cada vez más, el enfoque está ampliado y enfatizado a ***resarcimiento*** del daño a los damnificados, sumado a la ***punición*** de los actores (***caso Madoff***): **P+R**

“reparar el mundo (tikum olam)”

II. Contexto – caso Madoff a 2016

- Piramidación invertida: Ponzi
- Comenzó en 2007, formalmente acusado 2008
- Damnificados: más de 10,000 personas, organizaciones sin fines lucro, bancos, fondos de inversión y de cobertura (“hedge funds”)
- Daño: US$20bn
- Recuperación: US$12bn
- Repago integro ya efectuado: 1,800 personas
- Costos incluido Fideicomisario: US$1bn

II. Contexto

- Los delitos financieros son cada vez más mundiales, ya no solo locales ni regionales
  - Involucran cada vez más países (jurisdicciones legales, culturas e idiomas, entidades gubernamentales y privadas, regulaciones sobre protección de la información).
  - El delito y su información salta fronteras, sistemas financieros, entidades corporativas, monedas, cuentas personales y corporativas.
- No todos los países tienen acuerdos de Asistencia Penal Internacional (API) entre ellos – claves para lograr resultados
- Según el país, hay posiciones diferentes sobre la colaboración investigativa transnacional, por parte de las entidades locales en cada país de la fiscalía, judiciales, tributarias, reguladoras de sociedades financieras, policía
- Es necesario que la debida diligencia en preservar la cadena de evidencia cumpla con las particularidades de cada país

II. Contexto

- La tecnología utilizada para cometer delitos financieros es cada vez más variada y compleja
  - Recopilar la evidencia hoy en día abarca multi-media: computación, telefonía, computadores (PCs, laptops, tabletas), memorias portátiles y virtuales, passwords, internet (superficial y profunda), servidores (locales, internacionales, virtuales), y demás.
  - Acceder a los datos del delito y sus actores a veces requiere permisos especiales de los proveedores de servicios de conexión (Movistar, Claro) y de relación (Google, Facebook).
  - El volumen de los datos a coleccionar y procesar ha crecido exponencialmente (Terabytes, Petabytes, Hexabytes).
  - Analizar la evidencia requiere cada vez mayores capacidades (BigData) y software especializado y cambiante para encontrar las inter-conexiones del delito (p.ej.: Relativity, Brainspace).

II. Contexto

- El número y diversidad de los actores delictivos involucrados en un caso es cada vez más grande (e.j.: ***Lavajato***)
- Los equipos de investigadores crecen en complejidad y tamaño
  - Para un caso se necesita que al equipo concurran variadas disciplinas profesionales: investigadores financiero-contables, abogados, especialistas en tecnología informática, investigadores criminales y otros, que trabajen bien en conjunto
  - Con frecuencia se requiere personal multi-lingue y multi-cultural. En LATAM, al menos español (y portugués) e inglés
  - Usualmente hay que desplazar equipos a distintos países, coordinados e inter-conectados por medio de telecomunicaciones inter-activas
- La presión sobre producir resultados más pronto acortan cada vez más los plazos que tienen los investigadores
- A veces uno no sabe para quién realmente trabaja

II. Contexto – caso Lavajato a 2016

- Lavado de dinero por red paralela de cambistas (“doleiros) usando redes de gasolineras y lavadoras de autos
- Comenzó en 2009
- Daños: US$13bn más US$2bn en coimas
- Recuperación esperada: US$6,6bn; ya obtenida US$1bn y secuestrada US$0,7bn de activos de involucrados
- Involucrados:
  - Altos ejecutivos de Petrobras
  - 9 ejecutivos de principales empresas brasileras (Odebrecht, OAS, Andrade Gutierrez, Camargo Correa, Queiroz Galvão, Engevix, Galvão Engenharia, Mendes Júnior y UTC)
  - 53 políticos de casi todos los partidos políticos de Brasil, incluso ex-presidentes Rouseff y Lula
  - Juridícamente: 100 condenas, 74 prisiones preventivas, 91 prisiones temporales y 6 prisiones en flagrancia.
- Jurisdicciones: Brasil, USA, países de Latinoamerica, Europa

Indice

I. Introducción
II. Contexto
III. Situación global en LATAM
IV. Status en países selectos
V. Conclusiones

III. Situación global en LATAM

- En investigaciones de delitos financieros, tener acceso a los datos personales de los presuntos actores delictivos es frecuentemente necesario.
- En una investigación transnacional, hay que tomar en cuenta la particularidad de cada país en la protección de estos datos personales.
- La tendencia general es convergencia hacia el standard de Europa (Data Protection: Regulation, aplica desde mayo 25, 2016; Directive, aplica desde mayo 16, 2016 y debe ser convertida en ley nacional en cada país desde mayo 6, 2018; EU-US Privacy Shield desde julio 12, 2016).
- Otra tendencia regional es hacia más fuerte aplicación de sanciones (México, Colombia, Perú y Brasil).

III. Situación global en LATAM

- En la región LATAM, hay una diversidad en la existencia de leyes
  - Trece jurisdicciones en LATAM tienen leyes de privacidad: Argentina, Aruba, Bahamas, Chile, Colombia, Costa Rica, Curacao, República Dominicana, México, Nicaragua, Perú, Trinidad Tobago, y Uruguay.
  - Argentina y Uruguay tienen las leyes más parecidas a las de la UE. Chile enmendará su ley para fortalecer privacidad, establecer restricciones transfronterizas y una entidad reguladora.
  - Otras jurisdicciones como Brasil, Ecuador e Islas Caimán tienen leyes en proceso.

III. Situación global en LATAM

- Hay algunos ***aspectos comunes*** en la legislación sobre la privacidad de los datos personales.
  - **Notificación**: todas las leyes requieren que las personas sean notificadas cuál información personal es recopilada, para qué y con quién es compartida.
  - **Opciones**: todas las leyes estipulan poder escoger entre diversos niveles de privacidad.
  - **Seguridad**: todas las leyes requieren, en mayor y menor detalle, que las organizaciones que recopilan la información tomen precauciones sobre pérdida, mal uso y acceso, alteración y destrucción no autorizados.
  - **Acceso y corrección:** todas otorgan derecho a conocer y corregir rápidamente la información.
  - **Integridad de los datos:** todas requieren que la información esté completa y al día.
  - **Retención de datos:** todas las leyes estipulan limites sobre la retención de los datos (principalmente restrictas al plazo de uso).

III. Situación global en LATAM

- Hay ciertos ***aspectos diversos*** en la legislación sobre la privacidad de los datos personales.
  - **Transferencia transnacional:** dos tercios de las leyes limitan transferencia de información a otros países, en general si son considerados de insuficiente protección a la privacidad, obligando obtener consentimiento.
  - **Registro**: casi la mitad de las leyes requieren registro para acceder a datos.
  - **Anuncio de fugas**: un tercio requiere anunciar fractura de las seguridades y fuga de información.
  - **Acatamiento obligado:** Agencias de Protección de Datos (DPAs) son requeridos establecer en casi todas las leyes, y en muchas un Oficial de Protección de Datos (DPOs).

III. Situación global en LATAM

Acceso a Datos Personales:

- Más Restringido
- Restringido
- Algunas Restricciones
- Restricciones Mínimas
- Restricciones no efectivas
- No posee legislación o información
- La vigilancia del gobierno puede afectar la privacidad

Fuente: Forrester Privacy and Data Protection – Global Heat Map 2015

Indice

I. Introducción
II. Contexto
III. Situación global en LATAM
IV. Status en países selectos
V. Conclusiones

IV. Status en países selectos

Argentina

- Ley de Protección de Datos Personales (2000)
- Primer país reconocido por la UE dando adecuada protección
- Si requiere notificación y no requiere consentimiento, excepto para ciertos datos personales sensibles (como raza, religión, creencias religiosas y políticas, membresía sindical, salud y hábitos sexuales)
- Prohíbe transferencia transfronteriza a países de inadecuada protección, a menos que la persona haya consentido o haya convenios internacionales
- Requiere registro
- Establece tres niveles de seguridad (bajo, medio y alto: información personal sensible) y medidas detalladas
- No requiere notificación en caso de fugas de datos
- El acatamiento es por la Dirección Nacional de Protección de Datos Personales ubicado en el Ministerio de Justicia y Derechos Humanos.

Fuente: BakerHostetler 2015 International Compendium of Data Privacy Laws

IV. Status en países selectos

Brasil

- No tiene ley específica pero sí hay leyes aplicables y la Constitución (Artículos 5 y 29)
- Sin embargo, hay ciertos derechos consagrados en la Constitución Brasilera sobre colección de datos (incluida notificación y habeas corpus), y hay leyes aplicables en áreas específicas (secreto bancario, ética médica, protección al consumidor, crédito y telecomunicaciones)
- La "Ley de Marco Civil da Internet" (aplicada 2014) atiende temas de sitios web sociales, motores de búsqueda, hosting de usuarios y restringe compartir datos y comunicaciones personales
- No requiere registro
- En general, transferencia transfronteriza es permitida con consentimiento
- No requiere notificación en caso de fugas de datos
- No hay una entidad específica encargada del acatamiento a la privacidad de datos personales

Fuente: BakerHostetler 2015 International Compendium of Data Privacy Laws

IV. Status en países selectos

México

- Ley Federal de Protección de Datos Personales en Posesión de Particulares (2010) y sus regulaciones (2011)
- Si requiere notificación detallada y consentimiento, incluido específico para datos personales sensibles, procesamiento de datos financieros y de activos. No requiere consentimiento para datos públicamente disponibles
- Transferencia transfronteriza requiere notificación y consentimiento, excepto por ley, convenios internacionales, administración de la justicia, o dentro de un grupo controlado de emprendimientos
- Requiere importantes medidas de seguridad
- Requiere notificación detallada en caso de fugas materiales de datos y corrección inmediata
- El acatamiento es por el Instituto Federal de Acceso a la Información Pública y Protección de Datos

Fuente: BakerHostetler 2015 International Compendium of Data Privacy Laws

IV. Status en países selectos

Colombia

- Ley 1581 del 17 de Octubre de 2012 por la cual se Dictan Disposiciones Generales para la Protección de Datos Personales (aplicable desde Junio 2013)
- Si requiere notificación y consentimiento, especialmente para datos personales sensibles. Sin consentimiento datos al interior de una organización no pueden ser compartidos con terceros
- Prohíbe transferencia transfronteriza a países de inadecuada protección, a menos que la persona haya consentido, haya convenios internacionales o la Superintendencia haya aprobado
- No requiere registro, excepto vía regulaciones futuras
- Establece tres niveles de seguridad (bajo, medio y alto: información personal sensible) y medidas detalladas
- Requiere notificación en caso de fugas de datos con efectos materiales sobre las partes afectadas
- El acatamiento es por la Superintendencia de Industrias y Comercio, la cual administra el Registro Publico Nacional de Bases de Datos

Fuente: BakerHostetler 2015 International Compendium of Data Privacy Laws

IV. Status en países selectos

Panamá

- No hay ley específica pero sí legislación pertinente: Ley 51 del 22 de Julio del 2008, modificada por Ley 82 de Noviembre 9, 2012 (“Ley 40”) y Decreto Ejecutivo No. 40 de Mayo 19, 2009 (Decreto 40). Estas regulan la creación, uso y almacenamiento de documentos y firmas electrónicas en Panamá, por medio de proceso de registro y supervisión de proveedores de servicios de datos.
- No hay definición de datos personales ni de datos sensibles. Se entiende que datos personales son los que permiten identificar una persona incluidos nombre, direcciones, números de teléfono, correo electrónico y nombre de usuario, tarjeta de crédito
- La privacidad está protegida por la constitución y por el Código Penal Panameño, y se requiere autorización para ser compartida con terceros (excepto por solicitudes judiciales),
- Transferencia en general requiere autorización del dueño de los datos
- Si requiere registro
- No requiere notificación en caso de fugas de datos
- El acatamiento es por la Dirección General de Comercio Electrónico) (“**DGCE**”)

Fuente: BakerHostetler 2015 International Compendium of Data Privacy Laws

Indice

I. Introducción
II. Contexto
III. Situación global en LATAM
IV. Status en países selectos
V. Conclusiones

V. Conclusiones

ENFOQUE

- Las investigaciones de delitos financieros requieren amplia planeación, secuencia y meticulosa ejecución, combinada con gran flexibilidad (“jogo de cintura”) en adaptarse continuamente
- Uno sabe dónde comienza pero no puede anticipar dónde termina, qué y a quiénes abarca, y qué resultados logrará
- Es crítico ir consiguiendo los talentos, acceso a la información, y los recursos económicos y tecnológicos, crecientes, a medida que avanza la investigación
- Una impaciencia bien administrada y persistencia a toda prueba colaboran con obtener resultados
- Mantener el respaldo de la parte interesada es vital (“watch your back”) para tener éxito

V. Conclusiones

PRIVACIDAD

- Acceder a los datos de los delitos financieros requiere sortear los obstáculos de la privacidad, país por país
- Proteger los datos de las investigaciones requiere proteger fuertemente la integridad de los datos originales, su procesamiento, los hallazgos intermedios y los resultados finales (wikileaks, Panama papers)
- Administrar cuidadosamente la relación con los medios de información es vital para no contaminar los procesos investigativos y acceso a los datos personales de los presuntos actores de los delitos financieros

13-14 de Octubre, 2016 | Hard Rock Panamá Megapolis

Panel General 3: El enorme riesgo que corre la PRIVACIDAD de la información en los delitos TRANSNACIONALES y cómo mitigarlo

Rolf Stern
Presidente Ejecutivo
BDO Consulting
Ecuador

Conferencia Anual Latinoamericana Sobre Delitos Financieros de la ACFCS
13-14 de Octubre, 2016 | Hard Rock Panamá Megapolis