2017

GUÍA DE BUENAS PRÁCTICAS PARA OBTENER EVIDENCIA ELECTRÓNICA EN EL EXTRANJERO

UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA
DIRECCIÓN GENERAL DE COOPERACIÓN REGIONAL E INTERNACIONAL

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

2017

GUÍA DE BUENAS PRÁCTICAS PARA OBTENER EVIDENCIA ELECTRÓNICA EN EL EXTRANJERO

UNIDAD FISCAL ESPECIALIZADA EN CIBERDELINCUENCIA
DIRECCIÓN GENERAL DE COOPERACIÓN REGIONAL E INTERNACIONAL

GUÍA DE BUENAS PRÁCTICAS PARA OBTENER EVIDENCIA ELECTRÓNICA EN EL EXTRANJERO

Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)
Dirección General de Cooperación Regional e Internacional (DIGCRI)

Diseño: Dirección de Comunicación Institucional | Dirección de Relaciones Institucionales |
Ministerio Público Fiscal de la Nación.

CONTENIDO

PRESENTACIÓN

El objetivo de este documento es brindar a las y los investigadores una herramienta que sirva de guía en caso de que necesiten obtener información electrónica almacenada en el extranjero, en especial, en los Estados Unidos de América.

Las recomendaciones sistematizadas en este material fueron elaboradas conjuntamente por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) y la Dirección General de Cooperación Regional e Internacional (DIGCRI) del Ministerio Público Fiscal de la Nación sobre la base de documentos oficiales y la experiencia adquirida a lo largo de estos años de trabajo.

I. CLASES DE INFORMACIÓN Y FORMAS DE OBTENERLA

Las pautas y recomendaciones comprendidas en esta guía se centran exclusivamente en la obtención de evidencia electrónica almacenada por los proveedores de servicios, y no en la obtención en tiempo real de comunicaciones.

En este sentido, concentramos el análisis en la información almacenada, relacionada con cuentas de correo y con redes sociales (datos del usuario, historial de conexiones, contenido de correos electrónicos, etc.) u otros servicios de internet (como registro de nombres de dominio o alojamiento de sitios web) que es la que usualmente se solicita.

En términos generales, la legislación de los Estados Unidos de América (EUA) clasifica los registros en función de la mayor o menor invasión a la privacidad del usuario. En otros términos, cuanta mayor intrusión se requiera, más altos serán los estándares que deben satisfacerse para obtener la información.

De esta manera tenemos tres grupos de información: básica, transaccional y de contenido.

La importancia de la clasificación previa radica en que el canal que deba utilizarse dependerá de la información solicitada.

a. Información Básica del Suscriptor, que incluye usualmente:

- Datos del titular de la cuenta (nombre, país, dirección, teléfonos, edad, género, etcétera).
- Dirección de correo electrónico asociada (usada generalmente para verificar/recuperar la cuenta).
- Número de teléfono celular asociado (usado generalmente para verificar/recuperar la cuenta).
- Número de tarjeta de crédito asociada (que se brinda para hacer compras en la plataforma).
- Dirección IP[1] desde la que se creó la cuenta.
- Detalle de los últimos accesos a la cuenta (con fecha, hora, zona horaria y dirección IP).

1. La dirección IP identifica una conexión a internet desde un dispositivo (computadora de escritorio o portátil, celular, tableta o cualquier otro aparato con conexión a internet -televisores inteligentes, heladeras-. Esto es lo que se denomina: "internet en las cosas") en un momento determinado. Esas direcciones IP, que son únicas a través de toda la red de redes, están formadas por un grupo de cuatro segmentos (ej. 200.55.243.205, el número mínimo es 0.0.0.0. y el máximo 255.255.255.255.) y se encuentran distribuidas mundialmente en bloques y son asignadas a los clientes por proveedores del servicio de internet -ISP- (ejemplos de ISP en nuestro país son: "Fibertel" -de Cablevisión Argentina S.A.-, "Speedy" -de Telefónica de Argentina S.A.-, y "Arnet" -de Telecom Argentina S.A.-).

- Información sobre servicios a los que se ha suscripto el titular de la cuenta[2].

La obtención de esta información está sujeta al estándar de citación: sólo hay que demostrar que la misma es relevante y está relacionada con el caso.

Usualmente esa información es entregada por las empresas a autoridades judiciales extranjeras **sin exhorto internacional.** En la mayoría de los casos, bastará enviar un **oficio firmado por el juez** por algunos de los canales habilitados al efecto[3].

b. Información Transaccional, que incluye usualmente:

- Datos de remitente y receptor de correos electrónicos y sus direcciones IP de conexión.
- Día y hora de las comunicaciones que se efectuaron.
- Cantidad de datos que insumió la comunicación.
- Sitios web visitados por el usuario.

En estos casos, el estándar es un poco más exigente. Se van a requerir detalles específicos acerca de cómo los registros son relevantes para la investigación. Y la información sólo será entregada si media una orden de un juez local, para lo cual será necesario enviar un **pedido de asistencia jurídica internacional** (exhorto internacional).

c. Información de Contenido, que incluye usualmente:

- Contenido (texto y adjuntos) de los correos electrónicos que permanezcan en las carpetas de la cuenta (enviados, recibidos, borrador, papelera, etcétera).
- Contenido (texto y adjuntos) de los mensajes intercambiados en plataformas de redes sociales.
- Contenido de publicaciones realizadas en redes sociales cuyo acceso fue restringido al público en general[4].
- Historial de localización asociado a una cuenta.

---

2. En el caso de una cuenta Gmail, por ejemplo, indicará qué otros productos de Google Inc. se encuentran asociados a esa cuenta (tales como: YouTube, Google+, etcétera).

3. Muchas empresas proveedoras de servicios de internet han estableciendo portales o casillas de correo electrónico para que las fuerzas de seguridad o autoridades judiciales puedan cursar sus pedidos.

4. Por ejemplo, publicaciones en cuentas privadas de Twitter o biografías de grupos cerrados de Facebook.

- Fotos y otros documentos almacenados por el usuario en espacios de alojamiento en la nube asociados a una cuenta.

La obtención de esta información está sujeta al estándar más alto: el de orden de allanamiento, basado en una causa probable actual. También será necesario, en este caso, utilizar un **pedido de asistencia jurídica internacional** (exhorto internacional).

PARA TENER EN CUENTA:

- Si es necesario enviar un **exhorto internacional,** el Departamento de Justicia de Estados Unidos ha solicitado que, previamente, se identifique el lugar donde se encuentra la información. En ese sentido, más allá de que la empresa tenga su sede central en un país (por ejemplo, Estados Unidos de América), los datos pueden estar almacenados en servidores localizados en otros países.

  Este requisito surge a partir de un caso reciente[5] en el que se discutió si podía ordenarse a un proveedor de servicios de internet (ISP) registrado en Estados Unidos que entregue información almacenada en servidores alojados en el extranjero.

- Para obtener este dato puede hacerse un pedido directamente a la empresa en el momento de hacer la preservación de los datos (que trataremos a continuación) o antes.

- Nada obsta a que los diversos tipos de información sean pedidos en paralelo (por ejemplo, pedir la información de suscriptor por oficio y la de contenido por exhorto).

- Los investigadores deben tener en cuenta que la empresa puede llegar a notificar al usuario de la existencia de un pedido de entrega de datos (cualquiera sea el tipo) y que eso puede frustrar la investigación. Se recomienda analizar la política de la empresa en ese sentido y, eventualmente, solicitar -por exhorto- una orden judicial para evitar esa notificación (lo cual está sujeto a ciertos requisitos).

---

5. In the Matter of a Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985, 2016 WL 3770056 (2d Cir. July 14, 2016). El fallo puede consultarse desde el siguiente enlace: https://assets.documentcloud.org/documents/2997030/Microsoft-Ireland-2d-Cir-Opinion-20160714.pdf

Los Tratados vigentes sobre asistencia jurídica en materia penal podrán verse en el siguiente sitio web: http://www.mpf.gob.ar/cooperacion-ai/normativa/

Mientras que desde la intranet del MPF se puede acceder a un modelo de pedido de asistencia jurídica a los efectos de requerir evidencia electrónica electrónica: https://intranet.mpf.gov.ar/cooperacion-internacional/.

II. PRESERVACIÓN DE INFORMACIÓN

La información que almacenan los proveedores de servicios puede ser eliminada. En ciertas ocasiones,el usuario de la cuenta puede borrar información puntual (por ejemplo fotos, posteos, mensajes) o eliminar definitivamente la cuenta. También hay casos en los que el proveedor de servicios borra determinada información por el transcurso del tiempo (por ejemplo, los *logs* de acceso a las cuentas).

Se recomienda siempre preservar los datos antes de pedirlos, cualquiera sea la vía escogida (oficio o exhorto) y/o el tipo de información requerido (básica, transaccional o de contenido).

Es un procedimiento muy sencillo y rápido. La preservación usualmente se dispone por un **plazo de noventa días**, renovable por un lapso similar, aunque hay empresas que preservan por mucho más tiempo.

Para concretar la preservación, puede hacerse el pedido directamente a la empresa usando los canales habilitados al efecto (casillas de correo o portales) o a través de la **red 24/7**[6]**,** cuyo punto de contacto en la Argentina es el titular de la UFECI, fiscal Horacio Azzolin, dependencia a la que debe solicitarse la medida por formulario (al que se accede desde aquí: http://www.mpf.gob.ar/ufeci/enlaces/protocolos-y-guias-de-actuacion/) firmado por juez o fiscal y luego enviado a la casilla de correo: cibercrimen@mpf.gov.ar.

Usualmente, cuando se hace la preservación se brinda un número de referencia que recomendamos sea colocado en el pedido de obtención de esa información.

III. CASOS DE EMERGENCIA

Más allá del pedido de información (básica, transaccional o de contenido) y de la preservación, en algunos casos las empresas pueden **entregar voluntariamente** información (de suscriptor, de contenido o

6. La red G7 24/7 de crímenes de alta tecnología (G7 24/7 Network of High Tech Crime) está pensada para las investigaciones que involucran evidencia electrónica y que requieren asistencia urgente de miembros de fuerzas de seguridad o de autoridades judiciales extranjeras, para preservar datos alojados en otros países. El protocolo de la red prevé que los agentes policiales o judiciales que necesiten asistencia de otro país miembro se comuniquen con su punto de contacto nacional para que éste, a su vez, curse el pedido -de corresponder- a su contraparte en el país requerido. Sus miembros están comprometidos a realizar su mejor esfuerzo para lograr que la asistencia se brinde lo más rápidamente posible, pero se tiene presente que ello depende del marco legal y capacidad técnica de cada uno de los países.

ambas) **sin necesidad de exhorto**. El procedimiento se denomina *Emergency Disclosure Request* (EDR).

A esos efectos, debe demostrarse que existe una emergencia que involucra riesgo inmediato de muerte o de seria afectación a la integridad física de una persona, y que esta situación genera que se entregue la información sin demora.

En estos casos el pedido puede realizarse en forma **directa** a las empresas, las cuales evaluarán si el supuesto planteado amerita apartarse de las reglas generales, para lo cual usualmente solicitan información específica al requirente. También **puede utilizarse la red 24/7** para efectuar la solicitud.

Si la solicitud es rechazada por la empresa, puede intentar obtenerse la información por los carriles formales.

IV. RECOMENDACIONES PREVIAS AL PEDIDO

- Revisar términos y condiciones de las empresas a las que se requerirá información. En especial, los aspectos de privacidad (donde indican qué información guardan, por cuanto tiempo y cómo la comparten) y las directrices para las fuerzas de la ley (en las que se detalla el procedimiento para solicitar la información).

- Si se va a solicitar información transaccional o de contenido:

    i. Determinar previamente el lugar donde están ubicados los datos que se necesitan, para evaluar luego a qué país remitir el exhorto.

    ii. Gestionar la preservación de la información en el primer momento posible, con independencia de cuando sea enviado el requerimiento. Indicar en el exhorto que la información fue preservada y citar el número de caso que proporcionó la empresa.

- Si se va a solicitar exclusivamente información básica de suscriptor, analizar la conveniencia de preservar el contenido de la cuenta en función de la empresa a la que se le efectuará el pedido y el tipo de información que puede alterarse o eliminarse en el transcurso del proceso.

MINISTERIO PÚBLICO
FISCAL
PROCURACIÓN GENERAL DE LA NACIÓN
REPÚBLICA ARGENTINA

MINISTERIO PÚBLICO FISCAL | PROCURACIÓN GENERAL DE LA NACIÓN
Av. de Mayo 760 (C1084AAP) - Ciudad Autónoma de Buenos Aires - Argentina
+54 11 4338 4300
www.mpf.gob.ar | www.fiscales.gob.ar