CIBERCRIMEN

Medios digitales y uso de internet en la investigacion

Entrevista: Ezequiel Sallis
Fecha: Noviembre 2016
Lugar: La Plata
Duración: 11:47

¿De qué modo ayuda en la primera etapa de la investigación la utilización de internet y medios digitales?

En la actualidad, me parece que es una herramienta fundamental el hecho de conocer cómo trabajar en Internet para beneficio de la investigación, dado que hay gran cantidad de datos disponibles publicados en las redes sociales por las propias personas investigadas. La relación que las personas tienen hoy con la tecnología es cada vez mayor, es cada vez más intima: la gran mayoría de los aspectos cotidianos de nuestra vida pasa por Internet. Entonces, este tipo de cosas hace que haya mucha información y se transforme en un ámbito vital para que el investigador pueda empezar a desarrollar sus actividades en esa vía, que obviamente se complementa con la investigación tradicional.

El perfil de investigador hoy es muy diferente al que a lo mejor, era hace algunos años atrás. Basándonos en el principio de la criminalística, a las preguntas básicas que uno debe responder en una investigación, hay que sumarles algunos aspectos, como el conocimiento de idiomas; mínimamente los más representativos, por ejemplo, el inglés, ya que existe abundante material de actualización y muchas de las redes sociales lo utilizan en su dinámica de diálogo. Además, debe tener conocimientos técnicos básicos: cómo funciona una computadora, una red y por supuesto, el uso de las herramientas informáticas que van a estar montadas sobre esas plataformas.

Debe saber también, cuáles son los principios básicos de la seguridad de la información, conocer lo relacionado con las propiedades de la evidencia digital (volatilidad, duplicación exacta) y ser flexible ante los cambios. La capacidad de adaptación es una de las variables más importantes, porque la tecnología es dinámica, más allá de aspectos “estables” como la legislación o los efectos penales, con lo cual el investigador corre el riesgo de quedarse atrás.

¿Cuando se vuelve relevante la intervención de un Perito Informático?

En cualquier caso donde la tecnología tenga intervención, porque prácticamente no hay ningún delito que no la utilice, como medio o como finalidad; es transversal a todos los delitos. Aunque también puede estar presente en un delito que no tiene la tecnología ni como medio ni como fin; por ejemplo un homicidio: una llamada telefónica, un mensaje de texto, una notificación de WhatsApp, un correo electrónico, hacen necesaria la presencia de un especialista, que se acercará a esa información para saber cómo analizarla y que sea relevante para la investigación.

¿Qué es la inteligencia de fuentes abiertas?

La inteligencia de fuentes abiertas es una disciplina de la rama de la inteligencia, que tiene mejor relación costo – beneficio respecto de otras, como la de señales, fotografía o inteligencia humana. Se basa en realizar el análisis de cualquier fuente abierta de información. Esencialmente, esta disciplina tiene muchísimos años, siendo uno de los primeros registros en papel, como libros, publicaciones periodísticas, etc. Hoy toma otra relevancia, ya que Internet es la base de datos más grande e informal que existe. El análisis de fuentes abiertas de datos es transformar esa información, agregar nuevos datos no vistos o inferir información, garantizando que en ese proceso no se viole la garantía ni la integridad de ninguna persona, y se convierta en aporte para la investigación judicial.

¿Qué conocimientos mínimos resultan necesarios?

Las fuentes abiertas de datos es, en la jerga, "la frutal del árbol que más bajo cuelga". Es la información que más a mano uno puede tener. El conocimiento técnico no es complejo, pero el investigador o el analista deben tener dominio de las herramientas de acceso a internet, por ejemplo cómo funciona un buscador y un navegador, instalar aplicaciones y extensiones dentro de ese navegador, conocer los parámetros avanzados de búsqueda, entre otros. Es decir, debe contar con una metodología para contextualizar esa búsqueda, no diversificarse ni perderse en el mar de información, manejando algunas herramientas creadas con esos fines, pura y exclusivamente. De todas formas, existen algunas herramientas de mercado, gratuitas o pagas, que le pueden ahorrar al analista todo ese conocimiento técnico y brindarle directamente la información para realizar un análisis. Debe saber interpretar esa información, de dónde viene o ayudar a ampliar la información disponible en tal momento, relacionándola entre sí.

¿Qué dificultades de investigación y de prueba del delito puede presentar el cibercrimen?

Múltiples. Particularmente, los dos problemas o desafíos a resolver son diferentes. Uno es la evidencia digital y el tratamiento que se le da a la misma. La relatividad y fragilidad de la evidencia digital, tan simple de alterar, requiere tratamiento de un especialista, desde el

acceso (la escena del delito) hasta el final (la detención de su dueño); debe preservarla y autenticarla para garantizar la cadena de custodia y pueda ser presentada en la Corte. Hoy este tipo de perfil no abunda, es muy especifico y requiere de una actualización continua y de herramientas que en algunos casos, son costosas.

El otro problema está justamente en el tema de cómo hacer para identificar quién esta detrás de la maniobra delictiva cuando esto se produce a través de Internet. Sabemos que Internet no tiene fronteras, los delitos informáticos tampoco y hoy las mismas herramientas que nos garantizan privacidad a cualquiera de nosotros que hacemos buen uso de las redes, también le garantiza la privacidad y el anonimato a aquellos que no hacen buen uso de ellas. Muchas veces las técnicas de investigación tradicional que parten de una IP, para determinar la titularidad, termina llevándonos a caminos sin salidas, porque son IP que pertenecen a diferentes servicios que brindan anonimato; por ejemplo, TOR. Es una herramienta para que quien quiera proteger su privacidad, la proteja para bien; pero lamentablemente, quien la quiera usar para mal también la utiliza.

¿Cuáles son los límites de estas herramientas?

Las limitaciones geográficas no existen en Internet, tampoco las jurisdiccionales. El open source inteligence o fuentes abiertas de datos significa que la fuente se conserve disponible siempre y que pueda ser útil para la investigación. El único limite que tiene es la fuente de la cual se nutre; debe ser una fuente abierta de datos, de acceso público y que además, no tenga orígenes ilícitos (alguien en algún momento, robó y publicó en Internet). También puede partir de la propia información que tenga un organismo, ya que muchas veces se puede hacer el análisis de la información sobre los datos producidos dentro de la misma institución, con los cuales se puede realizar una correlación (bin data).