

FUNDAMENTOS DE LA INVESTIGACIÓN TECNOLÓGICA

No se puede abordar la problemática jurídica sobre la investigación tecnológica sin conocer los fundamentos técnicos del proceso de investigación, sin conocer el funcionamiento de internet.

Todo proceso de investigación, sea del ámbito que sea, tiene por objetivos la identificación y localización del delincuente, y el aseguramiento y presentación de las pruebas. No hay acción penal sin pruebas. Si el medio es el tecnológico, tanto la identificación como el aseguramiento de la prueba revisten unas características diferentes al resto de delitos, lo que han propiciado una técnica propia que se está sometiendo al debate jurídico.

La esencia de la investigación tecnológica se basa en la trazabilidad de las comunicaciones. Los delitos cometidos a través de las redes de comunicaciones, de Internet, tienen como elemento común el que se realizan a través de comunicaciones electrónicas. Se injuria a través de mensajes, se distribuye pornografía a través de mensajes, se ataca a un sistema a través de comunicaciones,... Y la única forma de investigar estos hechos es analizando las comunicaciones para determinar el punto origen de la comunicación, es decir, trazar la comunicación.

Esa trazabilidad de las comunicaciones es posible gracias al diseño de las redes de internet. Éstas se basan en distintos protocolos de comunicaciones, entre los que destacan los protocolos TCP/IP. La esencia de esos protocolos se resume en que cada equipo informático conectado a la red se identifica de forma unívoca mediante un identificador llamado número IP, y que toda comunicación que circula por la red, además del contenido del mensaje lleva datos adicionales al mensaje entre los que destacan el identificador del origen y del destino del mensaje y la fecha y hora de la emisión del mismo. A estos datos distintos de contenido del mensaje pero inherentes al mismo se le ha convenido en llamar datos de tráfico.

Estos datos son los que permiten trazar los mensajes para identificar el origen del mensaje, de forma que sin ellos, no es posible la investigación. Por tanto son datos que deben ser conservados y cedidos de forma eficiente para el buen fin de la investigación.

Tal como comentábamos, los datos de tráfico son inherentes a la comunicación y por tanto, en todos aquellos puntos por los que la comunicación pasa, pueden ser leídos y almacenados. La realidad es que solo lo van a almacenar, conservar, aquellos para los que resulten necesarios esos datos, aquellos puntos de la red cuya funcionalidad se puede ver afectada por el mal uso de las comunicaciones. Nos estamos refiriendo a los servidores de la red, todos aquellos equipos que prestan un servicio al resto de usuarios de la red.

Tanto la conservación como la cesión están reguladas por ley, En España disponemos de la ley 25/07 de Conservación de datos de comunicaciones electrónicas. Esta ley corresponde a la trasposición casi literal de una directiva europea. En ella, se establecen mediante una remisión a la Ley General de telecomunicaciones, quienes son los sujetos obligados a conservar los datos de tráfico. Esta remisión es muy deficiente toda vez que se limita el número de sujetos obligados a los Proveedores de acceso a Internet, olvidándose de los Prestadores de Servicios que previamente estaban regulados por la ley de servicios de la Sociedad de la Información, en su artículo 12, y que fue derogado por la referida ley 25/07. Y no solo es limitada en cuanto a los sujetos, sino

que además, la conservación la limita a delitos graves del código penal, con lo que se inhabilita la investigación para otros órdenes del derecho.

Pero hay otras normas que afectan a la conservación de los datos de tráfico. La Agencia Española de Protección de Datos ha definido el número IP como un dato de carácter personal, con lo que su conservación y tratamiento se ve afectada por la Ley de conservación de datos.

Por último, el legislador, ha introducido el último elemento de discordia en la conservación de los datos. Por ser inherentes a la comunicación, están afectados por los mismos derechos que ésta, el secreto de las comunicaciones, que exige unas determinadas garantías judiciales para su vulneración. De esta forma se ha llegado al contrasentido de que comunicaciones públicas de contenidos en la red, donde el contenido es público, los datos inherentes a ese contenido son privados y afectados por el secreto de las comunicaciones.

Esta protección de los datos de tráfico, lejos de ser la adecuada para su conservación, por las deficiencias u olvidos de determinados datos, resulta una traba para la agilidad de la investigación, convirtiéndose en una traba a la investigación. Se ha llegado a un procedimiento de cesión ineficiente muchas de las veces.

Pero obviemos la problemática de la conservación y cesión de los datos, y continuemos con el proceso de investigación. Tal como se ha comentado, los protocolos TCP/IP permiten la trazabilidad de las comunicaciones, es decir, determinar el punto origen de la comunicación. Identificar el equipo informático desde el que se ha iniciado la comunicación a través de la cual se ha cometido un delito. Pero detrás de la máquina, hay un usuario, autor del delito. Y el objeto de la investigación es la identificación de éste, no de la máquina. ¿Cómo se identifica al usuario? Pues no cabe otra solución que basarse en un conjunto de indicios que permitan concluir que el usuario identificado es el autor de los hechos investigados. Hay que establecer una vinculación entre equipo informático y usuario del mismo, y posteriormente encontrar los indicios que, valorados en su conjunto, conforme las leyes de la lógica y la experiencia, nos permitan concluir la autoría de los hechos investigados.

¿Dónde se localizan el conjunto de indicios? Además de los propios de la investigación técnica que ha permitido trazar comunicaciones hasta ese equipo, el resto, por lo general, se obtienen del propio equipo, de tal forma que resulta preciso el análisis técnico del equipo para poder obtener la prueba incriminatoria contra un determinado usuario de un equipo informático. Es decir, no hay incriminación posible sin incautación de equipo, sin registro domiciliario para intervenir el equipo informático.

Estas dos premisas, no hay investigación sin conservación de datos de tráfico, y sin registro domiciliario, serán el objeto de desarrollo de esta presentación.