



Medidas de investigación tecnológica

Jorge Bermúdez



De esto...



...a esto

Imagen: fotograma de "The Matrix" (Lilly y Lana Wachowski, 1999)

La gran asignatura pendiente del ordenamiento jurídico, la reforma procesal.

Tras el fallido Código Procesal Penal, tenemos la mayoría de sus disposiciones trasplantadas a la Ley Orgánica 13/2015, de 5 de octubre.

Principios: especialidad, idoneidad, excepcionalidad y necesidad.



Capítulo IV: Disposiciones comunes



“1.º La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.

2.º La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el artículo 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.

3.º Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida.

4.º La extensión de la medida con especificación de su contenido.

5.º La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.

6.º La forma de ejecución de la medida.

7.º La duración de la medida que se solicita.



Intervención de telecomunicaciones (Art. 588 Ter)



Imagen propiedad de "The Tech Journal"

- Comunicaciones "Telemáticas"
- Datos de contenido y metadatos
- Se acaba con la limitación de la ley 25/2007
- Catálogo de exigencias judiciales
- Se permite cruce de datos y "búsquedas inteligentes"
- Puede afectar a terceros
- IP: autorización judicial; teléfono: fiscal y policía judicial
- IMSI e IMEI: investigación de campo



Escuchas ambientales (Art. 588 quater)



Foto: Platon, publicada en "Wired" el 13 de junio de 2014

Aquí, lo más interesante es la reciente sentencia del Tribunal Supremo que valida las escuchas ambientales realizadas por teléfonos móviles incluso antes de descolgar la llamada, posibilidad técnica prevista en el sistema SITEL.

"1. Podrá autorizarse la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado, en la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados.

Los dispositivos de escucha y grabación podrán ser colocados tanto en el exterior como en el interior del domicilio o lugar cerrado.

2. En el supuesto en que fuera necesaria la entrada en el domicilio o en alguno de los espacios destinados al ejercicio de la privacidad, la resolución habilitante habrá de extender su motivación a la procedencia del acceso a dichos lugares.

3. La escucha y grabación de las conversaciones privadas se podrá complementar con la obtención de imágenes cuando expresamente lo autorice la resolución judicial que la acuerde.



Imagen, seguimiento y localización (Art. 588 quinques)



Imagen: fotograma de la película "Enemigo Público" (Enemy of the State, Tony Scott, 1998)

- Por CUALQUIER medio (¿incluye malware?)
- En exteriores (¿y el agente infiltrado?)
- Admite el GPS



Dispositivos de almacenamiento masivo de información (Art. 588 sexies)



- Se supera el anacronismo de papeles y documentos
- Se admite el “remote forensics”
- Resolución judicial motivada (¿incautación en plena calle? ¿jaula de Faraday?)
- Casos de urgencia: sin resolución
- Deber de colaboración



Deber de colaboración (Art. 588 sexies c], apartado 5º)



¿Algo así?

Imagen: fotograma de "La Jungla 4.0" (Live Free or Die Hard, Len Wiseman, 2007)

Las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia.



Registro remoto sobre equipos informáticos (Art. 588 septies)



“1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:”

Criminalidad organizada, terrorismo, menores, contra la Constitución y delitos informáticos.

Se debe precisar el qué, el cómo, por quién, la forma de hacer copias y las medidas de seguridad necesarias para evitar filtraciones o alteraciones fraudulentas.



“Troyanos policiales” y el poder de la nube



Imagen: fotograma de “Star Wars” (George Lucas, 1977)

- La utilización de los términos “datos de identificación y códigos” nos lleva a no ir al equipo local, sino a servicios en la nube.
- Esto se refuerza por el contenido del apartado 3º del 588 septies a).
- En realidad, el software de registro remoto puede ser un arma de un sólo disparo, por la virtualidad del principio de defensa y contradicción.
- Nuevamente, aparece el deber de colaboración de agentes externos.



Bonus track: el agente encubierto (Art. 282 bis. 6 y 7)





Muchas gracias por vuestra atención