IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas»

ARTÍCULO

La investigación policial en Internet: estructuras de cooperación internacional*

Antonio López

Fecha de presentación: mayo de 2007
Fecha de aceptación: junio de 2007
Fecha de publicación: septiembre 2007

Resumen
¿Cómo ha asumido la sociedad el fenómeno criminal en el entorno de las nuevas aplicaciones tecnológicas? ¿Cuáles son las contramedidas adoptadas por los poderes públicos sobre esta nueva realidad? El presente texto aborda ambas cuestiones tanto desde la praxis policial, cuanto desde las instituciones y foros de cooperación policial internacional, en especial los ficheros analíticos de Europol: las herramientas más sofisticadas de las que disponen las agencias de policía para la aproximación y tratamiento de esta nueva, y sin fronteras, fenomenología criminal.

Palabras clave
delincuencia informática, investigación policial, ciberinteligencia policial, cooperación policial internacional

Tema
Derecho penal y sociedad de la información

Police investigations on the Internet: structures for international cooperation

Abstract
How has society reacted to the criminal phenomenon within the area of new technological applications? What measures have been adopted by public authorities in regards to this new reality? This text addresses both questions through the police praxis as well as that of international police cooperation institutions and forums, especially the analytical files at Europol: the most sophisticated tools available to police agencies for addressing and dealing with this new, borderless criminal phenomenon.

* Texto adaptado por Jordi García Albero, profesor de los Estudios de Derecho y Ciencia Política de la UOC, a partir de la ponencia original presentada en el marco del III Congreso Internet, Derecho y Política, Barcelona, 2007.

Keywords
computer crime, police investigation, police cyber-intelligence, international police cooperation

Topic
Penal law and information society

1. Reproche penal versus reproche social. Sociedad del riesgo

Dentro de lo que genéricamente denominamos nuevas tecnologías, en especial Internet, amén de la aparición de nuevas acciones que se han reputado como penalmente típicas, (hacking, ataques DDoS,[1] etc.) y cuyo objeto es el control o la inhabilitación de una máquina dotada de un sistema informático y/o la información en ella contenida, existen multitud de viejas acciones criminales caracterizadas por nuevos *modi operandi*. Desde las injurias, calumnias y amenazas hasta las estafas; desde las infracciones contra los derechos de autor hasta la distribución de pornografía infantil; desde la apología del terrorismo hasta la negación del Holocausto. En algunos casos, estos bien conocidos delitos, evolucionados en su ejecución, no han supuesto más que un grado de sofisticación basado sobre todo en la inclusión del anonimato (tal es el caso de las injurias o amenazas); en otros, como en la pornografía infantil, la nueva dimensión que la Red les ha proporcionado ha transformado por completo su grado de peligrosidad y les ha conferido caracteres completamente novedosos.

¿Cómo ha asumido la sociedad el fenómeno criminal en este entorno de nuevas aplicaciones tecnológicas?

La respuesta requiere tomar prestado el concepto de sociedad del riesgo,[2] puesto que por él van a ser absorbidas buena parte de las amenazas ya descritas. Fenómenos como la propagación de código maligno (*viruses*) tipo gusano (no especialmente dañino), o las estafas, si lo son por una cantidad escasa, son ejemplos de acciones criminales que son asumidas por una buena parte de la población con una actitud que no suele ir más allá del mero fastidio, incluso en casos de victimación directa.[3]

1. El ataque DDoS consiste en dejar multitud de conexiones abiertas en el servidor, en espera de ser atendidas (SYN flood). El servidor reserva ciertos recursos de su sistema para atender a esas futuras conexiones, que nunca llegan a establecerse puesto que se refieren a direcciones que no existen. La máquina queda así sin recursos y deja de prestar servicio. Es como si llamáramos a una centralita telefónica y, una vez nos hubiera respondido un operador, le dijéramos «espere Ud. un momento, enseguida estoy con Ud.»; a continuación llamáramos a otro (o, más correctamente, otro socio lo hiciera desde otra línea) y repitiéramos la operación, reiterando el proceso hasta que la totalidad de los operadores quedaran con sus líneas abiertas esperando instrucciones que nunca llegarían. A las máquinas infectadas por el *malware* mencionado anteriormente se les conoce como máquinas *zombie*, y al conjunto de todas las que están a disposición de un atacante se le conoce como botnet (red de bots).
2. U. BECK(1998). *La sociedad del riesgo*. Barcelona: Paidós; M. CASTELLS (1999). *La era de la información. Economía, sociedad y cultura*. Madrid, Alianza editorial; y otros.
3. En 1999, muchos usuarios de Internet recibieron un mensaje de correo por el que se informaba de que «Gracias por haber adquirido nuestros productos. El cargo, por importe de (una cantidad entre 20.000 y 30.000 pesetas), ya ha sido procesado, y en breve será cargado en su cuenta. Si tiene alguna duda o reclamación, diríjase a nuestro departamento comercial, teléfono 90 3...». Tratándose de una compra inexistente, y siendo inminente el cargo en la cuenta bancaria, una gran mayoría de los que leyeron el mensaje se pusieron en contacto con el teléfono facilitado, que era de los de tarificación adicional y que mantenía la comunicación con la víctima hasta donde llegara su paciencia o su disponibilidad de tiempo libre. El coste de lo defraudado a cada víctima raramente llegaba a las cinco mil pesetas, cantidad que se daba por bien perdida a condición de asegurarse de que todo era una estafa y que, en realidad, nadie iba a pasar el cargo por un producto que nunca se había adquirido.

La percepción y valoración social del riesgo por parte de los responsables policiales está muy relacionada con el concepto de alarma social, fenómeno complejo, cuya evitación puede ser uno de los principales vectores de la acción policial en su conjunto.

Lo anterior merece reseñarse toda vez que, establecida una escala en cuyos extremos ubicáramos a los delincuentes que mayor y menor reproche social inspiran, ambos extremos estarían ocupados tal vez por actores propios del mundo de la «ciberdelincuencia». Así, en el extremo correspondiente al menor reproche podrían ubicarse los *piratas informáticos*,[4] mientras que a los distribuidores de pornografía infantil habría que reservar- nadie lo duda- el mayor grado de repulsa por parte del ente social.

1.1. Piratas informáticos

En la actualidad las acciones de los piratas informáticos han cambiado sustancialmente. A unas prácticas en las que los autores actuaban movidos por una suerte de inquietud intelectual por la vulnerabilidad de los sistemas informáticos, cuya calificación jurídica y posterior enjuiciamiento resultaba a veces algo comprometido si no díscolo, ha sobrevenido una realidad muy diversa: la de los denominados *hackers* al servicio de grupos de delincuencia organizada. Éstos han abandonado unos roles que en muchos casos sólo perseguían el simple reconocimiento, para ponerse a merced de grupos organizados que han sabido ver en sus habilidades un auténtico filón para explotar conjuntamente con sus estructuras criminales.

Es difícil determinar, en la actualidad, hasta qué punto ha variado la percepción social de estos *nuevos* piratas informáticos, más relacionados con las estafas y con la extorsión,[5] que con el «*hacking recreativo*».

1.2. Pornografía infantil

La persecución policial de la pornografía infantil por Internet se inició antes de que este tipo de conductas fueran criminalizadas. En efecto, con anterioridad a la modificación del Código penal sobre la materia,[6] los investigadores policiales no perseguíamos un objeto cuyo tráfico fuera ilícito (que no lo era), sino las pruebas materiales de un delito mucho más grave: la agresión sexual a menores. Y ése es el espíritu que debe continuar impulsando las actuaciones en contra de la pornografía infantil en Internet: la producción de ese material. Todo ello sin abandonar la persecución del «mero» tráfico, o incluso la tenencia de material pornográfico infantil, fundamentalmente, y en apretada síntesis, por tres poderosas razones: a) Los circuitos de pornografía infantil constituyen un monstruo que debe alimentarse constantemente con material nuevo,[7] es decir, que promueve las agresiones sexuales a menores. b) Los pedófilos son sujetos de indiscutible **interés policial**,[8] por lo que han de ser al menos

4. Por *piratas informáticos* quiere significarse un concepto vago pero muy extendido popularmente, que engloba a los *hackers*, *coders*, *crackers* (ingeniería inversa), e incluso a los que copian y distribuyen por Internet material sujeto a derechos de autor. Este término también tituló una película (1995) que contribuyó a popularizarlo y a asociarlo a las actividades características de *hacking*.
5. A finales del año 2006, agentes del Cuerpo Nacional de Policía detuvieron a un total de 23 personas entre Madrid y Cataluña, a quienes intervinieron, entre otros efectos, unas 1500 tarjetas de crédito clonadas. Las tarjetas, de una calidad nunca vista hasta entonces, incorporaban en sus bandas magnéticas los datos de entidades y ciudadanos de nacionalidad norteamericana. Estos datos habían sido almacenados en máquinas de comerciales norteamericanas que habían sido atacadas desde países del este de Europa. En este caso los *hackers* no se habían limitado a acceder al sistema y dejar pruebas de su vulnerabilidad, sino que habían obtenido los datos de las bandas magnéticas de las tarjetas de crédito, poniéndolos a disposición de la organización criminal que les contrató. Los paquetes de *dumps* – de este modo es como se conoce cada uno de los paquetes de datos magnéticos correspondiente a una tarjeta– así obtenidos son puestos en almoneda en determinados foros de Internet, o directamente explotados por éste u otro grupo criminal.
6. Operada por la Ley Orgánica 11/1999, de 30 de abril.
7. Véanse las teorías sobre la «caducidad» del poder erotógeno de la pornografía: Max TAYLOR; Ethel QUAYLE (2003). *Child pornography: an Internet crime*. Brunner-Routledge.
8. Por ejemplo, la detención de dos individuos en Barcelona y Valencia en marzo del 2007 por la **producción** de material pornográfico infantil y su distribución en Internet. Uno de ellos ya había sido detenido en el 2005 por distribución de pornografía infantil, pese a lo cual se dedicaba a «cuidar» menores en campamentos.
http://www.mir.es/DGRIS/Notas_Prensa/Policia/2007/np020402.html

identificados. c) La simple contemplación de una escena en la que aparece un menor vejado **perpetúa** la agresión contra su libertad y dignidad.

En la percepción social de este fenómeno tienen especial relevancia los medios de comunicación. Las grandes operaciones contra la pornografía infantil en Internet siempre son noticia, y los vectores que indican su importancia son invariablemente el número de detenidos y la edad mínima de los menores involucrados en las escenas. Otras consideraciones suelen ser irrelevantes. La sociedad considera peligrosa la pedofilia en sí misma, no admitiendo matices, de ahí que la repulsa social parifique conductas muy diversas: tanto da que se trate de quien elabora, quien distribuye o quien posee el material pornográfico.

La pornografía infantil no tiene su génesis en Internet, pero hay que reconocer que la red ha mutado por completo el fenómeno, haciéndolo mucho más pernicioso. La tecnología ha estado siempre especialmente unida a este tipo de agresión sexual al menor. Puede que el primer hito que le diera un nuevo impulso fuera el surgimiento de la fotografía y la cinematografía, que con toda probabilidad desplazaron al dibujo y la literatura obscenos. Las nuevas técnicas de producción de material pornográfico suponen y aportan, desde el punto de vista del consumidor, un grado de realismo hasta entonces desconocido, que trasciende a lo virtual e imaginativo.

Paralelamente, desde la óptica de la protección al menor, hay que señalar la trascendental circunstancia de que, contrariamente a lo que exige la producción de dibujo y literatura, la fotografía y la cinematografía sí requieren ineludiblemente la utilización de menores. Pero si este fue el primer hito tecnológico que revolucionó la pornografía infantil, el segundo, sin duda, ha sido Internet: **si el primero hizo inexcusable la participación del menor en la escena, el segundo ha promovido el surgimiento de la comunidad pedófila**.

En efecto, varias son las características de Internet que la configuran como un medio idóneo para los pedófilos. En primer lugar, facilita la transmisión de ficheros de un rincón a otro del Globo por un coste nimio; y, en segundo lugar, estas transacciones pueden realizarse desde identidades ficticias y de un modo más o menos anónimo, lo que indudablemente contribuye a debilitar los mecanismos de control, interiorizados o impuestos, que previenen la comisión del delito.

Pero si estos elementos son preocupantes por la mayor difusión de material pornográfico infantil que facilita la Red, lo más inquietante es que la misma posibilita la constitución de una comunidad pedófila. Así, frente a un individuo socialmente deprimido, marginado y acaso proclive a recibir terapia, emerge un *nuevo* pedófilo, miembro de una comunidad que le identifica, le refuerza y le asiste en su conducta desviada, proporcionándole no sólo el material gráfico o cualquier información necesaria para su propósito delictivo,[9] sino una razón de ser, e, incluso, la esperanza en un mundo posible en el que la pederastia tenga su cabida como una legítima opción sexual más. La publicación de argumentos y razonamientos a favor de la práctica del sexo con menores en los foros de estas comunidades se convierte en un bien tan preciado para el pedófilo como la propia pornografía infantil.

Así, el fenómeno de la pornografía infantil, considerado conjuntamente con el de las comunidades virtuales clandestinas, sí adquiere caracteres y consecuencias completamente nuevos, y requiere una consideración y tratamiento policial que necesariamente pasa por el uso de estructuras de cooperación internacional eficaces.

Paradójicamente, la proliferación de la pornografía infantil en la Red –utilizada como uno de los más poderosos argumentos por parte de los detractores de Internet– ha posibilitado la detención y posterior enjuiciamiento de agresores sexuales de menores que, en otro caso, hubieran podido permanecer ocultos mucho tiempo. Asimismo, gracias al descubrimiento y debate internacional de estas redes, muchos países han reformado sus cuerpos legales hasta ofrecer una homologada protección penal a los menores.

9. Ésta incluye desde cómo obtener sexo con menores hasta cómo prevenirse ante posibles investigaciones policiales, seguridad informática: anonimato, etc.

2. Más allá de la percepción social: la realidad de la amenaza

Un adecuado tratamiento profesional del fenómeno criminal en la Red exige conocer en qué consiste la verdadera amenaza, más allá de la mera percepción social y la alarma que pueda producir. Su determinación depende de un enfoque científico, metodológico y de ámbito internacional, que venga a determinar en forma de análisis estratégico cuáles son los elementos clave en los que deben centrarse los esfuerzos y cómo han de administrarse los recursos disponibles.

Los delitos investigados en el ámbito de Internet por las agencias policiales en todo el mundo recorren un abanico similar: pornografía infantil; fraudes (*phishing*, *pharming*, *vishing*, robos de identidad); terrorismo; tráfico de drogas (principalmente fármacos y drogas sintéticas); propiedad intelectual, etc.

¿Cuáles son las contramedidas adoptadas contra estas nuevas amenazas por los poderes públicos?

2.1. Creación de unidades de policía especializada

En 1995, el Cuerpo Nacional de Policía (CNP) creó el «Grupo de delitos informáticos» y en 1996 se estableció el «Grupo de delitos telemáticos» por parte de la Guardia Civil. Posteriormente, a medida que las policías autonómicas fueron asumiendo competencias, Mossos d'Esquadra, Ertzaina y Policía foral de Navarra crearon los suyos propios. Ubicados en sus estructuras centrales, estas unidades vienen haciéndose cargo de las investigaciones de relevancia e incluyen entre sus tareas las de asesoramiento, apoyo y/o coordinación a grupos periféricos en investigaciones de otro tipo, al menos en los casos de la Guardia Civil y el CNP. En este último, el modelo ha evolucionado con la creación de grupos especializados en su estructura periférica, con una dotación de personal, en algunos casos, de un rango similar a las unidades centrales y con una autonomía de actuación basada en el principio de subsidiariedad tan sólo limitada por una necesidad de coordinación especialmente significada[10] en las investigaciones por Internet.

Con carácter general, estas unidades policiales tienen un funcionamiento similar a las del resto de Policía Judicial;[11] si bien el resultado de su trabajo (informes, diligencias, cursos) requiere de una formación especial continua.

2.2. Establecimiento de un marco normativo adecuado

Varias son las especificidades que deben mencionarse aquí. Veamos:

a) El establecimiento de una legislación penal adecuada

El análisis de este apartado excede con mucho los propósitos de este trabajo, aunque el reconocimiento de acciones típicas entre la amplia e intrincada fenomeno-

10. La subsidiariedad constituye uno de los principios informadores de la estructura del CNP, por el que se persigue la descentralización para adaptarse a las necesidades específicas de los diversos ámbitos territoriales y lograr una mejor respuesta a las demandas de los ciudadanos. Por su parte, la coordinación, que genéricamente se refiere a las directrices de los órganos directivos superiores, a la evaluación de la actuación policial y a la inspección de los servicios, aquí tiene también un significado importante en cuanto a la competencia de la investigación dado que **los criterios de territorialidad suelen carecer de sentido en el momento de iniciarse la investigación**. De no existir herramientas eficientes de coordinación, los mismos hechos pueden ser investigados simultáneamente por varios grupos, por varios cuerpos policiales o, incluso, por varios países; y, desde luego, por varios juzgados: No conociéndose el lugar en el que se comete el hecho delictivo, resulta de aplicación el **artículo 15 de la LECr**: «*Cuando no conste el lugar en que se haya cometido una falta o delito, serán Jueces y Tribunales competentes en su caso para conocer de la causa o juicio: 1.- El del término municipal, partido o circunscripción en que se hayan descubierto pruebas materiales del delito; 2.- El del término municipal, partido o circunscripción, en que el presunto reo haya sido aprehendido; 3.- El de la residencia del reo presunto; 4.- **Cualquiera que hubiese tenido noticia del delito***». Esta cuarta opción es la que se da con mayor frecuencia. No tenemos más que imaginar que un nuevo sitio web con contenidos ilícitos es publicado en Internet, en foros de audiencia en español, y que es denunciado por cuantos usuarios se aperciben de su existencia. Tal vez convenga señalar que los gestos de sana competencia entre investigadores no debieran nunca llegar a perjudicar el resultado final de una operación, ni malgastar el erario público.
11. Con independencia de que otras unidades policiales hayan desarrollado grupos específicos para investigar en Internet las materias que les son propias, o que la Policía científica haya destinado buena parte de sus recursos a la informática forense, en la gran mayoría de los países europeos las unidades de *computer crime* se integran o asimilan a unidades de Policía judicial.

logía que Internet presenta es una de las principales tareas del investigador especializado, identificando nuevos *modi operandi*. El texto legal de referencia –El Código penal– se va modificando según las directrices de las instituciones europeas,[12] incorporando delitos nuevos o modificando los elementos de otros ya vigentes. Merece destacar la suscripción del Convenio de Cybercrime (Budapest, 23.XI.2001), por el que los países firmantes se comprometen, entre otras cosas, a incluir en su legislación penal una serie de conductas internacionalmente homologadas; base para satisfacer el principio de doble incriminación en los casos de auxilio judicial internacional.

b) La regulación administrativa del funcionamiento de los operadores de comunicaciones: en especial, el mantenimiento, conservación y tratamiento de los datos de tráfico de las mismas

La actitud de los investigadores policiales ante la retención de los datos del tráfico de las comunicaciones es fundamental, por cuanto debe entenderse que una limitación en los derechos fundamentales ha de estar debidamente justificada:

Si no existe retención de datos, no pueden investigarse los delitos en la Red.

La característica definitoria de Internet es el protocolo que le da nombre: *Internet Protocol*, siendo sus elementos individuales, las direcciones o números IP, elementos básicos de cualquier comunicación. Los **cuadernos de bitácora** en los que se registran las comunicaciones entre dos de estas direcciones son los llamados ficheros históricos o ficheros *log*. La llevanza de estos registros es automática y su conservación representa la única posibilidad de trazar *ex post facto* sucesos a nivel red. Los proveedores de servicios de Internet tienen la posibilidad de conservar unos ficheros históricos de especial relevancia: los que vinculan una dirección IP con un usuario (los que asocian la Red con el mundo real de los usuarios).

Se han defendido, sin embargo, otras actuaciones que se pretenden sustitutorias de la retención y que son mucho menos invasivas en el derecho fundamental de la privacidad, como el así denominado *quick freeze* –petición al proveedor de servicios concernido para que conserve unos determinados datos entretanto se obtiene la habilitación judicial necesaria. Esta práctica puede revelarse eficaz cuando existe un riesgo de eliminación de la información, en aquellos casos en los que, no estando regulado un periodo mínimo de conservación, puede presumirse que el proveedor va a proceder a su borrado; pero es obvio que carece de sentido si no existe un plazo de retención mínimo obligado. A mayor abundamiento, huelga sugerir el presumible comportamiento de administradores hostiles ante requerimientos tales, de no existir esta obligación general de conservación.

Se han postulado también técnicas de investigación basadas en la instalación discreta de dispositivos de *escucha*. Tales técnicas, eficaces en casos en los que existe ya un presunto autor, nada pueden aportar en el trazado *ex post facto* a nivel de red.

Como posteriormente se tratará, cualquiera de estas pesquisas policiales ha de ser habilitada judicialmente, lo que supone un trámite al que añadir el que se toma el propio proveedor de servicios para obtener y elaborar la información y respuesta, pudiéndose dilatar la averiguación de cada uno de estos escalones de trazado un plazo variable entre los diez días y varios meses, dependiendo del volumen de gestión y recursos del proveedor de servicios y la propia carga de trabajo del juzgado.

Hay otros niveles a investigar aparte del de red, pero la **comprobación de los hechos no puede obviar el enruta-**

12. Por ejemplo la DECISIÓN MARCO 2005/222/JAI DEL CONSEJO, en la que se inspira la modificación del artículo 197.3 del Código penal: «**El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo**, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo, será castigado con pena de prisión de seis meses a dos años». Sin embargo, el tipo aplicable como «intrusión», con anterioridad a la reforma –artículo 197.1– incluía un elemento subjetivo que dejaba sin efecto una alta proporción de accesos no autorizados: «*El que, **para descubrir los secretos o vulnerar la intimidad de otro**, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses*».

miento de las comunicaciones: Una investigación en la Red no puede prescindir del propio protocolo de Internet.

Puede argumentarse que existen técnicas y herramientas que pueden ser utilizadas por los delincuentes para obviar esta pesquisa de trazado, pero herramientas policiales como los ficheros analíticos –que más tarde se describirán– permiten ampliar enormemente el ámbito espacial y temporal de la investigación, de tal manera que habitualmente puede disponerse de un marco de referencia mucho más rico que la acción criminal propiamente dicha.

A partir de aquí corresponde a los poderes públicos evaluar la importancia de las investigaciones en Internet: hasta qué punto merece la pena menoscabar los derechos fundamentales de la privacidad y la intimidad en favor de la seguridad. El debate jurídico en el que se dilucida este asunto se sustenta en uno previo de naturaleza filosófica, social o antropológica, que afecta a la propia dialéctica de hombre individual-hombre colectivo, a la propia idea de persona, en el que todo el mundo está llamado a participar.

Personalmente, espero que los juristas sean capaces de regular con buena técnica la limitación de estos derechos fundamentales, facilitando la labor de los investigadores, la seguridad jurídica de los administradores de los proveedores de servicios, y la viabilidad comercial de sus empresas. No puedo compartir, sin embargo, el parecer de quienes identifican la retención como una práctica propia de un estado policial. Con toda honestidad, me cuesta imaginar indignación **por la retención de datos de tráfico, por un plazo de hasta doce meses, y a los que sólo se podrá acceder con habilitación judicial** cuando se analizan los hechos desde la práctica diaria y cotidiana de la limitación de los derechos. Una limitación de derechos que, en general, se admite con incomodidad (registro en el hotel; cacheos personales en el aeropuerto; revisión de bolsos y efectos personales; cámaras de vigilancia, etc.), pero que se asume e interioriza. Más bien parece que esta práctica de la retención es una mera actualización de las servidumbres que supone vivir en sociedades complejas. No faltará quien quiera ver en este incremento de las servidumbres un progresivo detrimento de los derechos individuales o de las libertades públicas, de tal manera que hoy preventivamente se guardan datos impregnados de intimidad que no se guardaban antes. Pero lo justo no es acumular un listado de cargos absolutos contra los estados e instituciones públicas, sino entenderlos en términos relativos o porcentuales, pues si bien la conservación de estas muestras impregnadas de intimidad representan una limitación en la privacidad de las personas, más cierto es que los miembros de estas sociedades modernas y desarrolladas hemos mejorado extraordinariamente las posibilidades de expresión y comunicación, así como la protección del individuo frente a los poderes públicos y la sociedad en general.

c) El carácter internacional *per se* de las acciones criminales llevadas a cabo a través de Internet

Todos los delitos relacionados con el crimen organizado tienen cierta proyección internacional. Las instituciones de cooperación policial internacional son cada vez más activas, sobre todo en el ámbito europeo, promoviendo foros de cooperación tanto a nivel estratégico como operativo. De tal proyección participan también los delitos cometidos a través de Internet, incluso más acusada, debido a su rápida evolución; pero al mencionar su carácter *per se* quiere significarse que no existe una diferencia esencial entre el uso de una máquina en Austria de una en Australia, es decir, que no existe ningún factor local de gran relevancia (salvo el del idioma). Así, el terreno de juego es el mundo entero, desvirtuando, en cierto modo, el principio de territorialidad del Derecho.

Siendo ésta una circunstancia de la mayor relevancia, su dimensión se hace más significativa si se tiene en cuenta su concurrencia con otra: la necesaria habilitación judicial desde las primeras fases de la investigación.

Metodológicamente, puede hablarse de una fase virtual de la investigación, que es la que conduciría hasta la máquina de la que partieron los hechos que la motivan. Esta fase muy pronto conduce hasta una dirección IP que, permítase la licencia de esta comparación, viene a ser la matrícula del vehículo desde el que supuestamente se ha cometido el hecho objeto de investigación. En este símil, la red pública de carreteras sería, naturalmente, Internet. Preguntémonos por las posibilidades a la hora de hacer uso de la misma con un vehículo:

- de nuestra propiedad;
- cuyo uso nos cede y asigna nuestra empresa;
- alquilado;
- taxi;
- robado;

- de un amigo;
- con placas robadas o falsas.[13]

Un vehículo de nuestra propiedad sería el equivalente a un acceso con IP contratada directamente por nosotros, adquiriendo el mismo rango que un proveedor de servicios. Si esta placa de matrícula es identificada en la comisión de una infracción, tan sólo ha de consultarse la base de datos de la Dirección General de Tráfico (DGT)[14] –o su equivalente en otro país– para saber quién es el propietario del vehículo y, en primera instancia, el infractor. Si accedemos con el vehículo que nuestra empresa nos ha asignado, nuestra IP será fija; pero en la base de datos de la DGT no constaremos como propietarios, sino nuestra empresa, que será la que tendrá que identificarnos ante la autoridad cuando para ello sea requerida: se corresponde con el caso –en nuestra comparación– de las IP fijas facilitadas por servicios ADSL. Si accedemos con un vehículo alquilado, estaríamos en el símil de acceso a través de una IP dinámica, típicamente un acceso telefónico o «dial-up», ya casi en desuso; o las que facilitan los proveedores de servicios de *cable* o, en general, los que utilicen servidores DHCP,[15] uno de los más extendidos. En este caso, un intermediario –el proveedor de servicios de Internet– ha adquirido un paquete de direcciones IP, que distribuye entre sus clientes, como la compañía de alquiler ha adquirido sus vehículos para alquilarlos entre sus clientes. La consulta a la base de datos de la DGT nos llevaría a la concreta compañía de alquiler de vehículos, que es la que consta como propietaria, y será necesario que ésta, a su vez, consulte en sus registros (en el símil estaríamos hablando de los registros de tráfico objeto de **retención**) para determinar a qué cliente concreto cedió un determinado vehículo en un determinado período de tiempo.

En el supuesto del taxi, se debería corresponder con un locutorio público o «cibercafé» dado que el taxista no registra la identidad del usuario de su servicio siendo –a los efectos que nos ocupan– el auténtico conductor del mismo, ya que es quien determina el destino (como tampoco el dueño del locutorio público registra a los clientes).

En el ejemplo del vehículo robado, en la actualidad se situaría en los accesos compartidos a Internet, típicamente corporativos, en los que tras identificarse ante el sistema con nombre de usuario y contraseña, se accede a la Red a través de un proxy: la averiguación del nombre de usuario y contraseña de otra persona y el uso del terminal usurpando sus credenciales, o el aprovechamiento de un descuido para controlar el ordenador con su conexión,[16] sería una casuística típica. Mucha más incidencia tiene, sin embargo, la interferencia de la señal de una red inalámbrica y su acceso a ella sin el conocimiento ni consentimiento de su legítimo titular.

Por otra parte, si la forma en la que accedemos a Internet fuera desde una conexión inalámbrica deliberadamente abierta (o con credenciales otorgados por su administrador), o si lo fuera desde una red corporativa haciendo uso de las credenciales de alguien que nos las cede voluntariamente, o de alguien que nos permite el uso de su equipo desde su propio domicilio, estaríamos en la correspondencia con el uso del vehículo de un amigo.

Por último, la última de las posibilidades que hemos relacionado, el acceso con un vehículo con una placa robada o falsa, se operaría mediante el uso de un troyano instalado subrepticiamente en la máquina de otro usuario, o del uso de un «proxy» para el que no estamos autorizados.

Pues bien, con excepción del primer caso, que no es más que una mera posibilidad teórica, en todos los demás es necesaria la habilitación judicial para obtener datos sobre el propietario del vehículo desde el que presuntamente se ha cometido el crimen.

Es decir, según este símil, lo que en el mundo real bastaría con una simple e inmediata consulta a la DGT, en las

13. En este caso, el símil contiene ciertas limitaciones: si bien a la red pública de carreteras se puede acceder TAMBIÉN con un vehículo sin placas, el acceso a Internet no es posible –por definición– sin una dirección IP.
14. En nuestro ejemplo, la base de datos de la DGT se corresponde con las de carácter público y abierto que relacionan rangos de IP con los proveedores de servicios que los gestionan: ARIN – Norte América www.arin.net; AfriNIC – África www.afrinic.net; APNIC – Asia – Pacífico www.apnic.net; LACNIC – América latina www.lacnic.net; RIPE - Europa, Medio oriente y Asia central www.ripe.net.
15. Dynamic Host Configuration Protocol.
16. Por ejemplo, ausentarse del lugar donde se halla el ordenador dejando la terminal sin bloquear.

investigaciones por Internet requiere necesariamente la previa obtención de un mandamiento judicial.[17]

La intervención judicial no se agota aquí, sino que se extiende a momentos posteriores en la investigación policial, siendo la más significativa, la entrada y registro en domicilio o lugar cerrado al objeto de la intervención y posterior análisis de los ordenadores desde los que se han cometido los hechos motivo de investigación. Éstas constituyen diligencias ineludibles,[18] cuya práctica, para que no quede desvirtuada, debe llevarse a cabo sin la prevención del presunto autor de los hechos. Así, el juez instructor debe decidir la proporcionalidad o desproporción entre la gravedad de los hechos investigados y la limitación de derechos solicitada: la entrada y registro en domicilio.[19]

En definitiva, puede concluirse que, desde los primeros estadios de la investigación, ésta debe ser tutelada por la autoridad judicial, habilitando la actuación de los policías mediante auto motivado en sucesivas ocasiones,[20] lo que seguiría siendo un problema asequible si el ámbito territorial se mantuviera en una misma jurisdicción; podría decirse incluso más: **seguiría siendo un problema asequible si se mantuviera en la jurisdicción nacional**.

3. Instituciones de cooperación policial internacional

Una de las primeras y más inmediata función de las organizaciones de cooperación policial internacional es la de actuar como canal de transmisión de las solicitudes de auxilio judicial internacional, cuando se opta por un canal policial por razones de urgencia, a saber: INTERPOL y EUROPOL.[21] Las razones de urgencia, si bien han de ser valoradas en última instancia por la autoridad judicial competente, tienen su origen en esta especialidad investigativa, en la gran volatilidad de los ficheros históricos de los proveedores de servicios. Sin embargo, en la mayoría de los casos, la información policial intercambiada entre agencias policiales de distintos países por canales oficiales puede recibir de las autoridades judiciales locales tanto valor como los informes de su propia policía. Las grandes operaciones internacionales se caracterizan porque concitan el interés directo de todos los países implicados, lo que trasciende al mero auxilio judicial.

3.1. La cooperación policial internacional actual en el ámbito de las investigaciones por Internet

La delincuencia en la Red ha evolucionado sobremanera desde las primeras operaciones internacionales. En materia de comunidades virtuales pedófilas, éstas son mucho más impenetrables, y sus miembros utilizan tecnología para la anonimización, la codificación y la eliminación de rastros que requieren otra estrategia de investigación, tal vez más a largo plazo. Las conexiones entre las redes de crimen organizado y los piratas informáticos configuran un tipo de delincuencia cuya respuesta policial es un continuo reto de actualización tecnológica.

17. Aclaremos que lo que tiene de adversativa esta proposición únicamente tiene que ver con la gestión y consumo de recursos por parte del investigador, requiriéndose, en muchas ocasiones, su personación ante la sede judicial.
18. Así lo previene el art. 282 de la Ley de Enjuiciamiento Criminal: «La Policía judicial tiene por objeto y será obligación de todos los que la componen, averiguar los delitos públicos que se cometieren en su territorio o demarcación; **practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la Autoridad Judicial**».
19. En ocasiones se han intentado otras medidas menos lesivas que la entrada y registro, con un resultado incierto; si bien la posibilidad de disponer de varias máquinas en el domicilio las hacen ya definitivamente ineficaces.
20. Podría llamar la atención que la tutela judicial en las fases tempranas de la investigación constituya un hecho excepcional; sin embargo, hasta que la comprobación del delito y el descubrimiento de los delincuentes adquiera un grado de maduración y concreción suficiente como para ser participado a la autoridad judicial, en otro tipo de delitos, pueden mediar multitud de gestiones de captación de inteligencia que pueden prolongarse mucho en el tiempo: *vigilancias, seguimientos, entrevistas...* Las investigaciones en Internet requieren un auto motivado por cada proveedor de servicios realmente implicado. Al final, también uno de entrada y registro.
21. El Convenio Europeo de asistencia judicial en materia penal (29 de mayo de 2000) establece en su artículo 6.4 que: «En caso de urgencia, las solicitudes de asistencia judicial podrán transmitirse por conducto de la Organización Internacional de Policía Criminal (INTERPOL) o de cualquier órgano competente según las disposiciones adoptadas en virtud del Tratado de la Unión Europea» (EUROPOL).

Con carácter general distinguimos tres vías de cooperación internacional policial:

a) Bilateral.[22] A través de los consejeros y agregados de Interior en las misiones diplomáticas permanentes del Reino de España. Este tipo de cooperación se caracteriza por:

- Utilización de las infraestructuras las misiones diplomáticas permanentes y personal orgánicamente adscrito a ellas.
- Comunicaciones personalizadas.
- Su operatividad merma con la aparición de terceros países.

b) Interpol. Sus principales finalidades son:

- Conseguir y desarrollar, dentro del marco de las leyes de los diferentes países y de la Declaración Universal de Derechos Humanos, la más amplia asistencia recíproca de las autoridades de policía criminal.
- Establecer y desarrollar todas las instituciones que puedan contribuir a la prevención y a la represión de las infracciones de derecho común.[23]

c) Europol. Cuyo objetivo se define como:

- Mejorar, en el marco de la cooperación entre los Estados Miembros de conformidad con el punto 9 del artículo K.1 del Tratado de la Unión Europea, la eficacia de los servicios competentes de los Estados Miembros y la cooperación entre los mismos con vistas a la prevención y lucha contra el terrorismo, el tráfico ilícito de estupefacientes y otras formas graves de delincuencia internacional, en la medida en que existan indicios concretos de una estructura delictiva organizada y que dos o más Estados Miembros se vean afectados por las formas de delincuencia antes mencionadas, de tal modo que, debido al alcance, gravedad y consecuencias de los actos delictivos, se requiera una actuación común de los Estados Miembros.
- Para alcanzar los objetivos definidos, Europol desempeñará prioritariamente las siguientes funciones:
  - Facilitar el intercambio de información entre los Estados Miembros.
  - Recoger, compilar y analizar informaciones y datos.
  - Comunicar sin demora a los servicios competentes de los Estados Miembros los datos que les afecten y la relación entre los actos delictivos de los que hayan tenido conocimiento.
  - Facilitar las investigaciones en los Estados Miembros transmitiendo a las unidades nacionales toda la información pertinente al respecto.
  - Gestionar sistemas informatizados de recogida de datos que contengan los datos previstos en los artículos 8, 10 y 11 del Convenio Europol (Sistema de Información de Europol y ficheros de trabajo con fines de análisis).[24]

3.2. Ficheros analíticos: una cuestión de inteligencia

El almacenamiento y tratamiento informático de datos de carácter personal requiere del establecimiento de un marco legal adecuado en términos de protección de datos.

Las unidades policiales nacionales de inteligencia criminal se rigen por sus respectivas legislaciones nacionales, por cuyo cumplimiento velan las autoridades nacionales correspondientes; en España en concreto, la Agencia de Protección de Datos.

En el ámbito europeo, esta labor de inteligencia en el ámbito del crimen organizado y su propio mandato la lleva a cabo EUROPOL, y el organismo encargado del cumplimiento de la normativa sobre protección de datos de carácter personal es el llamado Europol Joint Supervisory Body.[25] Los «recipientes» en los que esos datos son tratados son los *AWF* (*analysis work file*) o ficheros con fines de análisis. Estos ficheros analíticos

22. Regulada por Real Decreto 1300/2006, de 10 de noviembre sobre Organización y Funciones de las Consejerías de Interior en las Misiones Diplomáticas de España.
23. Artículo 2 del Estatuto de la INTERPOL.
24. Artículos 2.1 y 3.1 del Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una oficina europea de policía (**Convenio Europol**), hecho en Bruselas el 26 de julio de 1995.
25. http://europoljsb.consilium.europa.eu/.

son grandes bases de datos relacionales en los que se almacenan las contribuciones de inteligencia que realizan los Estados Miembros según un determinado criterio u orden de apertura. Los datos nuevos que se van incorporando son comparados con los ya existentes de todas las maneras posibles, incluyendo las técnicas de *data mining*.[26]

La aparición de *cruces* o *hits* da lugar a la elaboración de informes analíticos que incluyen hipótesis e *intelligence gaps* o *huecos de información,* sugiriéndose a la agencia policial que ha realizado la contribución o, en general, a todas las implicadas, que dirijan sus esfuerzos a resolver esas específicas incógnitas, materializándose de este modo casos concretos de la así llamada *intelligence-led policing*.[27]

Con esta poderosa herramienta puede decirse que el investigador ha conseguido trascender a dos principales limitaciones: aunar el mayor número de hechos semejantes que pudieran ser más o menos conexos, dando profundidad y perspectiva a los directamente investigados, y agotar todas la posibilidades de comparación entre ellos, más allá de los límites naturales de su retentiva e intuición. El fichero analítico de Europol es la respuesta policial natural a este tipo de criminalidad sin fronteras.

a) Fichero «Twins»

El fichero Twins tiene una especial preferencia por la comunidad pedófila que se expresa en inglés, aunque no excluye otras lenguas. Su propósito es apoyar a las autoridades competentes de los Estados Miembros, tal y como establece el Convenio de Europol, en la prevención y lucha contra las formas de criminalidad dentro del mandato de Europol asociadas con la actividad de redes criminales implicadas en la producción, venta o distribución de pornografía infantil y delitos asociados.

Caben aún un par de reflexiones sobre la propia pornografía infantil en el marco de las organizaciones policiales internacionales, que siquiera merecen mención.

- La primera tiene que ver con Interpol y con su base de datos de series de pornografía infantil, que contribuye de manera muy eficaz en la identificación de víctimas y agresores, dando continuidad en el mundo real a la virtualidad de los recursos gráficos distribuidos en la Red.

- La segunda se refiere de nuevo a Europol, que requiere de una definición más amplia que la que la circunscribe estrictamente al crimen organizado, en parte por esta especialidad delictiva de la distribución de pornografía infantil, cuya casuística en ocasiones no cumple con el requisito de delinquir con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material.[28] Parece que la competencia de Europol se va a dirigir más hacia la delincuencia grave transnacional que a las actuales organizaciones criminales.

b) Fichero «Terminal»

Su orden de apertura se dirige a los actos de *skimming* y *carding*.[29] Los múltiples datos que se deducen de intervenciones policiales en las que resultan detenidas personas portando tarjetas falsificadas, y el resultado de posteriores pesquisas constituyen paquetes de inteligencia idóneos para su inclusión en las bases de datos de Terminal. Los informes analíticos de este AWF están contribuyendo de manera determinante[30] a perfilar las redes de distribución de *dumps* y los flujos de capital en torno al *hacking*. Es decir, como ya se ha indicado, estas investigaciones policiales, que se refieren a hechos más o menos conectados en grandes espacios geográficos y temporales, no cuentan con una única fuente que pudiera haber burlado el trazado *ex post facto* a nivel de red, sino

26. Una actividad de extracción cuyo objetivo es descubrir hechos contenidos en las bases de datos.
27. http://www.fco.gov.uk/Files/kfile/Media%20brief%20-%20Intelligence-led%20policing%20annex.pdf.
28. Artículo 2.a de la Convención de las Naciones Unidas contra la delincuencia transnacional organizada, adoptada por la Asamblea General de las Naciones Unidas, el 15 de noviembre del 2000.
29. El *skimming* es el clonado ilícito de una tarjeta bancaria mediante la sustracción de la información contenida a través del copiado manual o electrónico de sus números (cuando se paga en comercios, restaurantes, etc.) o la instalación de dispositivos en cajeros automáticos que permiten realizar una copia de la banda magnética y la clave de acceso (generalmente mediante una cámara oculta). El *carding* se relaciona con el uso ilegítimo de tarjetas bancarias, principalmente en Internet.
30. http://www.europol.europa.eu/index.asp?page=news&news=pr070315.htm.

que en torno a estas transferencias de datos, que son clave, se circunscriben muchas otras, de muy variadas características técnicas y con una protección variable que pueden aportar inteligencia de gran valor analítico. El fichero Terminal procesaba a mediados del 2006 más de medio millón de entidades y más de 280.000 enlaces o relaciones; además, se beneficia especialmente de los acuerdos operativos suscritos por Europol con agencias policiales de EE. UU. y con Rusia, que permiten el intercambio de datos de carácter personal.

Conclusiones

La Red es una versión ampliada y mejorada del sistema nervioso de la Humanidad y sus nuevas posibilidades tienen que ver con su versatilidad y su interactividad. Esta nueva versión de las comunicaciones ha ampliado en la misma medida las posibilidades en cuanto a la comisión de actos criminales, tanto perfeccionando las herramientas y *modi operandi* para cometer los tipos delictivos bien conocidos, como haciendo surgir nuevos riesgos y amenazas: los que suponen la propia existencia de las máquinas que componen la Red.

La prevención y atenuación de esta faceta negativa de la Red, que puede afectar a la privacidad, seguridad, patrimonio e indemnidad sexual de sus usuarios y otras personas, requiere de contramedidas de concienciación, legislativas y de policía.

Las agencias de policía han evolucionado desarrollando unidades especiales cuyos miembros reciben formación permanente. Estas agencias de policía cooperan entre sí activamente, desarrollando herramientas conjuntas de inteligencia y análisis.

Así, a un fenómeno criminal que ignora las fronteras le ha de corresponder un tratamiento global, igualmente transparente al principio de territorialidad. Los *analysis work files* de Europol son el producto más elaborado para la coordinación de las investigaciones de esta comunidad policial internacional, y el que se está revelando como más eficiente contra este tipo de criminalidad.

Cita recomendada

LÓPEZ, Antonio (2007). «La investigación policial en Internet: estructuras de cooperación internacional». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 5. UOC. [Fecha de consulta: dd/mm/aa].

http://www.uoc.edu/idp/5/dt/esp/lopez.pdf

ISSN 1699-8154

Sobre el autor

Antonio López

Inspector del Cuerpo Nacional de Policía. Oficial de enlace en Europol. Spanish Desk