# "Análisis de la utilización de virus como diligencia de investigación en el Proyecto de Código Procesal Penal español"

Federico Bueno de Mata*

SUMARIO: I. Introducción: hacia un Gran Hermano mundial. II. Análisis de la regulación sobre utilización de troyanos con fines de investigación policial en el borrador de Código Procesal Penal Español. III. Reflexión final acerca de la idoneidad de la normativa en derecho español. Anexo: borrador Código Procesal Penal Español (Arts. 350 a 352).

**Resumen**

En este artículo analizamos la regulación otorgada en el proyecto de Código Procesal Penal español, aún pendiente de aprobación, acerca de la utilización de virus con fines investigativos. Para ello, reflexionaremos acerca de la idoneidad y necesidad de esta normativa para el esclarecimiento de determinados. Una regulación muy polémica que choca frontalmente contra una serie de derechos fundamentales y que hace qué debatamos sobre el nivel de control y espionaje que podemos llegar a sufrir por el Estado y plantearnos si realmente el fin siempre justifica los medios.

**Palabras clave**: Virus. Ciberdelitos. Policía. Proporcionalidad. Derechos fundamentales

**Abstract**

In this article we discuss the regulation given in the draft about the Spanish Code of Criminal Proceedings, pending approval, on the use of viruses for research purposes. To this end, we reflect on the necessity of this legislation to clarify certain acts. A very controversial regulation that clashes against a number of fundamental rights, and doing what we debate about the level of espionage can be suffered by the State and ask whether or not the end always justifies the means.

**Keywords**: Virus. Cybercrime. Police. Proporcionality. Fundamental Rights.

Recibido: 28/10/2014 • Aceptado: 30/11/2014

* Profesor Ayudante Doctor. Área de Derecho Procesal. Universidad de Salamanca. España.

## I. Introducción: hacia un Gran Hermano mundial

Podemos afirmar que George Orwell y su aclamado *Best-seller* "1984" tenían razón: vivimos en un Gran Hermano planetario. Hace poco más de un año, millones de ciudadanos de distintos puntos del planeta se conmocionaban al conocer la posibilidad de que muchas parcelas de su intimidad podrían haber sido violadas a través de PRISM, un programa secreto de vigilancia electrónica a cargo de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos de América, cuya confidencialidad saltó por los aires gracias a diversos datos filtrados a los periódicos *The Guardian* y *The Washington Post* por Edward Snowden[1], antiguo empleado de la Agencia Central de Inteligencia (CIA) y de la propia NSA. Desde ese momento, Snowden se ha convertido en un prófugo de la justicia estadounidense y continúa en paradero desconocido, aunque todo parece indicar que se encuentra en Rusia.

Pues bien, a partir de ese día sabemos que EE.UU. ha vulnerado constantemente los derechos fundamentales de millones de personas amparándose en sus propias leyes y obviando la jurisdicción de cualquier otro Estado del planeta Tierra, debido a que esta vigilancia tiene por objeto a personas no residentes en EE.UU. y el espectro de datos que controla es amplísimo: desde rastreo de direcciones IP hasta correos electrónicos, perfiles en redes sociales o transferencia de archivos[2].

Pensamos que esta impactante revelación, de la que muchos ingenieros informáticos siempre tuvieron sospecha, ha tenido un impacto triple en el resto de países. Por un lado, un retorno a una posición política de recelo ante la actuación del gigante americano, y por otro, el inicio de un cambio legal a nivel interno en el que muchos países están apostando por crear normativas encaminadas a favorecer el ciberespionaje y en fomentar el control ciudadano a través de técnicas más invasivas, ocasionando así un menoscabo de la libertad y la intimidad de sus ciudadanos. Por último, la sensación de oscurantismo y falta de ética trasladada a los justiciables de a pie ocasiona un evidente estado de desconfianza y genera una pregunta clara: ¿dónde está el límite?

Si estas reflexiones las trasladamos a un plano jurídico, el reto que debemos afrontar se basa en analizar las consecuencias legales que este acontecimiento puede conllevar y focalizar las distintas líneas rojas que dichos preceptos legales no pueden sobrepasar. De esta forma, si centramos nuestra atención en la

1 "Edward Snowden says motive behind leaks was to expose "surveillance state", *The Washington Post*, 9 de junio de 2013. Disponible en http://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html?tid=pm_politics_pop (Fecha de consulta: 19 de junio de 2014).

2 GREENWALD, G., "NSA collecting phone records of millions of Verizon customers daily". The Guardian, de 5 de junio de 2013. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (Fecha de consulta: 17 de junio de 2014).

normativa española vemos como existen nuevos proyectos de regulación procesal entre las que destaca por encima del resto el borrador del nuevo Código Procesal Penal (CPP), aún pendiente de aprobación[3].

Pues bien, si relacionamos directamente el tema del ciberesespionaje con el articulado de este futurible Código podemos ver cómo los artículos 350 a 352 del mismo contemplan una medida muy polémica, consistente en regular el *malware* y *spyware* como diligencia de investigación policial a través del uso de troyanos y distintos virus espía por parte de los Cuerpos y Fuerzas de Seguridad del Estado para perseguir distintos delitos producidos en Internet.

Muchos de los párrafos de su articulado responden a un contenido ambiguo y polémico que merece ser objeto de estudio y debate, pues debemos analizar hasta qué punto estas actuaciones, aunque gocen de autorización judicial para vulnerar distintos derechos fundamentales por razones de política criminal, podrían ser encuadrables o no dentro de lo que se denomina "*ethical hacking*[4]", ¿realmente todo vale? ¿el fin justifica los medios?, éstas y otras cuestiones serán analizadas a lo largo de este artículo desde un punto de vista procesal.

## II. Análisis de la regulación sobre utilización de troyanos con fines de investigación policial en el borrador de Código Procesal Penal Español

A continuación vamos a realizar un análisis de los artículos 350 a 352 del futurible Código Procesal Penal (CPP), en los que se regula la utilización de virus con fines de investigación policial, al tiempo que iremos focalizando las sombras que surgen de su lectura e interpretación, para a su vez intentar dar algo de luz a tan polémico asunto. Para una lectura más ágil, adjuntamos como anexo a esta ponencia el contenido íntegro de los artículos objeto de estudio.

Así, siguiendo un orden cronológico empezaremos por desgranar el primer punto del artículo 350 en el que se regulan los presupuestos para adoptar esta medida. En estas primeras líneas podemos ver como el CPP, tal y como regula anteriormente, confía la instrucción del caso al Ministerio Fiscal, quién deberá "pedir razonadamente" al Tribunal de Garantías la autorización de la medida, por lo tanto será éste último el órgano encargado únicamente de supervisar y cerciorar la idoneidad de las medidas a utilizar. Posteriormente al hablar de forma abstracta de "instalación de software" para el manejo remoto del equipo vemos como no cierra de forma concreta la modalidad de virus a usar por la

3 Texto íntegro del Borrador del Código Procesal Penal disponible en: http://www.fiscal.es/cs/Satellite?c=FG_Multimedia_FA&cid=1247141143692&pagename=PFiscal%2FFG_Multimedia_FA%2FFGE_fckDescarga (Fecha de consulta: 2 de abril de 2014).

4 REYES PLATA, A., "Ethical Hacking", Subdirección de Seguridad de la Información/ UNAM-CERT, disponible en http://www.seguridad.unam.mx/ (Fecha de consulta: 22 de junio de 2014). También definiciones y principios en http://www.ethicalhacking.com/ (Fecha de consulta: 17 de junio de 2014).

policía judicial, por lo que deja en el aire la naturaleza maliciosa del virus informático, aunque al hacer referencia al control y manejo remoto todo nos lleva a pesar que se trata de un *spyware* de naturaleza *zombie*[5].

En primer lugar, debemos manifestar que partimos de un sin sentido, al pensar que hacer público un artículo que podría posteriormente materializarse en un protocolo de investigación concreto e interno de los Cuerpos y Fuerzas de Seguridad del Estado (CFSE) no deja de ser un error, si el objetivo del texto es atajar conductas criminales de "verdaderos expertos en ciberdelincuencia"…Realmente, pensamos que esta normativa, tal y como está redactada, únicamente valdría para detener e incriminar a personas que tengan un control de las TICs medio-bajo, a lo que si a esto le sumamos que, como veremos posteriormente, se podría usar esta medida para ciberdelitos dolosos mayores a 3 años y que el nuevo Código Penal español penará la exportación de *links* o la bajada de contenidos y el "mercadeo" *P2P* en ordenadores situados en España…es realmente el usuario medio el que estaría en el punto de mira.

Igualmente, partimos de que el articulado es innecesario según el enfoque que se ha dado porque ya existen otras medidas que se podrían potenciar y que no dejan de ser menos invasivas y técnicamente menos complejas que el uso de virus espía, tales como la intervención de las comunicaciones, los ciberrastreos o la figura del agente encubierto en Internet. Igualmente, dada la publicidad del borrador del CPP, las personas que se dedican a cometer delitos en la Red a gran escala se pondrán aún más sobre aviso, brindándoles un tiempo que a nivel tecnológico es inmenso y teniendo así la reforma un efecto contraproductivo.

De nuevo la justicia avanza mucho más lenta que la tecnología, y la publicación de este tipo de articulado no deja de constituir una especie de alarma para las personas que se dedican a cometer este tipo de actividades ilícitas a través de la Red. Creemos que el legislador se ha dejado llevar por la imagen idealizada[6] que el ciudadano de a pie tiene de los *hackers*…es decir, asociamos la idea del hacker con una persona solitaria y hermética que se dedica a buscar retos informáticos que superar, cuando realmente dos de los tres ejes de delitos que abarca el borrador del CPP suelen estar perpetrados en su mayoría por grupos criminales coordinados a lo largo de varios países.

Por ello, tenemos que pensar realmente en el caso de que alguien con conocimientos técnicos avanzados, es decir algún ingeniero informático, leyera

5 Vid. VELASCO NUÑEZ, E., *Delitos cometidos a través de Internet. Cuestiones procesales*, Madrid, 2010, págs. 131-137, explica lo que significa un virus con naturaleza *zombie*, en el que infectas a un terminal y puedes usarlo a tu antojo sin que la persona propietaria del mismo perciba ningún cambio.

6 Vid. "Jueces hackers: el nuevo Código Procesal Penal podría permitir que se pirateen móviles y ordenadores", Diario Crítico, Edición del 4 de junio de 2014, disponible en: http://www.diariocritico.com/nacional/troyano/pirateria/codigo-procesal-penal/436117 (Fecha de consulta: 11 de junio de 2014).

el artículo. Sin duda el profesional se pondría rápidamente en la posición de *hacker* y pensaría la forma de eludir el ataque de este tipo de virus.

Normalmente las personas que realicen este tipo de delitos a gran escala no usan su ordenador personal e incluso suelen optar ellos mismos por controlar de forma remota otro tipo de terminales[7] a través de la inclusión de *malware* en diversos equipos informáticos con el fin de crear una red *zombie* de ordenadores y un ejército de *bots* que consumen la acción y así preservar su anonimato…aún así, si esto posteriormente se demuestra mediante un perito informático veríamos como no existiría dolo en este tipo de actuaciones y su conducta podría quedar impune. Todo ello, eso sí, al margen de que los potenciales ciberdelincuentes fabriquen nuevos virus autónomos para atacar distintos bienes jurídicos a distintas escalas: desde arremeter contra cuestiones personales de usuarios hasta llegar a desmantelar la seguridad y la infraestructura del propio Estado.

Una vez expuestas nuestras dudas sobre el enfoque del texto debemos analizar si realmente esta medida es, tal y como reza el texto "*idónea y necesaria para el esclarecimiento del hecho investigado*". Todo eso dependerá de qué hechos queremos investigar con esta medida.

Pues bien, en este caso el texto ve oportuno la utilización de esta medida para tres tipos de delitos para los que realmente existen otras medidas menos invasivas para los derechos fundamentales ya reguladas en España dentro del espectro de técnicas de interceptación de comunicaciones. Igualmente, los delitos deben ser dolosos y el catálogo contemplado sería el siguiente: ciberdelitos con pena de privación de libertad superior a 3 años, infracciones cometidas en Internet a gran escala que afecten a bienes jurídicos concretos como el *grooming*, el *cyberbullying* o el *phishing* y por último, ciberdelitos realizados por organizaciones criminales encaminadas a poner en peligro las infraestructuras tecnológicas del Estado, es decir, ciberterrorismo.

Así las cosas, ¿estamos ante una normativa correcta o realmente deberíamos abogar por una modificación del articulado antes de que el mismo entre en vigor? Claramente optamos por esta segunda opción con una premisa clara: debemos prestar atención a figuras ya contempladas en nuestro derecho interno y al mismo tiempo hacia la Unión Europea para solucionar este tipo de situaciones, al poseer muchas de ellas un alto componente transfronterizo, por todo ello, pasamos a exponer a continuación los razonamientos que nos llevan a sostener esta postura.

De esta forma, si el CPP siguiera adelante y utilizásemos la inclusión de troyanos para investigar ciberdelitos dolosos con pena de privación de libertad superior a 3 años, estaríamos ante una técnica excesivamente invasiva, más

7 Así lo expone también RUIZ HERVÁS, Y., "Troyanos para la investigación policial: el fin no justifica los medios", *El Diario.es*, número del 6 de junio de 2014, http://www.eldiario.es/zonacritica/Troyanos-investigacion-policial-justifica-medios_6_140395962.html (Fecha de consulta: 23 de julio de 2014).

aún cuando el proyecto de Código Penal español prevé penas superiores a tres años para cuestiones de redirección de *links* o descargas de música. Por ello, insistimos es que esta medida acabaría atacando prioritariamente al usuario medio y nos podría llevar a casos en los que un ordenador familiar, utilizado por varios miembros de la familia, podría ser investigado de forma remota e integral, vulnerando la intimidad del resto de usuarios, hayan realizado esas descargas o no[8].

Por todo ello proponemos para este primer punto una intervención que responda a los principios de proporcionalidad y necesidad a través de la regulación genérica ya establecida para la "interceptación de comunicaciones" a través del polémico programa SITEL (Sistema Integrado de Interceptación Telefónica), utilizado por los CFSE.

En España, la intervención de las comunicaciones consiste en la restricción del derecho fundamental al secreto de las comunicaciones contenido en el art. 18.3 de la Constitución[9], efectuada por una resolución judicial motivada. En este sentido, la problemática procesal que plantea la interceptación de esta figura en España es triple, por un lado los problemas de competencia territorial, en segundo lugar el fenómeno de la interceptación de esta figura y por otro los problemas de autoría y recepción[10].

En el orden jurisdiccional penal, las infracciones penales producidas a través de comunicaciones electrónicas desde distintos dispositivos plantean la situación de que, en muchas ocasiones, entre el lugar en el que el sujeto ejecuta el comando que activa el programa y el lugar en el que se produce la ofensa al bien jurídico exista, una notable distancia geográfica, posibilitando así que el resultado ofensivo al bien jurídico no se produzca en un único lugar[11]. Por tanto necesitaríamos una reforma con carácter previo a la solución acerca de qué órgano judicial ha de asumir el conocimiento de un determinado asunto resulta obligado ver si el hecho debe entenderse ejecutado o no en los límites de la jurisdicción española siendo partidarios de la teoría que dice que el delito sería cometido en todas las jurisdicciones y que por tanto cualquiera de los órganos jurisdiccionales tendría competencia en el asunto[12].

8 En este sentido también se manifiesta TEJERINA, O., Defensora del Internauta en España en el artículo publicado en http://www.internautas.org/html/7604.html (Fecha de consulta: 19 de julio de 2014).

9 GIMENO SENDRA "La intervención de las comunicaciones" *Diario La Ley, Nº 7192*, Sección Doctrina, 9 Jun. 2009, Año XXX, Ref. D-210, Editorial LA LEY.

10 BUENO DE MATA, F. "La interceptación de los e-mails", *Revista Justicia*, 2009, págs. 5 y ss.

11 MARCHENA GÓMEZ, M. "Dimensión jurídico-penal del correo electrónico", Diario La Ley Nº 6475, 4 de Mayo de 2006, págs. 15 y ss.

12 La Sala Segunda del Tribunal Supremo, en su Acuerdo de pleno no jurisdiccional, Sala General, fechado el día 3 de marzo de 2005, proclamó que "*el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de*

Del mismo modo, tampoco existe una regulación sobre los datos externos de los correos electrónicos, la custodia y destrucción de los soportes magnéticos o telemáticos, el valor probatorio de la prueba inconstitucionalmente obtenida en estos casos específicos, regulación para las personas jurídicas, la ausencia del tiempo máximo de intervención[13] o una regulación específica para el programa espía utilizado por la policía judicial: SITEL[14]. Por lo que realmente sería mucho más efectivo solucionar todas estas lagunas en el próximo CPP antes de apostar por una normativa nueva.

Por supuesto, no podemos confundir SITEL con otras herramientas conocidas a nivel mundial como PRISM, pues su alcance y objeto de actuación es muy reducido, al interceptar únicamente comunicaciones electrónicas dentro de la extensión y límites territoriales establecidos para la jurisdicción española. En referencia a la laguna legal que plantea su uso, se puede constatar por declaraciones políticas que el programa nació en 2001 y no fue hasta la ley ordinaria 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (LCDCE), cuando obtuvo un manto legal tardío e insuficiente. En este sentido, la regulación se debería dar siempre por una ley orgánica, es decir por mayoría absoluta, y no una ley ordinaria, al limitar derechos fundamentales.

En segundo lugar, sobre los temas que afectan a bienes jurídicos especialmente protegidos como es la distribución de imágenes pornográficas de menores de edad o las estafas a gran escala en el comercio electrónico, creemos que también existen medidas más efectivas ya contempladas cuando el sistema informático se encuentre situado en territorio sobre el que se extienda la jurisdicción española.

Por un lado, en primer lugar para los delitos de *grooming* o *cyberbullying*, tal y como llevamos apostando años atrás[15], pensamos que la potenciación de

*cualquiera de ellas que primero haya iniciado las actuaciones procesales será en principio competente para la instrucción de la causa"* La solución propugnada permite optar por el doble criterio de ubicuidad, entre el lugar de ejecución y el lugar de resultado.

13 Como referencia citar que de conformidad con lo dispuesto en el art. 579.3 el plazo de duración de las intervenciones telefónicas, salvo solicitud de prórroga, no puede ser superior a tres meses.

14 Vid. Para profundizar más sobre SITEL y la interceptación de las comunicaciones BUENO DE MATA, F., MARTÍN RUANI, H. y VARGAS BASILIO, A., "Interceptación y monitoreo de correo electrónico", *Diario El Dial*, 2012, págs. 4 y ss.

15 BUENO DE MATA, F., "El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia", *Los retos del Poder Judicial ante la sociedad globalizada. Actas del IV Congreso Gallego de Derecho Procesal (I Internacional) A Coruña, 2 y 3 de junio de 2011,* PÉREZ-CRUZ MARTÍN, A. (dir.), FERREIRO BAAMONDE, X. (dir). A Coruña: Universidade, 2012, págs. 295-306. Los "ciberrastreos" estaban pensados para investigar intercambio de archivos en redes P2P, como *Emule*, *Kaaza* o *Elephant*, pero ahora necesitamos otro tipo de investigación más personal y directa, valiéndonos de las ventajas aportadas por la figura de los agentes encubiertos en Internet

la figura del agente encubierto en Internet se vuelve algo preceptivo e imprescindible a nivel nacional.

La figura del agente encubierto para infiltraciones en terrenos físicos, encuentra su regulación en el art. 282 bis LECrim, gracias a una reforma de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la actividad investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves, efectuada por Ley Orgánica 5/ 1999, de 13 de enero. El problema es que dicho artículo establece un *numerus clausus*[16] o enumeración tasada de delitos para su uso, lo que impediría su uso en delitos cometidos en la Red. Aún así, a finales del mes de marzo de 2011 el Senado aprobó regular la figura del agente policial encubierto en Internet en investigaciones contra la pornografía infantil y la pedofilia[17].

Por todo ello, con el avance constante que tiene la tecnología, consideramos un error realizar una lista tasada de delitos a los que hacer frente con esta figura y nos decantaríamos más por establecer aquí un sistema de *numerus apertus* basado en categorías de delitos y no en figuras concretas; por lo que estaríamos hablando siempre de "compartimentos abiertos", para evitar de este modo clasificaciones a que queden rápidamente desfasadas. Así, si extrapolamos el concepto del agente encubierto en el terreno físico y lo llevamos al plano virtual, podríamos definir al agente encubierto en Internet como un empleado o funcionario público[18] que, voluntariamente, y por decisión de una autoridad judicial, se infiltra en la Red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de la Red, que causen una gran repulsa y alarma a nivel social. Cuestiones distinta sería valorar, al igual que con los virus, la técnica basada en el engaño y en la ocultación de la verdadera identidad con fines de investigación…una cuestión de *ethical hacking* que creemos plenamente justificada por la naturaleza concreta del delito a investigar y el bien jurídico lesionado relacionado con personas especialmente vulnerables como los menores de edad.

Ahora bien, dentro de este mismo segundo bloque, cuando los delitos anteriores adquieren el carácter de transfronterizos, al conllevar por su propia naturaleza una gran distancia geográfica entre el lugar de comisión y el lugar de lesión como en los casos de *phising*; optaríamos por redirigir la investigación a nivel europeo gracias al nuevo Centro Europeo Contra el Cibercrimen[19], EC3,

16 Vid. RIFÁ SOLER, J. M., se cuestiona si el listado recoge *numerus apertus o clausus*, en "El agente encubierto o infiltrado en la nueva regulación de la LECrim.", *Poder Judicial*, núm. 55, pág. 161; nosotros entendemos que con la actual redacción es una lista cerrada y tasada.

17 Vid. http://www.tecnoupdate.com.ar/2011/03/21/espana-agentes-encubiertos-en-internet-contra-la-pedofilia/ (Fecha de consulta: 13 de Abril de 2011).

18 BUENO DE MATA, F., "Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿Deberían ampliarse las actuales funciones del agente encubierto en Internet?", *El proceso penal en la sociedad de la información: Las nuevas tecnologías para investigar probar el delito*, coord. PÉREZ GIL, J., Madrid, 2012, págs. 311 y ss.

19 Vid. https://www.europol.europa.eu/ec3 (Fecha de consulta: 3 de abril de 2014)

con sede en la Haya y que empezará a funcionar en enero de 2015 siendo dirigido por la Oficina Europea de Policía, Europol. Ahora bien, hemos de reconocer que el articulado sí contempla el recurso a los mecanismos de cooperación internacional cuando los equipos no se encuentren en España al regular que *"se instarán las medidas de cooperación judicial internacional en los términos establecidos por la Ley, los Tratados y Convenios internacionales aplicables y el derecho de la Unión Europea"*, pero pensamos que debe ser a la inversa, un texto europeo que se transpusiera a la normativa interna de los Estados.

¿Qué nos lleva recurrir a este nuevo instrumento de cooperación judicial internacional? Al encontrarnos ante delitos con un gran carácter transfronterizo y analizando el carácter bipolar de la norma española, ya que por un lado se configura como un método excesivamente lesivo para los derechos fundamentales de los potenciales investigados por un lado, pero que acota la investigación únicamente a terminales que se encuentre en territorio español por otro; pensamos que para detener las acciones delictivas a gran escala es necesario que la Comisión Europea colabore para poder ampliar la capacidad analítica y operacional en investigaciones de este tipo. En este sentido, el EC3 nace con la idea de constituir un instrumento de coordinación en el terreno de los delitos informáticos y como centro de apoyo operativo y de investigación forense a nivel europeo[20], puesto que la lesión de bienes jurídicos en ciberdelitos de tal magnitud puede producirse en multitud de Estados miembros, con distintas jurisdicciones y normativas internas que pueden obstaculizar la investigación y posterior detención de los presuntos autores.

Según sus propios promotores, el EC3 proporcionará soporte operacional a los países de la UE, dando un mayor acceso a la experiencia técnica en las investigaciones conjuntas y podrá así fomentar la puesta en común de recursos de cada Estado miembro en la prevención del cibercrimen, ésta será la única manera de desmantelar redes organizadas de este tipo, gracias a una estructura europea capaz de atajar un problema de tal envergadura.

Pues bien, tras analizar los dos primeros bloques para los que está destinada la futura normativa, solo nos atreveríamos a preservar el precepto, tras una oportuna y detallada regulación mucho más específica garantista, su aplicación en casos de ciberterrorismo tal y como pretendió en su día hacer Alemania, ya que posteriormente el Tribunal Constitucional alemán declaró inconstitucional la norma, al considerarla, tal como apunta ORTIZ PRADILLO, contraria *"al derecho fundamental a la garantía de confidencialidad e integridad de los equipos informáticos"*[21]. Únicamente apostaríamos por su mantenimiento,

20 Vid. https://www.europol.europa.eu/ec3/infographic (Fecha de consulta: 5 de abril de 2014)

21 ORTIZ PRADILLO, J. lo apunta en un artículo con gran impacto, "La policía podrá usar troyanos para investigar ordenadores y tabletas", *periódico El País*, de 3 de junio de 2014,

al ser un problema nacional ante el que la población española está especialmente sensibilizada, siempre que la misma fuera fruto de una transposición de una Directiva europea a derecho interno, pues insistimos en que estos problemas se deben resolver, dada a su trascendencia desde un punto de vista normativo e institucional superior.

En este sentido, al igual que la tecnología evoluciona de una forma vertiginosa, la capacidad de adaptación por parte de las bandas terroristas es vertiginosa. El uso de las nuevas tecnologías como instrumento para cometer atentados y como elemento de ataque es una realidad inminente con una enorme proyección de futuro, ya que, por un lado los ataques crecen desmesuradamente año a año y sus autores, en la mayor parte de los casos, son personas jóvenes con gran poder de amoldarse a los cambios tecnológicos, lo que aviva el peligro[22].

Consideraríamos actos propios de ciberterrorismo[23] el uso de las TICs como acción del delito y no como instrumento o elemento de apoyo a una infraestructura criminal. Por tanto, esta convergencia del ciberespacio con el terrorismo podría ser definida como el ataque premeditado y políticamente motivado contra información, sistemas, programas y datos informatizados relativos a la integridad y la seguridad del Estado por parte de grupos terroristas. En conclusión, optaríamos por abogar igualmente por una normativa europea para el ciberterrorismo a nivel internacional.

Por último, debemos hacer una referencia a una parte concreta del articulado centrado en los deberes de colaboración de entidades personas externas que se regulan en los artículos 351 y 352.

Así, en el artículo 351 vemos como existe una obligación por parte de los proveedores de acceso o servicios telemáticos y los titulares o responsables del sistema informático a facilitar los datos e información recogidos en su sistema que puedan ser objeto de examen y visualización. Cuestión plenamente razonable, y que compartimos, siempre que se actúe caso por caso y no se deje abierta la puerta a un filtrado de información periódica, pues entonces estaríamos repitiendo a pequeña escala el caso de la NSA.

Pero la polémica se suscita con la llegada del art. 352. 2 al regular que *"Las autoridades y los 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*

disponible en http://sociedad.elpais.com/sociedad/2013/06/03/actualidad/1370289646_865495.html (Fecha de consulta: 3 de junio de 2014).

22 VELASCO NÚÑEZ, E. "Aspectos procesales de la investigación y de la defensa en los delitos informáticos", *La Ley*: *Revista jurídica española de doctrina, jurisprudencia y bibliografía*, ISSN 0211-2744, Nº 3, 2006, págs. 1857-1864.

23 Vid. BUENO DE MATA, F. "Ciberterrorismo: tratamiento procesal y penal del terrorismo del futuro", Estudios actuales en Derecho y ciencia política, coord. CARRIZO GONZÁLEZ-CASTELL, A., 2013, págs. 313-323

*en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia"*. Lo que nos transporta a una situación en la que todo está permitido, un "todo vale" para que la diligencia acabe bien y en el que se ve claramente que el fin justifica los medios, ya que con la denominación "cualquier persona" se desprenden dos efectos negativos inmediatos. En primer lugar, se desvalora o se reconoce como insuficiente la capacitación técnica de la policía judicial en términos de investigación policial, cuando existen unidades concretas con miembros con años de especialización que han sido formados para tal fin y están en constante reciclaje y capacitación, por lo que a nivel publicitario y de imagen exterior no creemos que nos haga ningún bien y, en segundo lugar, ¿qué perfil tiene esa persona? Al hablarse de un cualquier no se acota la identidad de ese sujeto, ¿se está hablando de un ingeniero informático profesional? O por el contrario ¿se abre la puerta al fichaje de *hackers* que actúen sin fines éticos e incluso criminales? Preguntas retóricas que a todas luces hacen urgente la clarificación de este apartado si la norma llegara a entrar en vigor.

## III. Reflexión final acerca de la idoneidad de la normativa en derecho español

Debemos dejar claro que partimos de un futurible, un Código Procesal Penal que si tenemos en cuenta la fecha en la que nos encontramos, y a sabiendas de que las próximas elecciones serán a finales del 2015, puede que no cumpla con los plazos de tramitación parlamentaria, a no ser que se opte por introducir reformas parciales que gocen de trámites más ágiles y tengan por objeto la regulación de esta diligencia de investigación.

Al margen del tema temporal y centrándonos en el análisis del borrador, vemos como por todo lo expuesto anteriormente, queda claro que no compartimos la redacción de los artículos 250 a 252 del CPP, ya que como hemos advertido, parte de un planteamiento desafortunado al ir enfocado a perfiles y tipos penales heterogéneos con un campo de actuación geográfico limitado. Así creemos que la normativa, tal y como está planteada, afectaría tanto a ciudadanos con conocimientos informáticos básicos, al imponer la medida para ciberdelitos dolosos mayores a 3 años como a cibercriminales y organizaciones internacionales encargadas de cometer delitos a gran escala en la Red, siempre que el terminal desde el que se cometieran los hechos estuviera situado en España. Igualmente existen cuestiones morales y éticas que chocan directamente con el uso de estas técnicas como son la creación de virus por parte de las propias autoridades o la contratación de *hackers* para preservar el buen fin de la diligencia…trasladando a la sociedad el mensaje de que el fin siempre justifica los medios.

Si unimos todas estas incógnitas a la creencia basada en que la autoridad judicial que permita el hipotético registro se encontraría con claros y continuos problemas de motivar la idoneidad, necesidad y proporcionalidad, cuando, como

hemos visto, existen alternativas menos lesivas para los derechos fundamentales de los investigados en la regulación nacional y que pueden resultar igual de eficaces de cara al fin perseguido, que no es otro que imputar determinados hechos delictivos a sus presuntos autores en el mundo del ciberespacio, por lo que el articulado acabaría poseyendo un corto recorrido.

De esta forma, descartamos de raíz el uso de *spyware* por parte de los CFSE para infracciones cometidas por particulares, al pensar que no se ajusta, dado el perfil criminal de los presuntos autores así como de la entidad de los delitos, a los principios de necesidad y proporcionalidad, manteniendo para estos casos lo ya regulado para la interceptación de comunicaciones en la normativa española, aunque eso sí, tratando de hacer frente a los problemas que lleva arrastrando la normativa desde hace más de una década, por lo que se solicita su urgente reforma.

En segundo lugar, para los casos de delitos en redes sociales, foros e incluso tráfico de imágenes pedófilas o estafas electrónicas, siempre que las mismas se comentan en la jurisdicción española vemos viable la potenciación de la figura del agente encubierto en Internet y no el uso de *malware*; mientras que si tienen un carácter transfronterizo lo ideal sería acudir al apoyo de fuerzas policiales europeas gracias a los mecanismos diseñados por EUROPOL y el Centro Europeo contra el Cibercrimen.

Todo esto nos lleva a demandar una Directiva europea sobre investigación policial para delitos cometidos a través de Internet, obligando en este caso a los distintos Estados Miembros a transponer la regulación a su Derecho interno e incorporar en ella las particularidades que crea oportunas, como puede ser en el caso español, dada su historia reciente, a implementar estrategias más invasivas como es el caso del uso de *malware* en casos de ciberterrorismo.

Para finalizar, debemos reconocer el carácter transgresor de la normativa al volver a agitar el debate sobre los límites entre el uso de medios de investigación basados en espionaje electrónico y los derechos fundamentales de los ciudadanos. Está claro que la justicia debe modernizarse pero no a cualquier precio, si introducimos preceptos limitativos de estos derechos nos toparemos de frente con la Carta Magna, que servirá como freno a la instauración de un estado policial y al monitorio de nuestra intimidad por los poderes públicos.

Internet es un gigante de dimensiones ingobernables, un "Goliat" ante el que no nos podemos enfrentar de forma individual, país por país, en la figura de "David". No es la hora de realizar regulaciones nacionales que permitan el ciberespionaje sino el momento de unificar esfuerzos entre los Estados de todo el mundo para impulsar regulaciones europeas y mundiales en la lucha contra los crímenes que se cometen en la Red.

## ANEXO: BORRADOR CÓDIGO PROCESAL PENAL ESPAÑOL (ARTS. 350 A 352)

Artículo 350.- Presupuestos

1.- El Tribunal de Garantías podrá autorizar, a petición razonada del Ministerio Fiscal, 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 la medida resulte proporcionada para la investigación de un delito de especial gravedad y sea además idónea y necesaria para el esclarecimiento del hecho investigado, la averiguación de su autor o la localización de su paradero.

2.- La resolución judicial que autorice el registro, además de motivar la idoneidad, necesidad y proporcionalidad, deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios de almacenamiento de datos informáticos o bases de datos y datos informáticos almacenados objeto de la medida.
b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.
d) Los agentes autorizados para la ejecución de la medida.
e) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.
f) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

3.- Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del Ministerio Fiscal quien podrá solicitar del Tribunal de Garantías una ampliación de los términos del registro.

4.- El registro remoto sólo podrá ser autorizado cuando los datos se encuentren almacenados en un sistema informático o en una parte del mismo situado en territorio sobre el que se extienda la jurisdicción española. En otro caso, se instarán las medidas de cooperación judicial internacional en los términos establecidos por la Ley, los Tratados y Convenios internacionales aplicables y el derecho de la Unión Europea.

Artículo 351.- Deber de colaboración

1.- Los proveedores de acceso o servicios telemáticos y los titulares o responsables del sistema informático o base de datos objeto del registro están obligado a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización.

2.- Las autoridades y los 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 para el buen fin de la diligencia.

Artículo 352.- Forma

Las actuaciones referentes al examen y registro a distancia de equipos, dispositivos o sistemas informáticos o electrónicos se sustanciarán en pieza separada y en régimen de secreto, sin necesidad de declaración expresa, el cual tendrá una duración máxima de diez días.