El cibercrimen y el agente encubierto *on line*

~Carmen Lapuerta Irigoyen~
Jurista y criminóloga. Socia FICP.

I. DE AMENAZA A REALIDAD

La reciente edición de El País Digital de 18.05.2017 titulaba en su portal de inicio: Así fue el impacto del ciberataque en España: "Los expertos señalan el severo impacto del virus informático que se propagó a gran escala pese al silencio de las numerosas compañías que se han visto afectadas". El ciberataque, que se propagó por medio mundo ha congelado equipos informáticos y ha pedido rescates a cambio de la recuperación de los datos, comienza a estar controlado gracias a las actualizaciones de Microsoft, al ingenio de los investigadores independientes y al estado de alerta que establecieron la mayoría de empresas e instituciones al conocer la noticia.

Un enorme ciberataque ha golpeado sistemas informáticos en decenas de países. El virus, conocido como *ransomware***,** afectó, entre otros, a los equipos de la sede de Telefónica en Madrid, al sistema de salud británico o el ministerio del Interior ruso. El *ransomware* causa un secuestro exprés de datos y pide un rescate para liberar el sistema. En un *tuit*, Costin Raiu, el director global del equipo de investigación y análisis de Kaspersky Lab, empresa de seguridad informática, estimó que ayer se habían registrado más de 45.000 ataques en 74 países. De momento, ninguna infraestructura crítica ha resultado afectada.[1]

Las investigaciones prosiguen, y todavía quedan muchas cuestiones que responder: quién es el "paciente cero", quién está detrás del ataque y cuáles han sido sus motivaciones. Las últimas pistas señalan directamente al grupo de ciberdelincuentes *Lazarus Group*, vinculado a Corea del Norte y conocido por el ataque a Sony Pictures en el que extrajeron información de carácter confidencial".[2]

II. CONCEPTOS DE CIBERCRIMEN, CIBERDELINCUENCIA Y CIBERDELITO, SU GLOBALIZACIÓN.

Sobre la diferencia entre el "delito informático", *que se vale de elementos informáticos para la perpetración* y el "ciberdelito" que *se refiere a una posterior*

[1] Enlace en: http://tecnologia.elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html
[2] Enlace en: http://tecnologia.elpais.com/tecnologia/2017/05/18/actualidad/1495108825_274656.html

generación delictiva vinculada a las TIC en el que interviene la comunicación telemática abierta, cerrada o de uso restringido, se entiende por *"*cibercrimen"[3] *cualquier infracción punible, ya sea delito –o falta- en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito.*[4]

En la red de redes, es pacífica entre los internautas la definición de la "ciberdelincuencia" como *cualquier tipo de actividad ilegal en la que se utilice Internet, una red privada o pública o un sistema informático doméstico,* y comprende, *cualquier acto criminal que utilice ordenadores y redes* entendiendo por "ciberdelitos" *aquellos atentados a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de la redes y los datos, así como el uso fraudulento de tales sistemas, redes y datos".* Pese a que un elevado porcentaje de ciberdelitos se establecen en torno a la obtención de información sensible para usos no autorizados, la ciberdelincuencia también comprende actos criminales tradicionales, como pueden ser robos, suplantación de identidad, fraude, acoso y así un innumerable etcétera de delitos.[5]

Una vez más la realidad demuestra que el fenómeno de la ciberdelincuencia revela que pese a ser una amenaza silenciosa no por ello resulta menos dañina. Los hábitos de vida se trasladan al ciberespacio, es el paradigma de la transformación digital. Pero este cambio implica nuevos retos, especialmente para el Derecho Penal. La ciberdelincuencia está hoy más activa que nunca, los ataques informáticos y el fraude económico a través de la tecnología alcanzan un grado de sofisticación hasta ahora inimaginable**.** El resultado es que las actividades ilícitas a través de internet pueden llegar a alcanzar un impacto económico de un billón de euros al año en el mundo, según estimaciones del Instituto Nacional de Ciberseguridad (Incibe), cifra equivalente al PIB de un país como España**.** Fuentes policiales aseguran que esta actividad supera al narcotráfico en lucro. En cambio, las inversiones en ciberseguridad en el planeta se estima que alcanzan los 70.000 millones de euros.[6]

[3] ROMEO CASABONA, C. De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal, Comares, Granada, 2006, pp. 1-42.

[4] RAYÓN BALLESTEROS / GÓMEZ HERNÁNDEZ. Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense, núm. 47, 2014, pp. 209-234.

[5] Enlace en: https://sites.google.com/site/criminologos20/noticias-del-blog/conceptoyevoluciondelaciberdelincuencia.

[6] Enlace en: http://www.elmundo.es/economia/2017/01/08/586fc1d222601d6f4b8b4584.html.

La generalización de Internet, de las redes privadas o públicas, de los sistemas informáticos que comporte la utilización de teléfonos móviles, de ordenadores y redes sociales, en las relaciones personales, sociales y económicas ha ido determinando la aparición de novedosos comportamientos -hasta ahora impensables-, que por incidir en bienes jurídicos merecedores de protección demandan un adecuado reproche mediante su tipificación en las legislaciones penales, al igual que está determinando nuevas dinámicas y mecanismos de ejecución de conductas ilícitas más convencionales que ya se encontraban sancionadas en los ordenamientos jurídicos de los distintos países, pero que encuentran en las *TICs* (Tecnologías de la Información y la Comunicación*),* otros cauces para llevar a efecto la actividad criminal de forma más fácil, segura y eficaz. Por otra parte, la existencia de estos instrumentos tecnológicos ha modificado también profundamente las técnicas de investigación criminal. Son indudables las ventajas que ofrecen estos nuevos medios tecnológicos para investigar comportamientos delictivos, no solamente aquellos relacionados con las nuevas tecnologías como pueden ser la distribución de pornografía infantil, el *phising (*suplantación de identidad, consiste en el envío de correos electrónicos que aparentan ser fiables y que suelen derivar a páginas web falsas recabando datos confidenciales de las víctimas*)* o el *childgrooming (*término de la lengua inglesa que significa en español "acicalar" y que se utiliza para hacer referencia a todas las conductas o acciones que realiza un adulto para ganarse la confianza de un menor de edad, con el objetivo de obtener beneficios sexuales), sino también respecto a comportamientos delictivos más tradicionales en los que la geolocalización de un teléfono móvil, la determinación de la dirección IP, o incluso la realización de registro remoto, puede contribuir al esclarecimiento del hecho delictivo. Sin embargo, es indudable que la utilización de estos instrumentos tecnológicos como medios de investigación criminal plantea importantes problemas en lo referente a la afectación que estos pueden producir en derechos fundamentales. Resulta evidente que hoy en día estos nuevos instrumentos tecnológicos representan un papel fundamental en la comunicación e interacción de los individuos por lo que todo registro de ordenador o intervención de Smartphone puede suponer una intromisión no solamente en el derecho de la intimidad sino también, claro está, en el derecho al secreto de comunicaciones que, como sabemos, tiene una protección constitucional privilegiada al exigir siempre resolución judicial no admitiendo, como en el caso de la intimidad, una intromisión en

la misma por parte de la Policía cuando concurre una situación de urgencia.[7]

III. LA CIFRA NEGRA Y VÍCTIMAS DE LOS DELITOS CIBERNÉTICOS.

Las cifras que presenta el Ministerio del Interior a través de la Estadística de Cibercriminalidad 2015[8], refieren que se contabilizaron para el año 2015, tan solo un total de 60.154 hechos, de los cuales el 67,9% corresponde a fraudes informáticos (estafas) y el 16,8% a amenazas y coacciones, esa cifra de denuncias no llega ni a un 10% de los delitos que se comenten.[9]

La contribución de la víctima a la comisión del delito cibernético es determinante en numerosas ocasiones para entender la elevada tasa de criminalidad, pero también la alta cifra negra, al no reconocer su condición de víctima, no presentar denuncias o no continuar hasta el final con sus pretensiones procesales.[10] Son numerosos los casos en los que las víctimas desconocen su condición de tales, lo que se explica como consecuencia de las dificultades de naturaleza técnica existentes. El sistema de trabajo a tiempo real que permite el tratamiento instantáneo de los datos o las modificaciones de los programas, o la copia de unos y de otros, por lo general, sin dejar huella de las operaciones realizadas, favorece un fenómeno criminal en el que la víctima desconoce la lesión sufrida o, en última instancia, toma constancia de la misma transcurrido cierto tiempo desde la comisión del hecho[11]. Son los supuestos de ataques dirigidos contra personas naturales en los que la cifra negra se relaciona como la llamada "invisibilidad del delito informático"[12]. Esta invisibilidad tendría su razón de ser en la relatividad del espacio y tiempo, a través de la cual el delincuente se inviste con los más absolutos atributos de intemporalidad y ubicuidad[13]. El carácter anónimo provoca en la víctima la sensación de que la justicia penal no podrá dar con el responsable y siente que se

[7] ZARAGOZA TEJADA, J.I., Jornadas de la FGEº de 27 octubre 2016 sobre uso de las nuevas tecnologías y nuevas formas de delincuencia. La modificación operada por la Ley 13/2015. El agente encubierto informático, pp. 2-3.

[8] Ministerio del Interior estudio sobre la cibercriminalidad en España 2015 Enlace en: http://www.interior.gob.es/documents/10180/3066430/Informe+Cibercriminalidad+2015.pdf/c10f398a-8552-430c-9b7f- 81d9cc8e751b.

[9] BARRERA, S. Jefa de la Sección Técnica del Grupo de Investigación en Redes de la Unidad de Investigación Tecnológica (UIT) del CNP, Entrevista 17.03.2013. Enlace en: http://www.muycomputerpro.com/2017/03/17/silvia-barrera-cnp.

[10] ANARTE BORRALLO, E. Impactos de las nuevas tecnologías en el sistema penal: aproximación al derecho penal en la sociedad de la información. Revista Derecho y conocimiento, vol.1, 2001 p. 206.

[11] ROMEO CASABONA, C.M, Poder Informático y Seguridad Jurídica, Editorial Fundesco. Madrid. 1988. p. 38.

[12] REYNA ALFARO, L. La víctima en el delito informático. Revista peruana de Doctrina y Jurisprudencia Penal. Núm. 1/2002 p 7.

[13] HERRERA MORENO, M. El fraude informático en el derecho penal español. Actualidad penal. Núm. 39, 2001. p. 931.

enfrenta a un ser invisible frente a cuyos ataques sólo queda resignarse, por lo que pocas veces denuncian los hechos que se dan en su perjuicio[14].

Cuando los ataques delictivo-informáticos son dirigidos contra empresas o corporaciones, la "cifra negra" de criminalidad encuentra también su razón de ser en la "publicidad negativa" y lo que ello significa para las propias empresas atacadas[15]. Los incidentes en Internet suelen estar asociados con el nivel de seguridad informática que poseen las empresas o corporaciones atacadas. Lo que genera desprestigio en la empresa[16] atacada, descrédito de la fiabilidad de la gestión de la propia empresa y, en diversas ocasiones, temor a que como consecuencia de las investigaciones policiales, se lleguen a desvelar estrategias o secretos comerciales, industriales o científicos[17]. Por esa razón un alto número de incidentes de seguridad en Internet son mantenidos en reserva por decisión de las propias víctimas[18].

En general, bien sea por el desconocimiento de la intromisión ilegítima, bien por el desprestigio que conlleva la denuncia de un ataque informático, la realidad de la "cifra negra" en el ámbito de la cibercriminalidad se hace más patente que en otros supuestos y genera inevitablemente un sentimiento de impunidad a la hora de afrontar la comisión de estos delitos a pesar de las ventajas de la presentación de denuncias.

IV. IDENTIFICACION DE LAS CIBERAMENAZAS Y SUS AGENTES.[19]

El Centro Criptológico Nacional al elaborar su Informe de Ciberamenazas y Tendencias de 2015 constata una vez más que la generalización del uso de los medios electrónicos incrementa la superficie de ataque y, en consecuencia, los beneficios potenciales derivados, lo que constituye sin duda uno de los mayores estímulos para los atacantes. En dicho informe publicado en 2016, se examina el impacto, en España y fuera de sus fronteras, de las amenazas y los ciberincidentes más significativos ocurridos en 2015:

[14] REYNA ALFARO, L.M. La víctima en el delito informático. Revista peruana de Doctrina y Jurisprudencia Penal. Núm. 1/2002 p. 8; en igual sentido MORÓN LERMA, E. Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red. Aranzadi. Pamplona 1999, p. 27.

[15] REYNA ALFARO, L.M. Aproximaciones Victimológicas. Capítulo Criminológico Vol. 31. núm. 4/ 2003 p. 101.

[16] ACURIO DEL PINO, S. Delincuencia informática. Revista de Derecho de UNAM 1990 p. 17.

[17] ROMEO CASABONA, C.M, Poder Informático. 1988. p. 39.

[18] HERRERA MORENO, M. El fraude informático. Actualidad penal. Núm. 39, 2001. p. 932; en igual sentido MORÓN LERMA, E. Internet y Derecho Penal. Aranzadi. Pamplona 1999. p. 37.

[19] Centro Criptológico Nacional. Informe 2015 Enlace en CCN-CERT.https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1483-ccn-cert-ia-0916-ciberamenazas-2015.

1. **Ciberespionaje / actores estatales / organizaciones privadas (por Estados y empresas, político o industrial).**

Ésta modalidad ha constituido la mayor amenaza para los países, estando especialmente dirigida a los sistemas de información de las corporaciones industriales, empresas de Defensa, alta tecnología, automoción, transportes, instituciones de investigación y Administraciones Públicas. La complejidad, volumen e impacto de estos ataques, habitualmente conducidos a través de APTs. Las evidencias de 2015 permiten afirmar que, en significativas ocasiones, tales acciones han sido llevadas a cabo por Servicios de Inteligencia o Departamentos de Defensa extranjeros, que siguen invirtiendo importantes recursos en dotarse de capacidades de defensa y, también, de ataque.

Entre los ataques más destacados de 2015 en España, destacan que los actores principales en el robo de información han sido los grupos: APT28, Snake, APT29 y Emissar y Panda.

Valoración de la amenaza: este tipo de ataques continuará en ascenso en los próximos años, al tiempo que lo hace su sofisticación y peligrosidad.

2. **Ciberdelito / ciberdelincuentes.**

Destaca su profesionalización y el crecimiento de la organización interna de sus actores. La sofisticación de las técnicas usadas, la disponibilidad de nuevas o renovadas herramientas (incluyendo la prestación de servicios delincuenciales bajo demanda - on demand-) y la pulcritud en la perpetración de tales acciones constituyen una preocupación en franco crecimiento. El año 2015 evidenció que las organizaciones cibercriminales están dispuestas a invertir grandes cantidades de dinero en la preparación de sus acciones. Del mismo modo, el denominado Cibercrimen como Servicio "CaaS Cybercrime-As-A-Service" ha incrementado su penetración y profesionalización, habiéndose percibido una cierta "competencia" entre los propios ciberdelincuentes, lo que obliga a sus autores a prestar a sus "clientes" un "servicio" cada vez más fiable.

Ataques más destacados de 2015:

- Campaña Carbanak dirigida contra entidades financieras de Europa del Este, en donde lograron infectar a varios bancos a través de spearphishing. Se estima que los autores fueron capaces de sustraer entre 250 y 1.000 millones de dólares.

- Corcow: un ataque dirigido usando técnicas de inteligencia, a entidades financieras (y sus clientes), que tuvo especial incidencia en Rusia y Ucrania.

- Ataque a Hacking Team: exfiltración y publicación de informes de esta empresa italiana especializada en la venta de herramientas y tecnologías de ataque y monitorización.

- Home Depot sufrió el robo de 56 millones de números de tarjetas de crédito y débito, además de 53 millones de direcciones de correo electrónico de sus clientes.

- Las sustracciones de datos personales de Community Health Systems (4,5 millones de pacientes), Anthem (80 millones de asegurados) y Premera (11 millones de aseguradas en Estados Unidos)

Valoración de la amenaza: los beneficios obtenidos y el acceso cada vez más fácil a las herramientas de perpetración de este tipo de ataques propiciará el incremento del número de ciberdelincuentes y, en consecuencia, el de sus acciones.

3. Ciberterrorismo / grupos terroristas.

Aunque la peligrosidad potencial de sus acciones sigue creciendo, no puede afirmarse que, en la actualidad, represente una grave amenaza, especialmente por las limitadas capacidades técnicas que se han observado en sus despliegues.

Valoración de la amenaza: las capacidades del ciberyihadismo no han hecho sino empezar a mostrarse. Es de esperar ciberataques más numerosos, más sofisticados y más destructivos en los próximos años, en tanto persista la actual situación en torno a Daesh

4. Hacktivismo.

Personas o grupos, más o menos organizados, que desarrollan sus acciones en el ciberespacio movidos generalmente por motivos ideológicos. En los últimos años sus ciberataques (desfiguración de páginas web, ataques DDoS12 o sustracción de datos confidenciales de sus objetivos) pretendieron ser la respuesta a determinadas medidas adoptadas por gobiernos y que consideraban perjudiciales para la libertad de Internet. En general, el año se ha caracterizado por un número reducido de operaciones hacktivistas comparado con años anteriores.

Ataques más destacados de 2015:

- Confrontación entre grupos en la órbita de 'Anonymous', por un lado, contra identidades hacktivistas que apoyan o muestran simpatía por el grupo yihadista 'Daesh'.

- Tras el ataque al semanario francés, Charlie Hebdo, se produjeron múltiples desfiguraciones a sitios web franceses. La operación de Anonymous #OpCharlieHebdo Anonymous dio lugar a la reacción #OpFrance, en la que decenas de sitios web franceses mostraron textos islámicos.

- En Iberoamérica se mantuvo una ofensiva contra el Gobierno de Nicolás Maduro (Venezuela) y varias operaciones antigubernamentales en México.

- En España se caracteriza por una baja densidad con la excepción de "La 9ª Compañía de Anonymous".

5. Ciberyihadismo / grupos yihadistas (acciones atribuibles a grupos de tendencia violenta y radical dentro del islam político).

En 2015 ha aparecido una nueva amenaza: el ciberyihadismo, que usando métodos, procedimientos y herramientas del terrorismo, el hacktivismo y la ciberguerra constituye una realidad incipiente y supone una de las mayores amenazas con las que se enfrentarán las sociedades occidentales en los próximos años. Las importantes vías de financiación de estos grupos (al socaire de Daesh) hacen posible que puedan llegar a adquirir los conocimientos y las herramientas precisas para el desarrollo de ciberataques o la contratación de los mismos. Hasta el momento, sus ataques se han limitado a la desfiguración de páginas web, ataques DDoS a pequeña escala o, más comúnmente, al uso de Internet y de las redes sociales para la diseminación de propaganda o el reclutamiento y la radicalización, actividades que no exigen grandes conocimientos o infraestructura.

Desde el mundo judicial se ha detectado la propagación del islamismo radical a través de las redes sociales, usando internet para reclutar y adiestrar a sus "soldados" y para obtener financiación.[20]

Ataques más destacados de 2015:

[20] ZARAGOZA J. / DELGADO, D. ex fiscal jefe de la Audiencia Nacional y coordinadora antiterrorista yihadista en la Audiencia Nacional, respectivamente. Entrevista. Enlace en: http://www.elmundo.es/opinion/2015/03/08/54fc94e3268e3ee02d8b456d.html.

- Uso de código dañino (por ejemplo, en Siria se detectaron ciberataques para obtener datos sobre posiciones de los objetivos locales).

- Ataque a sitios web.

- Instrucciones para el uso de una herramienta de acceso remoto (RAT14) para el control de equipos.

- Ataques a redes sociales para la obtención de información.

- Ataques de phishing para obtener datos de tarjetas de crédito y obtener información.

- El grupo CyberCaliphate afiliado a Daesh atacó y tomó el control de las cuentas de Twitter y Youtube del US Central Command.

Valoración de la amenaza: las capacidades del ciberyihadismo no han hecho sino empezar a mostrarse. Es de esperar ciberataques más numerosos, más sofisticados y más destructivos en los próximos años, en tanto persista la actual situación en torno a Daesh.

6. Cibervandalismo/vándalos y script kiddies.

Se denomina ***cibervándalos*** a aquellos individuos que, poseyendo significativos conocimientos técnicos, llevan a cabo sus acciones con el único motivo de demostrar públicamente que son capaces de hacerlo. Por su parte, los denominados ***script kiddies*** son aquellos que, con conocimientos limitados y haciendo uso de herramientas construidas por terceros, perpetran sus acciones a modo de desafío, sin ser, en muchas ocasiones, plenamente conscientes de sus consecuencias. Pese a la difusión mediática que durante 2015 han recibido las acciones de los cibervándalos, no constituyen una amenaza seria a los intereses de las organizaciones.

Ataques más destacados de 2015: Desfiguración de la página web de Malaysian Airlines.

Valoración de la amenaza: de cara a los próximos años no se prevén alteraciones sustanciales del comportamiento de estos actores.

7. Actores internos.

También denominados ***Insiders*** son personas que están o han estado trabajando para una organización (empleados o exempleados, colaboradores y proveedores) y que provocan brechas de seguridad importantes. En algunos casos se detecta exfiltración de

información por motivos económicos o políticos. En otros casos se debe a negligencia o despecho de determinadas personas. En varios de los ciberincidentes ocurridos en 2015 se pudo observar cómo algunos empleados manejaron información sensible en servidores privados sin adoptar las adecuadas medidas de seguridad.

Ataques más destacados de 2015

- Un empleado de una compañía de seguros depositó datos de las reclamaciones de 27.000 asegurados en un servidor privado para probar un determinado software.

- Caso de AMS-IX (compañía holandesa de intercambio de Internet): un error durante los trabajos de mantenimiento hicieron caer la plataforma y los servicios web no estuvieron disponibles durante diez minutos, lo que, pese a lo limitado del tiempo, tuvo repercusión internacional, dada la importancia del sistema afectado.

Valoración de la amenaza: los actores internos sólo han venido representando un pequeño porcentaje de los agentes de las amenazas (menos del 15%)

8. Ciberinvestigadores.

Buscan vulnerabilidades en entornos TIC al objeto de verificar la protección de los sistemas objeto de sus investigaciones. Con frecuencia, además de informar a las empresas, se publica en los medios de comunicación el resultado de sus investigaciones con un doble efecto: positivo y negativo. En el plano negativo es evidente que la publicidad de cualquier vulnerabilidad conlleva que los sistemas identificados sean más vulnerables a ataques externos, facilitando la acción de los atacantes, que pueden llegar a beneficiarse de los resultados de las investigaciones. Incluso, se han dado casos de ciberinvestigadores acusados de realizar extorsiones a las entidades investigadas.

V. REACCION INSTITUCIONAL Y NORMATIVA FRENTE A LOS RIESGOS DEL CIBERCRIMEN.

1. Compromiso internacional: Convenio de Budapest 23.11.2001.

El Convenio del Consejo de Europa sobre Ciberdelincuencia[21], firmado en Budapest por España el 23 de noviembre de 2001, supone la respuesta a la necesidad de tener medios eficaces de cooperación para la lucha contra la cibercriminalidad. Se refiere al desarrollo y la utilización, cada vez mayor, de las Tecnologías de la

[21] Publicado en el BOE núm. 226 de 17/07/2010.

Información y la Comunicación, así como la necesidad de aplicar una política penal común, encaminada a proteger a la sociedad frente a este nuevo tipo de delincuencia, adoptando y armonizando una legislación adecuada en todos los países y manteniendo una política de cooperación internacional. Dicho convenio no fue ratificado por España hasta 1 de octubre de 2010 y ha sido el inspirador de la Directiva 2013/40/UE. La reforma del Código Penal de 2015 está motivada por dicha directiva.

La plena conciencia de este fenómeno y de la repercusión que esa utilización irregular de estas nuevas herramientas puede tener en el pleno ejercicio de los derechos y las libertades de las personas, está impulsando en los últimos años un claro empeño de muchos Estados y de diversas organizaciones internacionales en articular de forma coordinada soluciones legales que, plenamente respetuosas con los principios y valores que informan el Estado de Derecho, resulten adecuadas y eficaces en la acción policial y judicial frente a estas novedosas manifestaciones criminales. Esta acción coordinada es la única respuesta posible ante un fenómeno criminal que se desarrolla en el ciberespacio, más allá de límites territoriales y fronterizos y cuyos artífices se sirven de las diferencias en los ordenamientos jurídicos nacionales para dificultar su persecución y sanción y, en definitiva, procurar su impunidad. De acuerdo con este planteamiento y en plena sintonía con los países del entorno más próximo, en nuestro país se publicó en el año 2013, la Estrategia Nacional de Ciberseguridad, en la que se fijaron las directrices para el uso seguro del ciberespacio *con una visión integradora a través de la adecuada coordinación y cooperación de todas las Administraciones Públicas, contando además, con el sector privado y con los ciudadanos.* Uno de los objetivos de este documento, el tercero de ellos, se refiere específicamente al tema que nos ocupa pues se concreta en *potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio.*[22]

2. Especialización en materia de cibercrimen de unidades policiales.

En nuestro país, al igual que en el resto del mundo, el aumento de los delitos tecnológicos ha crecido exponencialmente, para intentar luchar contra ellos se han creado unidades especializadas de investigación, tanto en el Cuerpo Nacional de Policía como en la Guardia Civil y algunas policías Autonómicas. Así encontramos que existen unidades especializadas en cibercrimen denominadas:

[22] Memoria de la FGE 2016 pp. 590-593

a) **U.I.T. /B.I.T.** [23]**(**Unidad de Investigación Tecnológica/Brigada de Investigación tecnológica, del Cuerpo Nacional de Policía). La Brigada de Investigación Tecnológica es la Unidad policial, encuadrada en la Unidad de Delincuencia Económica y Fiscal (UDEF), está destinada a responder a los retos que plantean las nuevas formas de delincuencia. Pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería, entre otros.

b) **G.D.T.** 24 **(Grupo de delitos telemáticos de la Guardia Civil), creado para** investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se cometen a través de Internet. Su origen se remonta al año 1996, cuando se constituyó el Grupo de Delitos Informáticos (GDI) para atender a las pocas denuncias que había entonces por los llamados delitos informáticos. Su buen hacer y el crecimiento exponencial de usuarios de la red, propiciaron el crecimiento del grupo, que pasó a llamarse Departamento de Delitos de Alta Tecnología (DDAT), asumiendo como nueva competencia el fraude en el sector de las telecomunicaciones. Con la socialización de Internet y el crecimiento de los hechos delictivos, se amplía el abanico de competencias de investigación, que alcanza a todas aquellas conductas delictivas realizadas a través de los sistemas de información o contra éstos, lo que se conoce popularmente como el cibercrimen. El departamento cambia de nombre por el actual, Grupo de Delitos Telemáticos (GDT). Estos cambios se acompañaron de la creación de los Equipos de Investigación Tecnológica (EDITE,) en cada uno de las provincias de España. El esfuerzo principal del GDT y de los EDITE,s ha sido, desde su creación, la investigación de la delincuencia que se vale de las redes y sistemas de información para su comisión. También cabe destacar los esfuerzos que realizan para fomentar un uso seguro de las nuevas tecnologías, consciente de que a la larga este esfuerzo ayudará a minimizar el impacto de la delincuencia.

c) **U.C.O.**[25] (Unidad Central Operativa de la Guardia Civil). Como Unidad específica de Policía Judicial, tiene como misión investigar y perseguir los asuntos relacionados con la delincuencia organizada, económica, internacional y aquella

[23] Enlace en: http://www.policia.es/orq central/iudicial/udef/bit quienes somos.html
[24] Enlace: http://www.guardiacivil.es/es/servicios/delitos telematicos/index.htmi
[25]Enlace en: http://www.gurdiacivil.es/es/institucional/estructuraorganización/orgcentral/direcadjunope/

otra cuyas especiales características así lo aconsejen; así como el establecimiento y mantenimiento del enlace, coordinación y colaboración con otros servicios afines, nacionales e internacionales.

3. Especialización judicial en cibercrimen

a) En el año 2011 se creó **LA FISCALÍA ESPECIALIZADA EN DELITOS INFORMÁTICOS**. Es a través de la Instrucción 2/2011 del Fiscal General del Estado, por la que se crea la denominada Fiscalía de Criminalidad Informática. Los delitos que investiga se estructuran en tres categorías:

1) Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TIC (sabotaje informático, acceso sin autorización a datos, programas o sistemas informáticos, revelación de secretos, entre otros),

2) Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TIC (estafas informáticas, delitos contra la propiedad intelectual, corrupción de menores y personas discapacitadas, pornografía infantil, entre otros),

3) Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TIC, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia (falsificación documental, injurias y calumnias contra funcionarios públicos, amenazas y coacciones, delitos contra la integridad moral, apología o incitación a la discriminación, el odio y la violencia, justificación de los delitos de genocidio, entre otros).

b) **EL CONSEJO GENERAL DEL PODER JUDICIAL** viene impulsando cursos formativos sobre "ciberdelincuencia" a los distintos operadores jurídicos, siendo uno de los más recientes el celebrado en Valencia los días 9 y 10 de marzo de 2017[26] en el que se abordó como tema central la "Problemática penal de las redes sociales".

4. Respuesta interna. reforma del Código Penal por las Leyes Orgánicas 1/2015 y 2/2015, ambas de 30 de marzo.

[26] Enlace en: file:///C:/Users/Usuario/Downloads/Ciberdelincuencia%20y%20redes%20sociales%20(1).pdf.

Como respuesta normativa íntimamente vinculada al problema, se encuentra la publicación de dos importantísimas reformas legislativas que afectan plenamente al ámbito de la ciberdelincuencia. Por una parte la reforma del Código Penal llevada a efecto por las leyes orgánicas 1/2015 y 2/2015, ambas de 30 de marzo que, en lo que aquí interesa, incorporan tipos penales novedosos con los que se pretende hacer factible la persecución penal de determinadas manifestaciones criminales surgidas al socaire de la evolución tecnológica y también adaptan figuras delictivas tradicionales en el derecho patrio a las especialidades detectadas en las formas comisivas como consecuencia de la utilización de herramientas TIC en la planificación y ejecución criminal. En ambos casos, y en línea con lo anteriormente indicado, ha de reseñarse que muchas de estas modificaciones derivan de la implementación en el ordenamiento jurídico español de normas internacionales sobre la misma materia. Así ocurre con la Directiva 2013/40/UE de 12 de agosto sobre ataques a los sistemas de información, inspirada a su vez en la Convención de Budapest del Consejo de Europa, cuya incorporación al CP además de servir para la reorganización sistemática de los delitos de descubrimiento y revelación de secretos y daños informáticos, ha dado lugar a la tipificación de conductas como la interceptación ilegal de las transmisiones de datos entre sistemas (artículo 197.bis.2) y el abuso de dispositivos (artículo 197 ter y 264 ter) así como a la reelaboración de los subtipos agravados y a la elevación de las sanciones respecto de los delitos de daños informáticos. La adaptación de nuestra normativa interna se ha dejado notar igualmente en los delitos contra la libertad e indemnidad sexual de los menores, por influencia en este caso de la Directiva 2011/93/UE sobre abuso, explotación de los menores y pornografía infantil y de la Convención de Lanzarote del Consejo de Europa. La publicación de la LO 1/2015 ha implicado modificaciones en la figura del child grooming (artículo 183 ter), así como en los delitos de pornografía infantil (artículo 189), entre las que han de destacarse la tipificación del acceso on-line a material de esta naturaleza, la previsión especifica 593 en el código penal de la retirada de contenidos ilícitos, la interrupción de servicios o el bloqueo de unos y otros por resolución judicial, o la formulación de un concepto legal de pornografía infantil. A su vez, la LO 2/2015 ha supuesto novedades significativas en la tipificación y sanción de los delitos de terrorismo (artículo 573 y ss.) con el objetivo, alguna de ellas, de facilitar la actuación penal frente al uso de Internet con fines terroristas de acuerdo, también en este aspecto, con las pautas marcadas internacionalmente y, en particular, las fijadas por la Decisión Marco 2008/919/JAI y la Resolución n.º 2178 de NNUU de 24-IX-2014. En otros casos

las variaciones en los tipos penales han venido determinadas por la necesidad de ofrecer respuestas legales ante algunos comportamientos surgidos al hilo del uso de las TIC y que se han entendido merecedores de un reproche penal poco factible con la previa regulación legal. Buen ejemplo de ello, es la tipificación de la cesión inconsentida de imágenes de carácter íntimo (artículo 197.7) y del acoso permanente a través de medios de comunicación (artículo 172 ter) o la redefinición de los delitos contra los derechos de propiedad intelectual cometidos a través de los servicios de la sociedad de la información que acoge en nuestro ordenamiento penal la doctrina Svensson fijada por el Tribunal de Justicia de la Unión Europea (TJUE) en sentencia de fecha 13-II-2014. Esta importante modificación legislativa se ha completado con la inaplazable reforma de la Ley de Enjuiciamiento Criminal, particularmente la llevada a efecto por LO 13/2015 de 5 de octubre que alcanza, entre otras materias, a la investigación tecnológica. Al margen de otras consideraciones sobre las novedades incorporadas en el proceso penal, en lo que afecta a los procedimientos sobre ciberdelitos, ha de reconocerse el acierto del legislador español al abordar de forma detallada y completa la utilización de las herramientas e instrumentos tecnológicos como medios de investigación criminal, materia en la que la regulación existente hasta ahora era claramente insuficiente –especialmente si tenemos en cuenta los derechos y libertades que pueden verse afectados por dichas técnicas de investigación– como ya habían puesto reiteradamente de manifiesto nuestros Tribunales y el propio Tribunal Europeo de Derechos Humanos (TEDH). El legislador además de incorporar al texto legal la doctrina que al respecto han ido elaborando el Tribunal Supremo y el Tribunal Constitucional para cubrir –en la medida de lo posible– las carencias legales, ha aprovechado también para incorporar a nuestro ordenamiento algunos mecanismos de investigación recogidos en disposiciones internaciones como es el caso de la orden de preservación de datos (artículo 588 octies) derivada de los artículos 16 y ss. de la Convención de Budapest del Consejo de Europa y cuyo objeto es evitar la destrucción de evidencias electrónicas en tanto se obtiene autorización judicial para el acceso a las mismas.[27]

VI. EL AGENTE ENCUBIERTO INFORMÁTIVO, ON LINE, 2.0 Ó VIRTUAL.

Se puede definir al agente encubierto en Internet como *"empleado o funcionario público que, voluntariamente, y por decisión de una autoridad judicial, se infiltra en la*

[27] Memoria de la FGE 2016 pp. 590-593.

Red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de la red" mediante "la ocultación de la verdadera identidad policial, con el fin de establecer una relación de confianza que permita al agente integrarse durante un periodo de tiempo prolongado en el mundo en el que los "ciberdelincuentes" actúan, con la finalidad primordial, igualmente oculta, de obtener la información necesaria para desenmascarar a los supuestos criminales".[28]

La figura del agente encubierto únicamente se encontraba regulada vía del artículo 282 bis LECrim, la entrada en vigor de la LO 13/2015, en el referido artículo añade dos apartados, los apartados 6 y 7, con la finalidad de introducir el agente encubierto informático, al que se le aplicarán las mismas condiciones fijadas para el agente encubierto tradicional.

El ámbito en el que podrán tener lugar las infiltraciones, viene limitado por tres exigencias.

1. la investigación esté orientada hacia actividades propias de la delincuencia organizada.

2. la investigación debe estar dirigida a esclarecer alguno de los delitos descritos en el artículo 282 bis 4, o cualquier delito de los previstos en el artículo 588 ter.

3. solamente podrán participar en comunicaciones mantenidas en canales cerrados de comunicación, limitando así su competencia -fuera quedarían "todos los contenidos informáticos de naturaleza abierta, como foros, blogs, chats o redes sociales con contenido público, denominado ámbito de ciberpatrullaje[29]-. Únicamente se podría usar para canales cerrados como mensajes privados de redes sociales o foros restringidos".[30]

La novísima figura de los *"agentes encubiertos informáticos"*, una suerte de espías en la red, ya habían sido aceptados por la Jurisprudencia, y que permitirán a la Policía Judicial, a través del uso de identidades falsas, intercambiar archivos ilícitos en

[28] VALDIVIESO VILLANUENA. L., Las diligencias de investigación tecnológica y su aplicación práctica en el Orden Jurisdiccional Penal. TFM. Universidad de Salamanca. 2016. pp. 13-16.

[29] ZARAGOZA TEJADA, J.I., Jornadas de la FGEº octubre 2016 sobre uso de las nuevas tecnologías y nuevas formas de delincuencia. pp 2-3.

[30] BUENO DE MATA, F. Comentarios críticos a la inclusión de la figura del agente encubierto virtual en la Ley de Enjuiciamiento Criminal. Fodertics 4.0 estudios sobre nuevas tecnologías y justicia. Editorial Comares, Granada. 2015 pp. 117-123.

Internet así como distribuir troyanos en el transcurso de una investigación para identificar a los presuntos delincuentes. Estos agentes podrán, a través de la creación de un pseudoperfil en cualquier red social, intercambiar con otro usuario material que -por su propia naturaleza- sea constitutivo de delito a fin de poder identificar al autor material. Asimismo, se encontrarán habilitados para grabar imágenes y conversaciones cuando ello sea necesario, así como para analizar los algoritmos asociados a estos archivos ilícitos con la finalidad de localizar a los supuestos autores de determinados hechos delictivos.

Con la última reforma procesal por Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, se menciona esta figura al considerar que *"resulta ocioso explicar la importancia del denominado agente encubierto a efectos de la persecución de determinadas modalidades delictivas. Pues bien, íntimamente relacionado con las anteriores medidas de investigación tecnológica, la reforma actualiza el uso de tales recursos por el agente encubierto en las tareas que tiene encomendadas. En concreto, de una parte se prevé la posibilidad de que los agentes encubiertos puedan obtener imágenes y grabar conversaciones, siempre que recaben específicamente una autorización judicial para ello; y de otra, se regula la figura del agente encubierto informático, que requiere autorización judicial para actuar en canales cerrados de comunicación (puesto que en los canales abiertos, por su propia naturaleza, no es necesaria) y que a su vez, requerirá una autorización especial (sea en la misma resolución judicial, con motivación separada y suficiente, sea en otra distinta) para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación"*[31].

En todo caso ha de tenerse en cuenta que la infiltración únicamente sería constitucionalmente valida si se excluye totalmente la posibilidad de la provocación delictiva. En relación con ello existe una doctrina muy consolidada en la Sala Segunda del Tribunal Supremo a cuyo tenor: no cabe identificar ni confundir el delito provocado con el que ha venido a denominarse delito comprobado, que tiene lugar cuando la actividad policial, sin quebrar legalidad alguna, pretende descubrir delitos ya cometidos,

[31] Apartado IV de la Exposición de Motivos de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. BOE núm. 239, de 6 de octubre de 2015.

generalmente de tracto sucesivo, como suelen ser los de tráfico de drogas, toda vez que en estos supuestos el agente infiltrado no busca ni genera la comisión del delito, sino allegar pruebas de una ilícita actividad ya cometida o que se está produciendo, pero de la que únicamente se abrigan sospechas. En el delito provocado no se da en el acusado una decisión libre y soberana de delinquir. En el delito comprobado esa decisión es libre y nace espontáneamente. (STS entre otras de fechas 09.12.1998; 16.04.1999; 19.02.2003 y 30.10.2006). Más recientemente se ha referido a esta materia la Sala II del Tribunal Supremo en sentencia de fecha 10.05.2013 (marginal Aranzadi 8073). En esta resolución nuestro más alto Tribunal además de dejar constancia de que el delito provocado es una rechazable e inadmisible actividad policial que traspasa los límites de la legalidad, recuerda expresamente que es clara la distinción entre el delito provocado instigado por la policía y aquella otra actividad policial tendente a acreditar el delito ya decidido de forma autónoma y libre por la persona concernida reduciéndose la actividad del agente policial a comprobaría1 delito. En igual sentido ha de citarse la STEDH caso Nosko y Nefedov contra Rusia, de fecha 30.09.2014 que rechaza de plano la incitación policial como medio de investigación al quebrar la exigencia de un juicio justo.

VII. CONCLUSIONES

1. Resulta acuciante dar una respuesta ágil y efectiva en el plano del Derecho Internacional para este tipo de delitos que no conocen de fronteras, para que se intensifique la colaboración internacional y se pueda hacer frente a su extraterritorialidad.

2. En general, existe un desconocimiento en el mundo judicial de la mayor parte de los aspectos relacionados con las nuevas tecnologías de la información y la comunicación, por lo que resulta inaplazable la adaptación a la actual situación de todos los operadores jurídicos mediante cursos de formación que permitan, dada que la complejidad técnica de los procesos, conocer el alcance de las medidas que puedan solicitarse y de las infracciones que pueden cometerse.

3. A nivel policial, se detecta falta de medios personales y materiales que puedan llevar con éxito este tipo de investigaciones, lo que causa gran perplejidad en el ciudadano al ver como en ciberataques masivos como el reciente, sean personas civiles, normalmente jóvenes, quien de forma voluntariosa y altruista consigan hacer un “cortafuego” de lo que pudiera ser una infección informática a escala mundial.

4. Necesario compromiso del sector privado en el mantenimiento de sus sistemas informáticos protegidos con sistemas de seguridad perfecta y constantemente actualizados. Instauración y difusión de planes de prevención y concienciación entre sus empleados, para que eviten los riesgos de infestaciones informáticas, mediante uso de terminales y claves individuales y no transferibles.

5. Necesaria concienciación de los poderes públicos para articular campañas de divulgación pública, especialmente entre los más jóvenes, que favorezcan la presentación sistemática de denuncias, que permitirían aminorar la invisibilidad de muchas de esas conductas, ante la falta de inmediación entre autor y víctima.

6. Uno de los graves problemas que se pueden presentar con la reciente figura del agente informático encubierto, serán las vías a través de la cuales los medios de prueba por él obtenidos puedan ser introducidos en el acto del juicio oral. El nuevo art. 282bis LECr, además, parece dejar fuera la posibilidad de mantener la identidad falsa del agente encubierto en el juicio oral en los supuestos del agente encubierto *on line* del apartado 6º del citado artículo.

7. Habrá que estar atento a las resoluciones de nuestros tribunales para el caso de que el investigado confiese el delito ante el agente encubierto informático toda vez que, como Agente de la Fuerzas y Cuerpos de Seguridad del Estado, no puede ser valorado su testimonio de referencia por los Tribunales a la hora de adoptar una resolución sobre el fondo del asunto (Pleno no Jurisdiccional de la Sala II de 03.06.2015).