Revista de Estudios en Seguridad Internacional

Vol. 4, No. 1 (2018)

Editada por:
Grupo de Estudios en Seguridad Internacional (GESI)

Lugar de edición:
Granada, España

Dirección web:
http://www.seguridadinternacional.es/revista/
ISSN: 2444-6157
DOI: http://dx.doi.org/10.18847/1

Para citar este artículo/To cite this article:

José Enrique Anguita Osuna, "Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea", *Revista de Estudios en Seguridad Internacional*, Vol. 4, No. 1, (2018), pp. 107-126.

DOI: http://dx.doi.org/10.18847/1.7.7

Si desea publicar en RESI, puede consultar en este enlace las Normas para los autores: http://www.seguridadinternacional.es/revista/?q=content/normas-para-los-autores

Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea

Historical and Legal Analisys of the Fight against Cybercrime in the European Union

JOSÉ ENRIQUE ANGUITA OSUNA

Universidad Rey Juan Carlos, España

RESUMEN: La delincuencia informática se ha convertido en uno de los principales problemas del siglo XXI, y no ha dejado de ser una preocupación para las instituciones de la UE y los Estados miembros. En este trabajo se analizarán los primeros pasos dados por la UE en la lucha contra el cibercrimen, y se realizará un seguimiento de las principales actuaciones y mecanismos que la UE ha ido desarrollando para combatirla, y así tratar de proteger a sus ciudadanos, empresas y entidades de la Unión creando un nuevo marco basado en la ciberseguridad, dentro de una nueva Europa Digital.

PALABRAS CLAVE: Unión Europea, Cibercrimen, Delincuencia, Cooperación, Ciberserguridad

ABSTRACT: Cybercrime has become one of the most relevant issues in the 21st century, and it has not stopped concerning the European Union's (EU) institutions and its member States. In this work it will be analyzed the first steps taken by the EU to fight against Cybercrime, and it will follow up on the main actions and mechanisms that the EU has developed to combat it, and then try to protect its citizens, enterprises and entities of the Union creating a new frame based on Cybersecurity within a new digital Europe.

KEYWORDS: European Union, Cybercrime, Crime, Cooperation, Cybersecurity

Recibido: 29 de noviembre de 2017

Aceptado: 14 de diciembre de 2017

Revista de Estudios en Seguridad Internacional, Vol. 4, No. 1 (2018), pp. 107-126. http://www.seguridadinternacional.es/revista/

ISSN: 2444-6157. DOI: http://dx.doi.org/10.18847/1.7.7

ASPECTOS GENERALES: LA SOCIEDAD DE LA INFORMACIÓN

Los avances tecnológicos que están transformando la sociedad actual y las nuevas formas de delincuencia, en donde obviamente podemos incluir la delincuencia informática o ciberdelincuencia, se enmarcan dentro de la denominada Sociedad de la Información. Según Sieber desde mediados del siglo XX se produjeron tres cambios fundamentales que tuvieron repercusión en la evolución social. Nos estamos refiriendo, en primer lugar, a la evolución desde la Sociedad Industrial a la denominada Sociedad de la Información mediante la "Revolución Informática"; en segundo lugar, al desarrollo de la denominada Sociedad de Riesgos; y finalmente, la aparición de una Sociedad Global con pérdida de relevancia de las fronteras nacionales (Rovira del Canto, 1995: 14).

De este modo, la evolución desde la Sociedad Industrial hacia una nueva Sociedad de la Información (López Coronado, Abril Domingo y Mompó Gómez, 1999: 73-86) es un proceso en continua expansión, y que afecta a toda la sociedad en forma de red, y no en forma piramidal. La base que sustenta la Sociedad de la Información no es tanto la riqueza material, como los recursos intelectuales de las personas y su capacidad de procesar información y proyectar innovación, de modo que este componente de conocimiento e información implica que los elementos culturales son la base de poder, y este poder, la base del capital (Valls Carol, 2001-2010: 20).

Se puede definir la Sociedad de la Información como *"una sociedad en la que los ciudadanos sean capaces de hacer uso de diversos servicios de telecomunicaciones avanzados para mejorar los distintos aspectos de su vida cotidiana"* (López Coronado, Abril Domingo y Mompó Gómez, 1999: 73-86). No obstante, para otros miembros de la comunidad académica como Schiller, la Sociedad de la Información es *"la producción, proceso y transmisión de una cantidad muy elevada de datos relativos a todo tipo de cuestiones –individuales y nacionales, sociales y comerciales, económicas y militares–* "(Schiller, 1981).

Ha sido significativo en el estudio de la Sociedad de la Información la obra de Castells titulada "*La Era de la Información",* en donde se hace referencia a la la creación de *"una nueva estructura social dominante, la sociedad red; una nueva economía, la economía informacional/global; y una nueva cultura, la cultura de la virtualidad real"* (Castells, 1998: 370), añadiendo en su obra que ésta es la nueva estructura de la Era de la Información que se denomina *"sociedad red porque está compuesta por redes de producción, poder y experiencia, que construyen una cultura de la virtualidad en los flujos globales que trascienden el tiempo y el espacio*" (Castells, 1998: 385).

A partir de 1962 Marshall McLuhan acuñó el término *"Aldea Global"* para hacer referencia a aquellas comunidades cuyos miembros se comunicaban entre sí, y se interrelacionaban mediante el uso de los medios de comunicación de masas. Sin embargo, según Morón Lerma, actualmente esta expresión no carece de validez, puesto que considera que son unas notas que caracterizan a un determinado ámbito social, ya que es absolutamente asequible y normal conseguir información y comunicarse de forma rápida mediante el uso de los medios de comunicación de masas, como son el teléfono, la prensa escrita, la televisión, Internet, el fax, etc (Morón Lerma, 1999: 78).

Desde los últimos años del siglo XX se ha experimentado un incremento sin precedentes tanto de los avances científicos y tecnológicos como del uso de las nuevas tecnologías de la información y de la comunicación, aumentando la gestión de la información en todos sus sentidos, es decir, desde los tradicionales medios de

comunicación de masas, hasta el abundante caudal de información comercial y de todo tipo, que circula a través de Internet (López Coronado, Abril Domingo y Mompó Gómez, 1999: 73-86). Según el informe Bangeman, que se presentó al Consejo de la Unión Europea, la Sociedad de la Información *"tiene el potencial para mejorar la calidad de vida de los ciudadanos de Europa y la eficacia de la organización económica y, reforzar la cohesión social, haciendo referencia al mismo tiempo al "efecto multiplicador de la información" y a los rasgos esenciales de la infraestructura de la propia Sociedad de la Información basándose en la interconexión de redes y la interoperabilidad de servicios y aplicaciones para trabajar en conjunto"* (Bocco Nieto, 1998).

La información se ha convertido en la piedra angular del progreso social y humano, siendo un proceso paralelo a la actual e imprescindible utilización y desarrollo de las tecnologías de las telecomunicaciones, pasándose de simples llamadas telefónicas o de fax, a garantizar que toda la información pueda ser transmitida y recibida por todos los ciudadanos a través de una red universal y mediante unos terminales lo más estandarizados posibles (López Coronado, Abril Domingo y Mompó Gómez, 1999: 73-86).

A pesar de todos los grandes avances que se han producido en la Sociedad de la Información, y la ayuda que en el día a día nos aportan las nuevas tecnologías de la información y la comunicación, hay que hacer referencia a los efectos devastadores que pueden causar estas nuevas herramientas en el siglo XXI, si no se utilizan correctamente, con mesura, prudencia y responsabilidad. Desgraciadamente en el ámbito de actuación de las organizaciones criminales internacionales, europeas y nacionales, aprovechando las ventajas que aporta la Sociedad de la Información y las nuevas tecnologías, han aumentado los índices de la comisión de delitos informáticos, en sus diferentes formas, como son los fraudes informáticos, la violación del derecho a la intimidad, el acoso, o las extorsiones, entre otros.

La Unión Europea ha sido uno de los principales promotores de la Sociedad de la Información desde los años 90 del siglo pasado, llegando a adoptar un plan de actuación denominado *"Europa en marcha hacia la Sociedad de la Información"* que contenía el informe Bangemann de 1994. En 1996 se elaboró otro documento llamado *"Europa a la vanguardia de la Sociedad de la Información. Plan de actuación móvil"*. Asimismo, en la Cumbre de Helsinki de 1999 se presentó la iniciativa e-Europe para divulgar el uso de la Sociedad de la Información entre todos los ciudadanos europeos con un conjunto de acciones que tendrían que ser aprobadas en la Cumbre de Lisboa sobre el empleo en marzo del año 2000 (López Yepes, 2001: 14-15).

LA LUCHA CONTRA LA DELINCUENCIA INFORMÁTICA

Aspectos generales relativos a la delincuencia informática

En términos generales, el derecho penal y el derecho procesal penal clásicos fueron construidos sobre la base de un modelo de criminalidad física, marginal e individual (Fernández Teruelo, 2011: 16). No obstante, Internet ha supuesto una revolución tecnológica, pero al mismo tiempo, un problema para la represión de los delitos, puesto que existe una especial dificultad para la detección y persecución de los delitos informáticos, entre otros motivos, por el anonimato, la insuficiente conciencia de los

usuarios para mantener unas medidas preventivas de seguridad, o incluso el carácter transnacional de determinadas conductas delictivas (Fernández Teruelo, 2011: 16).

Las nuevas tecnologías e Internet constituyen unos de los principales impulsores de los cambios de muchas de las actividades desempeñadas por los ciudadanos, empresas, organizaciones y gobiernos en el actual mundo digital, convirtiéndoles en actores digitales cada vez más maduros e interactivos. Actualmente existen unos 2.400 millones de usuarios conectados a la red, de los que 540 millones se conectan desde Europa, y entre ellos, unos 29 millones se conectan desde España (Gómez Hidalgo, 2014: 81-82). El coste que provoca la ciberdelincuencia en la economía es enorme. Según un informe cada año las víctimas pierden unos 388.000 millones USD en todo el mundo a causa de la ciberdelincuencia, lo que convierte a este tipo delictivo, en un negocio más rentable que el comercio global conjunto de mariguana, cocaína y heroína (Comisión Europea, 2012: 2).

Para analizar la situación de la delincuencia organizada, y en concreto la ciberdelincuencia en la Unión Europea, son muy relevantes los datos aportados por el informe titulado *"Internet Organised Crime Threat Assessment"* (IOCTA), valoración estratégica anual, realizado por Europol sobre los delitos informáticos, en virtud de la cual se podrán adoptar mejores decisiones y establecer prioridades en el ámbito de la lucha contra los delitos informáticos, la explotación sexual infantil a través de Internet, los fraudes de pagos en la red, y otros tipos de delitos incluidos en este marco (Europol, 2016b: 19).

La lucha contra la delincuencia informática se encuadra en el Espacio de Libertad, Seguridad y Justicia de la Unión Europea, concretamente dentro del ámbito de la Europa de la Justicia, donde se articulan instrumentos y mecanismos para garantizar una cooperación judicial penal. Actualmente la lucha contra la delincuencia informáctica se debe desarrollar en el marco de la Estrategia de Europol 2016-2020 (Europol, 2016a: 5-20), en base a la cual deberán trabajar de forma coordinada las instituciones europeas, los Estados miembros, y otras entidades, como Europol, para combatir cualquier tipo de delincuencia. La Comisión Europea ha mostrado en reiteradas ocasiones su compromiso para luchar contra la delincuencia informática o ciberdelincuencia y sofocar cualquier crisis de ciberseguridad, sosteniendo que *"una respuesta eficaz ante los incidentes y crisis de ciberseguridad a gran escala a nivel de la UE requiere una cooperación rápida y eficaz entre todas las partes interesadas pertinentes y se basa en la preparación y en las capacidades de cada uno de los Estados miembros, así como en una acción común coordinada apoyada en las capacidades de la Unión"* (Comisión Europea, 2017d:2).

El artículo 82.1 del Tratado de Funcionamiento de la Unión Europea recoge el principio de reconocimiento mutuo y la aproximación de legislaciones en materia penal y procesal penal. Estos principios no fueron novedades del Tratado de Lisboa, puesto que el principio de reconocimiento mutuo en la cooperación judicial europea ya estaba contemplado desde su instauración oficial en el Consejo Europeo de Tampere de 1999, en el Programa de la Haya de 2005 y en el Programa de Estocolmo cuya vigencia comprendió los años 2010 y 2014 (Jimeno Bulnes, 2010). Para hacer efectiva la cooperación judicial penal, basada en el principio de reconocimiento mutuo de las resoluciones judiciales, el Parlamento Europeo y el Consejo podrán establecer normas mínimas conforme al procedimiento legislativo ordinario, respetando en todo caso, las tradiciones jurídicas de los Estados miembros. Para conseguirlo, será necesario fortalecer la confianza mutua que surgirá entre los Estados miembros a partir de la existencia en todos ellos, de normas y criterios penales y procesales, siendo necesaria

mucha confianza para avanzar en la cooperación penal sin que haya obstáculos ni trabas (Pérez Marín, 2013).

Los motivos que han provocado el aumento de la delincuencia informática son varios. Nos referimos a nuestras conductas, las cuales actualmente parece que únicamente se desarrollan en un contexto puramente digital, favorecidas por la absoluta digitalización de nuestra vida diaria, familiar, personal y profesional. El anonimato en la red es otra circunstancia que motiva la comisión de estos tipos delictivos, ya que se pueden cometer con más facilidad, pueden ser ocultados y pasar inadvertidos, y en ocasiones puede haber más dificultades para perseguirlos ante los tribunales (De la Mata Barranco, 2010: 19).

La sensación de miedo y temor en la sociedad cuando se navega en Internet, utilizan las redes sociales o realizan transacciones comerciales electrónicas existe. Actualmente el miedo al delito y la percepción de inseguridad son temas de interés para la investigación científica, los medios de comunicación, las instituciones competentes, y por supuesto para los ciudadanos. De modo que podemos definir el término de miedo al delito como *"la respuesta emocional de nerviosismo o ansiedad al delito o símbolos que la persona asocia al delito"* (De la Cuesta Arzamendi y San Juan Guillén, 2010: 69-70). Por tanto, la sociedad percibe que ha aumentado el nivel de riesgo de ser una víctima, lo que les produce ansiedad, inseguridad y desconfianza cuando utilizan las nuevas tecnologías de la información y la comunicación.

Desde un primer momento la Unión Europea fue consciente de los peligros que entrañan el uso incorrecto de las nuevas tecnologías de la información y comunicación, Internet y las redes sociales. En el año 1993 aprobó el Libro Blanco de la Comisión Europea sobre *"Crecimiento, competitividad, empleo. Retos y pistas para entrar en el siglo XXI"*(Comisión de las Comunidades Europeas, 1993), en el cual se intentaba reaccionar ante la convulsión social que suponían las nuevas tecnologías en nuestra sociedad, y asimismo, reconocía que el sector privado era el encargado de dirigir un proceso de creación de un espacio común de información, por lo que estimaba indispensable arbitrar un marco jurídico, que por un lado, fomentase su desarrollo, y por otro, garantizase el interés general (Morón Lerma, 1999: 102-103).

Desde el punto de vista de la criminología, según Bueno Arus, la delincuencia informática *"presenta dificultades especiales para su persecución en relación con la delincuencia tradicional, dada la rapidez de su comisión, el que puede tener lugar a distancia, y atendida la complejidad de la fijación de la autoría, así como la facilidad para encubrir el hecho y borrar las pruebas que habrían permitido enjuiciarlo"* (Rovira del Canto, 1995: 75). Ante la indeterminación del concepto de la delincuencia informátiva, la Comisión Europea elaboró su propia definición sobre la ciberdelincuencia en su Comunicación de 2007 denominada *"Hacia una política general de lucha contra la ciberdelincuencia"*. En esta Comunicación se establecía que el término ciberdelincuencia engloba tres tipos de actividades delictivas.

En primer lugar, comprende las formas tradicionales de delincuencia, como son el fraude o la falsificación, pero hemos de referirnos a estos delitos cometidos mediante las redes de comunicaciones y los sistemas de información electrónicos. En segundo lugar, se habla de contenidos ilegales a través de medios de comunicación electrónicos, como son las imágenes de abuso sexual a menores o incitaciones al odio racial. En tercer lugar, se hace referencia a los delitos específicos de las redes electrónicas, como por

ejemplo, los ataques contra los sistemas informáticos y la piratería (Comisión Europea, 2007: 2). Esta nueva amenaza sin duda tiene un carácter transfronterizo, lo que dificulta su investigación ya que la mayoría de los datos probatorios son intangibles y transitorios (Oficina contra la Droga y el Delito de Naciones Unidas UNOCD, 2005).

Hemos de añadir que la Oficina contra la Droga y el Delito de Naciones Unidas también realiza una aproximación al fenómeno de los delitos informáticos. Considera que éstos*"son conductas prescritas por la legislación y/o la jurisprudencia, que implican la utilización de las tecnologías digitales en la comisión del delito, se dirige a las propias tecnologías de la computación y las comunicaciones o incluye la utilización incidental de computadoras en la comisión de otros delitos"* (UNOCD, 2005).

Se pueden señalar algunos bienes jurídicos a tutelar en el derecho informático, siendo cada vez más las voces académicas que sostienen que en el ámbito de la ciberdelincuencia debe crearse una nueva categoría jurídica penal que englobe las conductas vinculadas con el derecho informático, y en donde se lesionen no solamente los bienes jurídicos tradicionales, sino también unos nuevos bienes jurídicos protegidos propios de la era digital. Según Hernández Díaz podemos identificar como bienes jurídicos protegidos en el delito informático a la intimidad informática, a la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos, a la intimidad informática o incluso la confianza en el funcionamiento de los sistemas informatizados (Hernández Díaz, 2010: 44-49).

La lucha contra la delincuencia informática se está desarrollando a nivel internacional, regional y nacional, no obstante, nosotros nos centraremos en el análisis de la lucha contra la delincuencia informática en la Unión Europea. La evaluación SOCTA UE de 2017 recomienda contemplar a la ciberdelincuencia como una de las cinco amenazas prioritarias. En concreto, según este estudio, se consideran amenazas prioritarias las siguientes: la ciberdelincuencia; el tráfico y la distribución de droga; el tráfico ilícito de migrantes; los robos y asaltos organizados; y la trata de seres humanos (Comisión Europea, 2017a: 7).

En el mes de julio de 2017 se publicó el *Noveno informe de situación relativo a una Unión de la Seguridad genuina y efectiva,* con carácter mensual, donde se explican los progresos realizados hacia la construcción de una Unión de seguridad genuina y efectiva, abordando la lucha contra el terrorismo, la delincuencia organizada y la ciberdelincuencia. En este informe se ha destacado la importante labor del Centro Europeo de Ciberdelincuencia (EC3) de Europol apoyando las autoridades nacionales en la lucha contra la ciberdelincuencia y la respuesta policial a los ciberataques a gran escala, mediante el asesoramiento forense o con información relacionada con la ciberdelincuencia, procedente de fuentes públicas, privadas e abiertas (Comisión Europea, 2017b: 7). Asimismo, se resalta la importancia de la cooperación entre las autoridades públicas y la industria en la lucha contra la ciberdelincuencia y la radicalización en Internet (Comisión Europea, 2017b: 8). Se destaca que la reunión informal de ministros de justicia y asuntos de interior de la UE celebrada en Tallin el pasado 7 de julio, se centró en la lucha contra la ciberdelincuencia, la lucha contra la corrupción y la reformas judiciales esenciales, donde se reiteró el compromiso conjunto de adoptar nuevas medidas para luchar contra la ciberdelincuencia y reforzar la ciberseguridad. Asimismo se debatieron los retos legislativos y operativos en la lucha contra la ciberdelincuencia con el fin de mejorar la cooperación a nivel regional e internacional (Comisión Europea, 2017b: 12).

Evolución histórica de la lucha contra la ciberdelincuencia en la Unión Europea

La preocupación en la Unión Europea por la lucha contra la delincuencia informática es muy antigua. Los términos de ciberdelincuencia, ciberdelito y análogos son más recientes, pero ello no impide que la Unión Europea se preocupara con anterioridad, por bienes jurídicos protegidos relacionados como la protección de los datos personales. La cooperación internacional es una de las mejores herramientas para luchar de forma eficaz contra la delincuencia transnacional. En el ámbito de la ciberdelincuencia, las principales propuestas internacionales para luchar contra los delitos cometidos a través de Internet, se han basado, por un lado, en una mayor armonización internacional de lo que debe considerarse ilícito, y por otro lado, en promover la cooperación entre las autoridades de los Estados miembros para mejorar la transmisión de pruebas (Ortíz Pradillo, 2013: 75).

En 1987 los profesores Sieber, Kaspersen, Vanderbergue y Stuurman elaboraron un informe denominado *"Los aspectos legales sobre el delito informático y la seguridad"*, cuyos aspectos más importantes fueron debatidos en 1990 en una conferencia conjunta de la Comisión Europea y del Consejo de Europa celebrada en Luxemburgo (Rovira del Canto, 1995:322). Quizá sea en el marco de la Unión Europea donde más avances se han logrado en la homologación normativa en materia de lucha contra la criminalidad informática en el ámbito internacional. Desde la aprobación del Tratado de Ámsterdam se fomentó la creación y desarrollo de un Espacio de Libertad, Seguridad y Justicia, con el respaldo de las conclusiones del Consejo Europeo de Tampere de 1999, que permitió adoptar iniciativas comunitarias durante la primera década del siglo XXI, dirigidas a adoptar medidas legislativas penales comunes en los Estados miembros de la Unión Europea para luchar contra la delincuencia informática (Flores Prada, 2012: 30-31).

Según De la Mata Barranco y Pérez Machío a finales del siglo XX se constituyeron varios instrumenros jurídicos que incluían una preocupación por las conductas delictivas que actualmente se engloban dentro de las delincuencia informática (De la Mata Barranco, Pérez Machío, 2010: 135-136). Entre las iniciativas y acciones llevadas a cabo por el Consejo de la Unión Europea en relación a la lucha contra la delincuencia informática destaca la *Decisión del Consejo del año 2000 relativa a la lucha contra la pornografía infantil en Internet* (Consejo de la Unión Europea, 2010), creado para reforzar la prevención y lucha contra la producción, el tratamiento, la posesión y la difusión de pornografía infantil.

Igualmente relevante fue la Comunicación adoptada en el año 2000 por la Comisión Europea denominada *"Creación de la Sociedad de la información mas segura mediante la mejora de la Seguridad de las infraestructuras de información y la lucha contra los delitos informáticos"* (Comisión Europea, 2001), en donde la Comisión Europea analizaba los diferentes caminos para mejorar la prevención de los delitos informáticos y la lucha contra cualquier actividad delictiva relacionada con las nuevas tecnologías de la información y la comunicación. Esta Comunicación tuvo su antecedente en el lanzamiento por la Comisión Europea de la denominada iniciativa eEuropa en 1999 (Comisión Europea, 1999), lo que permitió que la Unión Europea centrara su actuación en mejorar la protección de las infraestructuras de información y comunicación, y se adoptaran medidas para luchar contra el contenido ilícito y perjudicial en Internet, y así proteger los derechos de la propiedad intelectual y los datos de carácter personal.

Otro hito importante en la lucha contra la ciberdelincuencia fue el *Convenio de Budapest de 2001 sobre la ciberdelincuencia* adoptado en el Consejo de Europa. Aunque no es un intrumento en sentido estricto elaborado en el marco de la Unión Europea, fue considerado en el momento de su aprobación como el principal exponente regulatorio en la materia a nivel internacional (Jiménez García, 2014: 51). Constituye el principal instrumento internacional en materia de cooperación internacional en la lucha contra la delincuencia informática, y fue firmado en Budapest 23 de noviembre 2001, entró en vigor el mes de julio de 2004, y fue ratificado por España en 2010. Este instrumento permite la adhesión de Estados no miembros del Consejo de Europa (Canadá, Estados Unidos, Japón y Sudáfrica se han adherido). Asimismo, otros Estados han adaptado parte de su normativa al Convenio, aunque sin adherirse oficialmente a él. En definitiva, la Unión Europea siempre ha mostrado un fuerte interés en *"animar a todos los Estados miembros y terceros países a ratificar el Convenio del Consejo de Europa sobre el Cibercrimen"* (Ortíz Pradillo, 2013: 76). En el primer capítulo de este convenio se hace referencia a varias definiciones como son las de "sistema informático", "datos informáticos", "proveedor de servicios" y "datos sobre el tráfico" (Consejo de Europa, 2001: 4).

Por otra parte, fue destacable la adopción de la *Recomendación del Consejo del año 2001 relativa los puntos de contacto en los que se ofrecía un servicio ininterrumpido de 24 horas para luchar contra la delincuencia en el ámbito de la alta tecnología* (Consejo de la Unión Europea, 2001). En esta Recomendación se recomendaba que los Estados miembros que aún no se habían incorporado a la red de puntos de contacto de servicio ininterrumpido destinados a combatir la delincuencia de alta tecnología pudieran proceder a su incorporación (Consejo de la Unión Europea, 2001: 6).

Para contribuir a la protección de los datos personales y del derecho la intimidad, se aprueba la *Directiva 2002/58/CE, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad el sector de las comunicaciones electrónicas* (Parlamento Europeo, 2002), autorizando a los Estados miembros a que regulen por ley la obligación, a cargo de los prestadores de servicios, de conservar los datos electrónicos de tráfico de sus clientes, por razones de seguridad nacional, defensa, seguridad pública y lucha contra la criminalidad, durante un tiempo limitado, que será determinado libremente por cada Estado miembro (De la Mata Barranco y Pérez Machío, 2010: 135-136).

Con posterioridad se adoptó el *Reglamento de 2004 del Parlamento Europeo y del Consejo en virtud del cual se crea la Agencia Europea de Seguridad de las Redes y la Información* (Parlamento Europeo, 2004), en cuyos preceptos se incluye el ámbito de aplicación de la Agencia Europea de Seguridad de las Redes y de la Información, y se justificaba la creación de esta Agencia europea para *"garantizar un nivel efectivo y elevado de Seguridad de la red y de la información en la Comunidad y con el fin de desarrollar una cultura de la Seguridad de las redes de información en beneficio de los ciudadanos, los consumidores, las empresas y las organizaciones del sector público de la Unión Europea, lo que contribuirá al correcto funcionamiento del Mercado Interior*"[1].

Otro hito importante en la represión de la delincuencia informática en la Unión Europea lo constituyó la *Decisión Marco adoptada en 2005 por el Consejo relativa a*

[1] Artículo 1 del Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, DO nº L 77 de 13.3.2004.

los ataques de los que son objeto los sistemas de información (Consejo de la Unión Europea, 2005), cuyo objeto consistía en luchar contra la delincuencia informática y promover la seguridad de la información, reforzando la cooperación entre las autoridades judiciales, policiales y otras autoridades que tuvieran competencia en la lucha contra la delincuencia informática, a través, entre otras medidas, de aquellas que aproximen las normas jurídicas penales que luchen contra los ataques informáticos a los sistemas de información (Velascos San Martín, 2012: 111-112).

Del mismo modo se destaca la *Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 marzo 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones* (Parlamento Europeo, 2006), incorporándose en el contenido de esta norma comunitaria una estrecha relación entre el aumento de la importancia de los datos relativos al uso de comunicaciones electrónicas y la prevención, investigación, detección y enjuiciamiento de delitos, en especial contra la delincuencia organizada.

No es fácil realizar un análisis de la situación actual de este tipo de delincuencia, no obstante, se observaban una serie de tendencias:*"el número de delitos informáticos está aumentando y las actividades delictivas se están sofisticando e internacionalizando cada vez más; indicios inequívocos apuntan a una implicación creciente de grupos de delincuencia organizada en la ciberdelincuencia; sin embargo, el número de procedimientos incoados en Europa en el marco de la cooperación transfronteriza de los organismos encargados de la aplicación de ley no está aumentando"* (Comisión Europea, 2007).

La Comunicación del año 2007 elaborada por la Comisión Europea denominada *"Hacia una política general de lucha contra la Ciberdelincuencia"* (Comisión Europea, 2007), en donde en primer lugar, se realizaba una aproximación a términos parecidos como son los de "ciberdelincuencia", "delincuencia informática", "delincuencia relacionada con los ordenadores o "delincuencia de la tecnología", entendiéndose finalmente en esta comunicación que la "ciberdelincuencia" era considerada como las actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas (Comisión Europea, 2007: 2-4).

Otro hito importante en la lucha contra la delincuencia informática lo constituyó la Comunicación de la Comisión Europea de 2009 titulada *"Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia"*(Comisión Europea, 2009). Hemos de precisar que esta Comunicación se centraba en la prevención, preparación y el conocimiento, y en ella se definía un plan de medidas inmediatas para potenciar la seguridad y resistencia de las infraestructuras críticas de información (ICI).

Las autoridades comunitarias se propusieron dar un paso más en la lucha contra la delincuencia informática, y se plantearon aprobar un instrumento clave para contrarrestar el abuso sexual de menores en línea. Nos estamos refiriendo a la *Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011 relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil* (Parlamento Europeo, 2011), y por la que se sustituía a la Decisión marco 2004/68/JAI del Consejo. En virtud de esta directiva se trataba de luchar contra los abusos sexuales y explotación sexual de los menores, incluida la

pornografía infantil, siendo estas violaciones de derechos fundamentales, y en concreto los derechos del niño a la protección y los cuidados necesarios para su bienestar, reconocidos en la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989 y la Carta de los Derechos Fundamentales de la Unión Europea. El delito de la explotación sexual de los menores y la pornografía infantil exige la adopción de un marco común que incluya la acción judicial contra los delincuentes, y garantice la protección de los menores víctimas y la prevención de estas actividades delictivas, salvaguardándose siempre el interés superior del menor.

Otro elemento clave para luchar contra la delincuencia informática es el Centro Europeo de Ciberdelincuencia (EC3), creado en 2013 como parte de Europol (Comisión Europea, 2012). La Comisión Europea propuso la creación de este centro, como una parte de Europol, estando orientado hacia la lucha contra la ciberdelincuencia en la Unión Europea. En la comunicación de la Comisión Europea, que plantea su creación y desarrollo, se propone que esta nueva entidad centre su lucha contra las siguientes parcelas de la ciberdelincuencia: ciberdelitos cometidos por grupos de la delincuencia organizada, especialmente los que generan extensos réditos ilegales mediante el fraude en línea; ciberdelitos que provocan daños graves a sus víctimas, como la explotación sexual de menores en línea; y ciberdelitos (incluidos los ciberataques) que afectan a infraestructuras y sistemas de información esenciales de la Unión (Comisión Europea, 2012: 4-6).

La Unión Europea tiene la obligación de garantizar la libertad y democracia dentro de sus fronteras, y para ello se elaboró una Comunicación donde se plantea la necesidad de crear un entorno digital más seguro, garantizando un funcionamiento adecuado de las nuevas tecnologías de la información y la comunicación, de modo que, se proyectó crear una Europa digital más fuerte y segura (Comisión Europea, 2013). La mencionada Comunicación plantea el desarrollo de la *Estrategia de Ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro* en 2013, en virtud de la cual, se trata de garantizar el respeto de los principales principios de la ciberseguridad a nivel nacional, europeo e internacional. Los principios a los que nos referimos son los siguientes: los valores esenciales de la Unión Europea no son tanto en el mundo físico como en el digital; la protección de los derechos fundamentales, la libertad de expresión, los datos personales y la intimidad; el acceso para todos; la gobernanza multilateral democrática y eficaz; y garantizar la seguridad, siendo una responsabilidad compartida (Comisión Europea, 2013: 4).

Se puede destacar la aprobación de la *Directiva de 2013 relativa a ataques sobre sistemas de información* (Parlamento Europeo, 2013), cuyo objeto consiste en *"aproximar las normas de Derecho penal de los Estados miembros en materia de ataques contra los sistemas de información, mediante el establecimiento de normas mínimas relativas a la definición de las infracciones penales y las sanciones aplicables, y mejorar la cooperación entre las autoridades competentes, incluida la policía y los demás servicios especializados encargados de la aplicación de la ley en los Estados miembros, así como los organismos especializados de la Unión, como Eurojust, Europol y su Centro Europeo contra la Ciberdelincuencia y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)"*[2]. Este instrumento trata de armonizar las normas relativas a los delitos y las penas relativas a algunos delitos contra los sistemas de información. Los principales tipos penales que se incluyen

[2] Considerando nº 1 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra sistemas de información, DO L 218/8, 14.08.2013.

son los ataques contra los sistemas de información, entre los que se encuentran los ataques de denegación de servicio, concebidos para dejar fuera de servicio un servidor, la interceptación de datos o el ataque de botnets.

Medidas y mecanismos recientes para mejorar la ciberseguridad en la Union Europea

Según los estudios realizados por Davara Fernández, el concepto de Ciberseguridad *"debe ser tomado en base a su objetivo, esto es, preservar la seguridad, integridad y confidencialidad de todos los activos de una entidad u organismo, ya sea éste de carácter público o privado, teniendo en cuenta los riesgos –tanto internos como externos- a los que se exponen"* (Davara, 2017: 257).

En este campo se fueron aprobando recientemente nuevos instrumentos y medidas que plantean la profundización en la lucha contra la delincuencia informática, y al mismo tiempo tratan de consolidar la ciberseguridad dentro de la Unión. En 2008 se elaboró en la Unión Europea la *Estrategia de Ciberseguridad*, donde se determinan los activos que hay que proteger, priorizando la protección de los derechos fundamentales, la libertad de expresión, los datos personales y la intimidad (Morán Blanco, 2017: 209). Asimismo, se procedió a la aprobación y publicación de la *Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión* (Parlamento Europeo, 2017a).

Esta norma establece medidas con el objeto de lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior. Además, según el artículo primero de la citada Directiva se imprementarán ciertas medidas, entre las cuales se pueden destacar las siguientes: establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información; crea un grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos; crea una red de equipos de respuesta a incidentes de seguridad informática con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz[3].

La Comunicación de 2016 titulada *"Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora"*, propuso a los Estados miembros que se esforzaran por sacar el máximo partido a la Directiva (UE) 2016/1148, relativa a la seguridad de las redes y sistemas de información ("Directiva SRI"), sobre medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. De este modo, sería posible potenciar la cooperación transfronteriza para estar preparados ante cualquier ciberincidente a gran escala. Asimismo, estableció que se obtendrían mejores resultados, si se creaba un enfoque coordinado de la cooperación ante las crisis entre los diferentes elementos del ecosistema cibernético, que se debería plasmar en un "plan director" (Comisión Europea, 2017d: 3).

[3] Artículo 1 de la Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, DOUE, 19.7.2017, L 194/1.

En las Conclusiones del Consejo Europeo celebrado el 22 y 23 de junio de 2017 se recordó que la Unión Europea, durante toda su trayectoria, *"ha dedicado su atención al fortalecimiento de Europa y a la protección de los ciudadanos mediante medidas eficaces destinadas a luchar contra el terrorismo y a desarrollar su seguridad y defensa comunes…"*. Dentro del marco de la lucha antiterrorista, el Consejo Europeo condenó los recientes atentados terroristas, y ha mantenido su postura firme en la lucha contra el terrorismo, el odio y el extremismo violento, de modo que ha fortalecido la determinación de cooperar a escala de la Unión Europea para reforzar nuestra seguridad interior y combatir la propagación de la radicalización en Internet. Asimismo, el Consejo Europeo entendió que un acceso efectivo a las pruebas electrónicas es fundamental para la lucha contra la delincuencia grave y el terrorismo, y que al mismo tiempo, debe asegurarse la disponibilidad de los datos (Consejo Europeo, 2017: 1-2). Asimismo, actualmente los grupos terroristas utilizan las tecnologías de la información y comunicación (TIC) para diferentes fines, como es la difusión de la propaganda, que puede incluir contenidos basados en comunicaciones de audio e imágenes de vídeo de actos de violencia, presentaciones en las que incorporan instrucciones ideológicas, y animan a los usuarios seguir su causa (Morán Blanco, 2017: 205). Según señala Javier Jordán, *"la propaganda que se distribuye a través de esas comunidades virtuales transmite elementos racionales, emocionales y cognitivo-normativos y dicha comunicación pública refuerza los valores y convicciones del imaginario yihadista"* (Jordán, 2009: 197-216).

Finalmente, respecto al desarrollo de la Europa digital, en el Consejo Europeo celebrado el 22 y 23 de junio de 2017, se debatió y pusieron en común propuestas que se plantearían en la cumbre digital celebrada en Tallin el 29 de septiembre de 2017. El Consejo Europeo recordó la importancia global de tener una visión digital ambiciosa para Europa, su sociedad y su economía. Además de planterar otras cuestiones, se hizo hincapié en tratar de mejorar la ciberseguridad en Europa, y con el fin de hacer frente a los retos actuales y futuros en materia de ciberseguridad, el Consejo Europeo refrendó el objetivo de la Comisión Europea de revisar la Estrategia de Ciberseguridad en el mes de septiembre de 2017 y de plantear más acciones selectivas antes de que finalizase el año (Consejo Europeo, 2017: 12).

El pasado 13 de septiembre de 2017 se publicó la Comunicación de la Comisión Europea titulada *"Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE*" (Comisión Europea, 2017c), donde se insta a mejorar la cooperación transfronteriza relativa a la preparación y prevención ante cualquier ciberincidente a gran escala. Por otro lado, se recuerda que sería conveniente establecer un "plan director" que creara un enfoque coordinado de la cooperación ante las crisis entre los diferentes elementos del ecosistema cibernético. En la mencionada Comunicación se resalta la importancia que la ciberseguridad tiene para nuestra prosperidad y seguridad, ya que la vida cotidiana de los ciudadanos europeos y la economía cada vez dependen más de las tecnologías digitales (Comisión Europea, 2017c: 2-3).

En definitiva, se requiere reforzar la resiliencia de la Unión Europea a los ciberataques, por lo que habrá que adoptar un enfoque colectivo y amplio, implantando medidas de diferente tipo (Comisión Europea, 2017c: 4-14):

— Fortalecer la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA). La Comisión presentará un proyecto de reforma que incorpore un mandato permanente de la agencia[4].

— Creación de un mercado único de la Ciberseguridad.

— Aplicación plena de la Directiva relativa a la seguridad de las redes y sistemas de información. Es necesario fortalecer las normas que regulan la ciberdelincuencia y ciberseguridad.

— Resiliencia mediante una respuesta rápida de emergencia. Es necesario tener respuestas rápidas y eficaces ante un ataque cibernético, para poder disminuir su impacto. La Comisión Europea ha propuesto la creación de un plan director que asegure un proceso eficaz de respuesta operativa a nivel de la Unión y de los Estados miembros ante un incidente cibernético a gran escala.

— Creación de una red de competencias en ciberseguridad con un Centro Europeo de Competencia e Investigación en ciberseguridad. La capacidad de la ciberseguridad de la Unión Europea continuará reforzándose mediante una red de centros de competencia ciberseguridad, cuyo eje será un Centro Europeo de Competencia e Investigación en Ciberseguridad, que fomentarán el desarrollo de tecnología de la ciberseguridad y complementarán los esfuerzos de capacitación en este ámbito a nivel nacional y de la UE.

— Creación de una base sólida de competencias cibernéticas de la UE. Deben adoptarse medidas para fomentar la educación en el ámbito de la ciberseguridad.

— Promover la ciberhigiene y la ciberconcienciación. Las Administraciones Públicas, las empresas y la ciudadanía deben tratar que todo el mundo entienda la amenaza que supone la ciberdelincuencia.

Por otra parte en la comunicación que estamos analizando se observa la necesidad de crear una ciberdisuasión efectiva en la Unión Europea, mediante la aplicación de medidas que sean creíbles y disuasorias para potenciales ciberdelincuentes y ciberatacantes. La directiva relativa a ataques contra los sistemas de información de 2013[5] supuso un gran avance en la lucha penal contra los ciberataques, no obstante, todavía se pueden mejorar los resultados en la aplicación de esta directiva. Sin embargo, la Comisión Europea plantea la aplicación de mejores medidas para reforzar la ciberseguridad (Comisión Europea, 2017c: 14-23):[6]

— Identificar a los actores maliciosos.

— Reforzar la respuesta policial. A pesar de que la investigación y la adopción de acciones penales contra la ciberdelincuencia son eficaces, se debe mejorar el

[4] PARLAMENTO EUROPEO: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), Brussels, 13.9.2017, COM(2017) 477 final, 2017/0225(COD).

[5] PARLAMENTO EUROPEO: Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, DOUE, 14.8.3013, L 218/8.

[6] COMISIÓN EUROPEA: Comunicación conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la Ciberseguridad de la UE, Bruselas, 13.9.2017, *op. cit*., pp. 14-23.

marco procesal para adaptarse mejor a las nuevas tecnologías y a Internet. Según se planteó en el marco de la Agenda Europea de Seguridad, a principios de 2018 la Comisión Europea va a presentar propuestas para facilitar el acceso transfronterizo a las pruebas electrónicas[7].

— Cooperación de los sectores público y privado contra la ciberdelincuencia. La cooperación con el sector privado, industria y sociedad civil es clave para que las autoridades públicas puedan luchar con eficacia contra la delincuencia.

— Reforzar la respuesta política. La colaboración política se consigue gracias a la aplicación del "conjunto de instrumentos de la ciberdiplomacia", para establecer vínculos de comunicación y diplomáticos en relación a las actividades cibernéticas maliciosas[8].

— Aumentar la disuasión de la ciberseguridad a través de la capacidad de defensa de los Estados miembros.

— Fortalecer la cooperación internacional en materia de seguridad.

A continuación vamos a mostrar una síntesis de las Recomendaciones que el pasado 13 de septiembre de 2017 planteó la Comisión Europea a los Estados miembros para mejorar la ciberseguridad en la Unión (Comisión Europea, 2017d: 6-8):

"1. Los Estados miembros y las instituciones de la UE deben crear un Marco de respuesta a las crisis de ciberseguridad de la UE donde se integren los objetivos y las modalidades de la cooperación que se presentan en el Plan director siguiendo los principios rectores allí descritos.

2. El Marco de respuesta a las crisis de ciberseguridad de la UE debe identificar en especial a los agentes, instituciones de la UE y autoridades de los Estados miembros que sean pertinentes, a todos los niveles necesarios (técnico, operativo y estratégico/político) y elaborar, en caso necesario, procedimientos de trabajo normalizados que definan cómo han de colaborar en el contexto de los mecanismos de gestión de crisis de la UE. Debe hacerse hincapié en permitir el intercambio de información, sin demoras indebidas, y en coordinar la respuesta durante incidentes y crisis de ciberseguridad a gran escala.

3. A tal fin, las autoridades competentes de los Estados miembros deben trabajar juntas en el sentido de especificar en mayor medida los protocolos de cooperación y de intercambio de información. El Grupo de cooperación debe intercambiar sus experiencias sobre estas cuestiones con las instituciones pertinentes de la UE.

4. Los Estados miembros deben velar por que sus mecanismos nacionales de gestión de crisis den la respuesta adecuada a los incidentes de ciberseguridad y establezcan los procedimientos necesarios para la cooperación a nivel de la UE en el contexto del Marco de la UE.

5. Por lo que se refiere a los mecanismos existentes de gestión de crisis de la UE, en consonancia con el Plan director, es conveniente que los Estados miembros, junto con los servicios de la Comisión y el SEAE, establezcan directrices para la aplicación

[7] PARLAMENTO EUROPEO: Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión marco 2001/413/JAI del Consejo, Bruselas, 13.9.2017, COM(2017) 489 final, 2017/0226 (COD).

[8] CONSEJO DE LA UNIÓN EUROPEA: Conclusiones del Consejo sobre la ciberdiplomacia, Bruselas, 11 de febrero de 2015 (OR. en), 6122/15.

práctica por lo que respecta a la integración de sus entidades y procedimientos nacionales en materia de gestión de crisis y ciberseguridad en los mecanismos existentes de gestión de crisis de la UE, a saber, el DIRPC y el CRM del SEAE. En particular, los Estados miembros deben velar por la existencia de estructuras apropiadas que permitan el flujo eficiente de información entre sus autoridades nacionales de gestión de crisis y sus representantes a nivel de la UE en el contexto de los mecanismos de crisis de la UE.

6. Los Estados miembros deben hacer pleno uso de las oportunidades que ofrece el programa de infraestructuras de servicios digitales (ISD) del Mecanismo «Conectar Europa» (MCE), y cooperar con la Comisión para que el mecanismo de cooperación de plataforma central de servicios, actualmente en elaboración, aporte todas las funcionalidades necesarias y cumpla sus requisitos para la cooperación también durante las crisis de ciberseguridad.

7. Los Estados miembros, con la ayuda de la ENISA y sobre la base de los trabajos realizados anteriormente en este ámbito, deben cooperar en la elaboración y la adopción de una taxonomía y un formato comunes para los informes de situación a fin de describir las causas técnicas y las consecuencias de los incidentes de ciberseguridad y reforzar su cooperación técnica y operativa durante las crisis. A este respecto, los Estados miembros deben tener en cuenta el trabajo en curso del Grupo de cooperación en relación con las directrices sobre notificación de incidentes, y en particular los aspectos relacionados con el formato de las notificaciones nacionales.

8. Los procedimientos establecidos en el Marco deben someterse a prueba y, en caso necesario, modificarse tras las lecciones aprendidas de la participación de los Estados miembros en los ejercicios de ciberseguridad a escala nacional, regional y de la Unión, así como en los de la ciberdiplomacia y de la OTAN. En particular, deben someterse a prueba en el contexto de los ejercicios de CyberEurope organizados por la ENISA. CyberEurope 2018 representa la primera de tales oportunidades.

9. Los Estados miembros y las instituciones de la UE deben practicar regularmente su respuesta a los incidentes y crisis de ciberseguridad a gran escala a nivel nacional y europeo, incluida su respuesta política, cuando sea necesario y con la participación de entidades del sector privado según proceda".

CONCLUSIONES

El trabajo de los Estados miembros y la Unión Europea en la lucha contra la delincuencia informática ha sido muy positivo durante los últimos años, mediante la aplicación de instrumentos normativos, iniciativas, políticas y proyectos para mejorar la calidad de vida de los ciudadanos europeos, haciéndola más segura ante la proliferación de las actividades delictivas informáticas. A pesar de los grandes logros conseguidos en los últimos años en la lucha contra la ciberdelincuencia, todavía queda mucho trabajo por realizar, y por ello debemos de hacer frente a una serie de retos en el futuro más cercano. A continuación vamos a mostrar algunos de los retos actuales de la ciberdelincuencia en la Unión Europea.

Dificultad de la persecución de delitos los informáticos. La dificultad reside en el funcionamiento de los sistemas informáticos y en la estructura de Internet, ya que se trata de una estructura mundial con canales digitales que dificultan el control fronterizo,

se favorece el alto nivel de opacidad de las conexiones y el anonimato de los internautas, y de momento existe una generalizada libertad normativa y lagunas legales.

Especialización de las autoridades judiciales y policiales. Es necesario contar con la formación y especialización necesaria de la policía y de los jueces y tribunales, para que cuenten con el apoyo de técnicos y de nuevos mecanismos de investigación, así como con mejores instrumentos legislativos que regulen los medios de prueba tecnológicos. Debe continuar la cooperación internacional entre cuerpos policiales de todos los Estados miembros, hay que crear fiscalías especiales, y modificar las normativas procesales nacionales para introducir medidas de interceptación de comunicaciones informáticas, datos de navegación o rastreo de contenidos delictivos.

Delitos de alta tecnología, ciberataques y programas maliciosos. Han aumentado los ataques con malwares, de los cuales el 50% de estos programas no son detectados por los antivirus. También se extienden los gusanos, troyanos, webs maliciosas, de las cuales el 88% se encuentran en Europa y Norteamérica.

Fraudes en pagos. Una de las actividades principales es la manipulación de las credenciales que perjudican a los titulares de tarjetas de crédito, la proliferación de talleres ilegales de fabricación de dispositivos y programas para manipular los terminales de puntos de venta o la clonación de tarjetas de crédito.

Explotación infantil en la Red. Hay que continuar la lucha contra la explotación sexual infantil en la Unión Europea, eliminando las redes ilegales de pederastas que explotan sexualmente en línea a menores mediante servicios ocultos, y mejorar la operación internacional de los cuerpos de policía europeos para investigar las redes de producción y distribución de material sobre abusos infantiles en las plataformas de Internet.

Crecimiento del número de delincuentes. El número de actos delictivos y de delincuentes en el marco de la ciberdelincuencia ha continuado aumentando en los últimos años, ampliando sus campos de acción a otros sectores de la economía, creándose una economía clandestina en la que se comercia con drogas, armas, se abusa de menores, y existe la sustracción de documentos oficiales, asesinatos, etc.

Fomento de la globalización. La globalización y la expansión de Internet y su número de usuarios provocarán un aumento de la comisión de ciberdelitos en lugares que en principio no tenían tanto acceso a las redes, de modo que se prevé un incremento de la ciberdelincuencia en América del Sur, África y Asia.

Pirateo de servicios en la nube. No solamente se cometen ciberdelitos mediante el "Pirateo" de los medios visuales, audiovisuales, intelectuales o industriales, sino que se prevé un aumento del pirateo de los servicios en la nube, ya que es una actividad muy lucrativa que permitirá a los delincuentes espiar para obtener datos de las víctimas y poder extorsionarlas.

NOTA SOBRE EL AUTOR:

José Enrique Anguita Osuna es Doctor y Profesor Visitante en la Universidad Rey Juan Carlos de Madrid, España.

REFERENCIAS

Bocco Nieto, M. E. (1998). Sociedad de la Información: un flujo de información a lo largo de la historia. *Revista latina de comunicación social,* (9).

Castells, M. (1998). *La era de la información. Fin de milenio*. Madrid: Alianza editorial.

Comisión de las Comunidades Europeas (1993). *Libro Blanco, "Competitividad, Empleo Retos y Pistas para entrar en el siglo XXI.* Luxemburgo, Boletín de las Comunidades Europeas. Suplemento 6/93.

Comisión Europea (1999). *Comunicación, de 8 de diciembre de 1999, relativa a una iniciativa de la Comisión para el Consejo Europeo extraordinario de Lisboa de 23 y 24 de marzo de 2000: eEurope - Una sociedad de la información para todos*, COM (1999) 687.

Comisión Europea (2001). *Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones: Creación de una sociedad de la información más segura mediante la mejora de la Seguridad de las infraestructuras de información y la lucha contra los delitos informáticos*, Bruselas, 26.1.2001, COM (2000) 890 final.

Comisión Europea (2007). *Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones, de 22 de mayo de 2007, "Hacia una política general de lucha contra la ciberdelincuencia"*, Bruselas 22.5.2007, COM (2007) 267 final.

Comisión Europea (2009). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 30 de marzo de 2009, sobre protección de infraestructuras críticas de información: "Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, Seguridad y resistencia"*, Bruselas, 30.3.2009, COM(2009) 149 final.

Comisión Europea (2012). *Comunicación de la Comisión al Consejo y al Parlamento Europeo: La represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia,* Bruselas*,* 28.3.2012 COM(2012) 140 final.

Comisión Europea (2013). *Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro*, Bruselas, 7.2.2013, JOIN(2013) 1 final.

Comisión Europea (2016). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. "Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora*, Bruselas, 5.7.2016, COM(2016) 410 final.

Comisión Europea (2017a). *Informe de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo. Sexto informe de situación relativo a una Unión de la seguridad genuina y efectiva*, Bruselas, 12.4.2017, COM(2017) 213 final.

Comisión Europea (2017b). *Informe de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo. Noveno informe de situación relativo a una Unión de la seguridad genuina y efectiva*, Bruselas, 26.7.2017, COM(2017) 407 final.

Comisión Europea (2017c). *Comunicación conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la Ciberseguridad de la UE*, Bruselas, 13.9.2017, JOIN(2017) 450 final.

Comisión Europea (2017d*). Recomendación de la Comisión de 13.9.2017 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala*, Bruselas, 13.9.2017, C(2017) 6100 final.

Consejo de Europa (2001). *Convenio del Consejo de Europa sobre la Ciberdelincuencia*, Budapest, 23.11.2001.

Consejo de la Unión Europea (2000). *Decisión del Consejo, de 29 de mayo de 2000, relativa a la lucha contra la pornografía infantil en Internet*, DO L 138 de 9.6.2000.

Consejo de la Unión Europea (2001). *Recomendación del Consejo, de 25 de junio de 2001, relativa a los puntos de contacto en los que se ofrece un servicio ininterrumpido de veinticuatro horas para luchar contra la delincuencia en el ámbito de la alta tecnología*, DO C 187 de 3.7.2001.

Consejo de la Unión Europea (2005). *Decisión marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques de los que son objeto los sistemas de información*, DO L 69 de 16. 3. 2005.

Consejo de la Unión Europea (2015). *Conclusiones del Consejo sobre la ciberdiplomacia*, Bruselas, 11 de febrero de 2015 (OR. en), 6122/15.

Consejo Europeo (2017*). Conclusiones del Consejo Europeo de 22 y 23 de junio de 2017*.

Cuesta Arzamendi, J. L. y San Juan Guillén, C. (2010). La cibercriminalidad: interés y necesidad de estudio. Percepción de seguridad e inseguridad. *Derecho Penal Informático*, dirigido por José Luis de la Cuesta Arzamendi, Ed. Civitas.

Davara Rodríguez, M. Á. (Coordinador), Davara Fernández de Marcos, Elena, Davara Fernández de Marcos, Laura (2017). *Delitos informáticos*. Navarra: Editorial Aranzadi.

De la Mata Barranco, N. J. (2010). Ilícitos vinculados al ámbito informático: la respuesta penal. *Derecho Penal Informático*, dirigido por José Luis de la Cuesta Arzamendi, Ed. Civitas, 15 – 30.

De la Mata Barranco, N. J. y Perez Machío, A. I. (2010). La normativa internacional para la lucha contra la cibercriminalidad como referente de la regulación penal española. *Derecho Penal Informático*, dirigido por José Luis de la Cuesta Arzamendi, Navarra, Ed. Civitas, 123 – 145.

Europol (2016a). *Europol Strategy 2016-2020*. Luxemburgo, Publications Office of the European Union.

Europol (2016b). *Europol Review. General Report on Europol activities 2015*. La Haya, European Police Office.

Fernández Teruelo, J. G. (2011). *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*. Valladolid: Lex Nova.

Flores Prada, I. (2012). *Criminalidad informática. Aspectos sustantivos y procesales*, Monografías 818. Valencia: Ed. Tirant lo Blanch.

Gómez Hidalgo, M. (2014). Ciberseguridad y protección en la Red: los certs/csirts. En E. Jordá Capitán y V. De Priego Fernández (Directoras), *La protección y seguridad de la persona en Internet: aspectos sociales y jurídicos*. Madrid: Editorial Reus.

Hernández Díaz, L. (2010). Aproximación a un concepto del derecho penal informático. *Derecho Penal Informático*, dirigido por José Luis de la Cuesta Arzamendi, Navarra, Ed. Civitas, 31 – 54.

Jiménez García, F. (2014). La ciberseguridad en el marco internacional. El sistema del Convenio de Budapest de 2001 sobre la ciberdelincuencia adoptado en el Consejo de Europa. En E. Jordá Capitán y V. De Priego Fernández (Directoras), *La protección y seguridad de la persona en Internet: aspectos sociales y jurídicos*. Madrid: Editorial Reus.

Jimeno Bulnes, M. (2010). Las implicaciones del Tratado de Lisboa en la cooperación judicial europea en materia penal. En C. Arangüena Fanego (), *Espacio Europeo de Libertad, Seguridad y Justicia: últimos avances en cooperación judicial penal*. Valladolid: Lex Nova.

Jordán, J. (2009). Proceso de radicalización yihadista en España. Análisis sociopolítico en tres niveles. *Revista de Psicología Social*, *24*, 197 – 216.

López Coronado, M., Abril Domingo, E. J. y Mompó Gómez, R. (1999). La necesidad de indicadores sociales y económicos para el estudio de la evolución de la sociedad de la información. *Revista de investigación económica y social de Castilla y León*, (1), 73 - 86.

López Yepes, J. (2001). La política de la Sociedad de la Información en España. (Jornadas de documentación administrativa y Sociedad de la información. Zaragoza, 22-24 octubre 2001), *Documentación de las Ciencias de la Información*, (24), 14 – 15.

Morán Blanco, S. (2017). La ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo. *Revista Española de Derecho Internacional*, *69*, (2), 195 – 221.

Morón Lerma, E. (1999). Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red. *Revista de Derecho y Proceso Penal*, (1), Navarra: Ed. Aranzadi.

Oficina contra la Droga y el Delito de Naciones Unidas (2005). *Delitos Informáticos* (11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal 18 a 25 abril 2005, Bangkok, Tailandia).

Ortiz Pradillo, J. C. (2013). *Problemas procesales de la ciberdelincuencia*. Madrid: Editorial Colex,.

Parlamento Europeo (2002). *Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas*, DOUE, L 201/37, 31.7.2002.

Parlamento Europeo (2004). *Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información*, DOUE L 77 de 13.3.2004.

Parlamento Europeo (2007). *Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones, de 22 de mayo de 2007, "Hacia una política general de lucha contra la ciberdelincuencia"*, Bruselas 22.5.2007, COM (2007) 267 final.

Parlamento Europeo (2011). *Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo*, DOUE L335/1 de 17.12.2011.

Parlamento Europeo (2013). *Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra sistemas de información*, DOUE L 218/8, 14.08.2013.

Parlamento Europeo (2017a). *Directiva 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*, DOUE, L 194/1, 19.7.2017.

Parlamento Europeo (2017b). *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")*, Brussels, 13.9.2017, COM(2017) 477 final, 2017/0225(COD).

Parlamento Europeo (2017c). *Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y por la que se sustituye la Decisión marco 2001/413/JAI del Consejo*, Bruselas, 13.9.2017, COM(2017) 489 final, 2017/0226 (COD)

Pérez Marín, M. A. (2013). *La lucha contra la criminalidad en la Unión Europea. El camino hacia una jurisdicción penal común*. Barcelona: Ed. Atelier.

Rovira del Canto, E. (2002). *Delincuencia informática y fraudes informáticos*. Granada: Editorial Comares.

Schiller, H. (1981). *Who knows: information i the age of the fortune 500*. 1ª edición, Norwood, 1981. El poder informático. Imperios Tecnológicos y relaciones de dependencia. México: Ediciones Gustavo Gili S.A.

Téllez Valdés, J. (1996). Los delitos informáticos. Situación en México. *Informática y Derecho,* (9-11), UNED, Mérida, Centro Regional de Extremadura.

Valls Carol, M. R. (2001). Educación permanente y Sociedad de la información. *Tabanque: Revista pedagógica*, (16).

Velasco Nuñez, E. (2010). *Delitos cometidos a través de Internet. Cuestiones procesales*, Ed. La Ley.

Velasco San Martin, C. (2012). *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e Internet*. Valencia: Tirant Monografías 807.