Revista Internacional de
Doctrina y Jurisprudencia

Volumen 26, Diciembre de 2021

CIBERCRIMINALIDAD: HACIA LA NUEVA REALIDAD -VIRTUAL- DEL DERECHO PENAL

Jacinto Pérez Arias[1]
Universidad de Murcia
Email. jacintoperez@um.es

RESUMEN: El fenómeno de la cibercriminalidad se expande cada vez más. Y lo hace de una manera desterritorializada y anónima. Esta situación provoca una lógica preocupación en el derecho penal y la criminología. El presente estudio pretende aproximarse a la problemática de la cibercriminalidad, partiendo de su conceptos y contexto, e intentando describir los problemas que plantea su tratamiento jurídico-penal y análisis criminológico, así como planteando algunas soluciones provisionales de lege ferenda.

Palabras clave: Derecho Penal, Criminología, cibercriminalidad, cibercrimen, ciberdelincuente, víctima, nuevas tecnologías, delito.

ABSTRACT: The phenomenon of cybercrime is expanding more and more. And it does so in a deterritorialized and anonymous way. This situation causes a logical concern in criminal law and criminology. This study aims to approximate the problem of cybercrime, starting from its concepts and context, trying to describe the problems posed by its legal-criminal treatment and criminological analysis, as well as proposing some provisional solutions in Spanish criminal law

Keywords: Criminal Law, Criminology, cybercrime, cybercriminal, victim, new technologies, crime.

*ISSN 2255-1824

I. INTRODUCCIÓN

No puede extrañar que, en la era de la ciber-civilización[2], la sociedad muestre su preocupación por conocer el nivel de protección que el Derecho confiere a víctimas de delitos

1 Profesor de Derecho Penal y Criminología. Universidad de Murcia.

2 Sorprende leer que Wiener, en el año 1958, afirmara que "*Desde que terminó la segunda guerra mundial, he trabajado en la teoría de los mensajes. Además de la parte electrotécnica de su transmisión, existe un campo muy amplio que*

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

cometidos a través de un medio tecnológico. Y dentro de esta protección, es aún más lógico que la sociedad se cuestione (y con mayor motivo los intérpretes) si, el Derecho Penal, ha sido debidamente actualizado y modernizado hasta el punto de otorgar protección frente a determinados delitos que discurren por medios, y fines, por completo desconocidos, hasta fechas muy recientes.

El Derecho Penal no queda extramuros de todo este nuevo mundo. Por ello, se ha afirmado que *la revolución social y técnica que implican las nuevas tecnologías traen consigo también efectos en lo que al Derecho penal respecta* (MATA Y MARTÍN[3]).

Para aclarar y responder tales cuestiones, debemos valorar, como premisa, si existe diferencia entre la categoría -ya conocida- de delitos informáticos y aquella otra que, avanzando algo más, habla de cibercriminalidad. El desarrollo de esta importante distinción -si acaso existiera, que no anticipamos- ocupará el primer apartado del presente trabajo. Lo que sí podemos adelantar es que el código penal no contiene, como tal, ni un delito informático[4], ni mucho menos ocupa un solo artículo a la cibercriminalidad.

El Código Penal español, a fuerza de tratado internacional, ha ido introduciendo, poco a poco, delito a delito (allá donde fuera necesario) determinadas modalidades delictivas, que incluían lo informático como medio comisivo autónomo y específico, pero en ningún caso ha denominado a alguno de ellos delito informático, ni mucho menos ha creado un título autónomo a este fenómeno criminal. Como afirma ROMEO CASABONA[5], y recuerda HERNÁNDEZ DÍAZ[6], *no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que la única nota común es su vinculación de alguna manera con los ordenadores*. Y estando de acuerdo con esta afirmación, debemos tener en cuenta que desde aquel año 1988 (fecha de publicación de esa obra) hasta la actualidad ha cambiado absoluta y sustancialmente todo. Ya no hablamos de ataques a un sistema informático local (en donde sí podía tener sentido referir lo "informático", como piedra angular de este fenómeno), hablamos de una red de redes, de un ciberespacio que es capaz de comunicar y permitir la comunicación, de lesionar y de generar biografía vital (personal y económica).

*ISSN 2255-1824

---

incluye, no sólo el estudio del lenguaje, sino además el estudio de los mensajes como medio de manejar aparatos o grupos humanos, el desarrollo de las máquinas de calcular y otros autómatas similares, algunas reflexiones sobre la psicología y el sistema nervioso y una tentativa de enunciar una nueva hipótesis del método científico. Esta teoría más amplia de los es probabilística y parte intrínseca de aquella corriente que debe su origen a Willard Gibbs y que describí en la introducción. Hasta hace muy poco tiempo no existía una voz que comprendiera ese conjunto de ideas; para poder expresarlo todo mediante una palabra, me vi obligado a inventarla. De ahí: cibernética, que derivé de la voz griega kubernetes o timonel, la misma raíz de la cual los pueblos de Occidente han formado gobierno y de sus derivados. Por otra parte, encontré más tarde que la voz había sido usada ya por Ampere, aplicada a la política, e introducida en otro sentido por un hombre de ciencia polaco; ambos casos datan de principios del siglo XIX. He escrito un libro más o menos técnico intitulado Cibernética, que apareció en 1948. Respondiendo a ciertos pedidos para que pusiera esas ideas al alcance de los profanos, publiqué en 195O la primera edición de Cibernética y sociedad. Desde entonces, el tema, que consistía en esa época en unas pocas ideas compartidas por los doctores Claude Shannon, Warren Weaver y yo, se ha convertido en un campo permanente de investigación (WIENER, N. Cibernética y Sociedad (trad. Novo Cerro). Buenos Aires. 1958. PP 15-16).

3 MATA Y MARTÍN, RM. *Criminalidad informática: una introducción al cibercrimen*. Actualidad Penal, Núm. 37, Sección Doctrina, Semana del 6 al 12 Oct. 2003, Ref. XXXVI, tomo 3, Editorial LA LEY. P. 935

4 Tampoco entendemos su necesidad en abstracto, sin perjuicio de lo que luego se indicará.

5 ROMEO CASABONA, CM. *Poder informático y seguridad jurídica*. la función tutelar del derecho penal ante las nuevas tecnologías de la información. Madrid. 1988. PP 42 y ss.

6 HERNÁNDEZ DÍAZ, L. *El delito informático*, en EGUZKILORE, núm. 23, San Sebastián, diciembre 2009. P. 233

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

Cuando se habla de cibercriminalidad se realiza en un nuevo ámbito o espacio con características estructurales intrínsecas y extrínsecas tan distintas a las del espacio físico en el que se ejecuta la delincuencia tradicional, que obliga a una revisión criminológica de la explicación del evento delictivo, así como una adaptación de las normas jurídicas para su mejor prevención. La denominación delitos informáticos o computercrimes expresaba perfectamente la preocupación por un nuevo tipo de delincuencia surgida con la aparición de los primeros sistemas informáticos, en la que éstos eran el medio o el objetivo del crimen (MIRÓ LINARES[7]).

De la importancia de esta ciberactividad da debida cuenta la ONU, en año 2015, cuando afirmó que uno de los principales elementos impulsores de la ciberdelincuencia contemporánea y del uso creciente de pruebas digitales es el desarrollo de la conectividad electrónica global. Hoy existen casi 3.000 millones de usuarios de Internet, cerca del 40% de la población mundial[8].

II. DELITOS INFORMÁTICOS VS CIBERCRIMINALIDAD

En la precisión mencionada en el apartado anterior, es donde radica la principal diferencia de la cuestión que analizamos: *sistema local informático* versus *ciberespacio* (redes sociales, aplicaciones, domótica, banking, mercado de valores, etc.). El legislador penal, sobre todo en los últimos años, trata[9] de adaptarse a los tiempos, intentando actualizar no solo conceptos que quedan anticuados (sobre todo en lo que se refiere a medios comisivos o instrumentos[10]), sino introduciendo nuevas figuras[11], o nuevos giros[12] criminógenos que aparecen en los delitos tradicionales. El riesgo de que tales giros -de no ser normativizados- conviertan a una conducta claramente antijurídica (con relevancia penal) en atípica es la preocupación constante del Derecho Penal, y la principal guía que debe seguir el legislador.

La informática es, sin lugar a dudas, uno de estos giros copernicanos que ha revolucionado no solo el Derecho Penal tradicional (incluyendo nuevos métodos o medios comisivos), sino la misma civilización en su conjunto. Sería ilusorio pensar que esta tecnología informatizada no está generando un nuevo derecho penal (su alcance lo veremos), que introduce la cibercriminalidad, como espacio criminal autónomo necesitado de un tratamiento

7 MIRÓ LINARES, F. *La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen*. Revista Electrónica de Ciencia Penal y Criminología. RECPC 13-07 (2011). P. 3

8 ONU. (A/CONF.222/12) 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Seminario 3: El fortalecimiento de las respuestas de prevención del delito y justicia pena frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional, celebrado el 2 de febrero de 2015. P. 7

9 A veces a golpe de telediario, generando una mala técnica legislativa, que luego, cuando los focos del telediario se apagan, provoca no pocos problemas de interpretación y aplicación de la norma penal.

10 Las tecnologías de la información y comunicación son, sin duda, el mejor ejemplo de esta actualización del código penal, en materia de medios comisivos.

11 Por ejemplo, el delito de child grooming, previsto en el art. 183 ter CP e introducido por la LO 5/2010, de 22 de junio, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal (B.O.E. 23 junio).

12 Por ejemplo, la estafa informática (art. 248.2 CP)

*ISSN 2255-1824

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

jurídico diferenciado[13]. Pese a todo, esa actualización, en materia informática, no ha sido uniforme, ni constante, ni tampoco se encuentra completada en nuestro Código penal.

Y aunque no deba minusvalorarse[14] el esfuerzo del legislador penal español, en la búsqueda de esta continua actualización, lo cierto y verdad es que nunca, o casi nunca, innova, sino que termina -como por otra parte es lógico- traduciendo normas supranacionales que o bien le conminan a trasladar al derecho interno o bien le "recomiendan" -en términos políticos- a hacerlo. Ni una ni otra opción impiden valorar a nuestro legislador como mero ejecutor de normas supranacionales[15], lo que resta, cada vez más, autonomía e innovación al legislador nacional, que termina siendo un delegado normativo de organismos y entidades que sobrepasan las fronteras estatales. Esta falta de autonomía deviene de formar parte de ese mundo global que vivimos: ningún Estado quiere quedarse aislado del mundo con políticas nacionales que, por ejemplo, limiten, o pongan en riesgo el comercio electrónico internacional.

Para tratar esta temática tan particular, y partir del origen normativo que hizo posible la evolución del código penal español, hemos de reseñar, someramente, las siguientes normas internacionales que resultan de interés:

1. Como primera norma supranacional, dentro de la ámbito territorial europeo, debemos partir de la ya clásica Directiva 95/46/CE, de 24 de octubre de 1995; norma que, actualmente, se encuentra derogada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Esta norma inició la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Se trata de una norma que, dentro del ámbito que estudiamos, es secundaria e indirecta, ya que su objeto no es, como resulta evidente (dado el año de su aprobación), la realidad cibernética y, sobre todo, el contexto de protección de datos que circulan en la red, tal y como lo conocemos hoy en día.

Sin embargo, en esta Directiva 46/96 *se procuró tutelar los datos personales almacenados en bases de datos de numerosos organismos públicos y privados, cuya nueva trascendencia permite su aplicación para un sinnúmero de fines diversos, que van desde la seguridad pública y la defensa del Estado (v.gr. registros de naturaleza penal) hasta la ponderación de riesgos en la concesión de préstamos o servicios* (EDUARDO ABOSO[16]).

2. El llamado Convenio de Budapest (Convenio sobre la ciberdelincuencia) de 23 de noviembre de 2001, cuyo objetivo, tal y como expone su preámbulo, es satisfacer la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional. Y todo ello dado los

13 Desde perspectivas criminológicas es evidente la importancia y la trascendencia de este fenómeno delincuencial específico o alternativo al tradicional.

14 Sin que tampoco podamos tildar de vanguardista

15 Terminando el código penal por embarrarse con nuevas figuras que, por muy necesarias que sean, destruyen el esquema original y de principios establecidos en el código penal del 95. Hasta el punto de que, tras tantas reformas, y tanto parcheo legislativo, empieza a ser necesario una reconfiguración y/o refundición del código penal para buscar el denominador común de tanta política criminal puntual, dispersa y oportunista que, lamentablemente, ha encontrado acomodo, en las sucesivas legislaturas, en el código penal.

16 EDUARDO ABOSO, G. *Derecho Penal Cibernético. La cibercriminalidad y el Derecho Penal en la moderna sociedad de la información y la tecnología de la comunicación*. Buenos Aires. 2017. P. 59

*ISSN 2255-1824

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de redes informáticas.

Es de destacar la capacidad de antelación que tuvo este convenio, que ya en el año 2001, cuando las redes aún se encontraban en un momento muy incipiente (respecto, al menos, de consumidores particulares y finales), se percató del riesgo que las redes informáticas y la información electrónica fueran utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos fueran almacenadas y transmitidas por las redes (así se expresa el preámbulo del convenio). En aquel año ya se hablaba de la necesidad de que los Estados firmantes (España lo ratificó, no obstante, en el año 2010[17]) incorporaran en la regulación sustantiva penal determinados delitos que, poco a poco, y en años posteriores, fueron quedando integrados en el código penal español, a partir de sus diversas reformas. Estas figuras eran los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (artículos 3 a 6 del convenio); delitos informáticos, propiamente dichos (artículos 7 a 8); delitos relacionados con el contenido (en materia de pornografía infantil, art. 9); delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (art. 10), así como otras disposiciones en materia de Derecho Penal general.

3. La Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información. La etiología de la norma la plasma su misma exposición de motivos, al indicar que *se ha comprobado la existencia de ataques contra los sistemas de información, en particular como consecuencia de la amenaza de la delincuencia organizada, y crece la inquietud ante la posibilidad de ataques terroristas contra sistemas de información que forman parte de las infraestructuras vitales de los Estados miembros. Esto pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia, y por tanto exige una respuesta por parte de la Unión Europea*.

Es sorprendente que estos peligros se advirtieran en el 2005; mucho antes de que las redes sociales y el mundo virtual "de verdad" coparan nuestra existencia y, con ella, definieran un nuevo modelo de sociedad. La pregunta que debemos hacernos es si hoy en día, en un mundo para nada imaginado en aquel 2005, tenemos esa seguridad que guiaba el sentido teleológico de la norma. Mas aún, debemos indagar si en la actualidad se ha modernizado mucho, o poco, la normativa que permite proteger, investigar y sancionar los comportamientos delictivos derivados de la cibercriminalidad. Se deberá compartir que la cibercriminalidad actual no tiene mucho que ver con aquella delincuencia informática esperada o pensada en décadas anteriores.

Lo que dejaba claro esta norma, y hoy en día sigue siendo un objetivo principal de la cibercriminalidad (entendida como rama de conocimiento), es que, para combatir los delitos cibernéticos, cada Estado miembro debe garantizar una cooperación judicial efectiva.

El gran límite de la Decisión Marco 2005/222/JAI[18], consecuencia de la época en la que nace, es que la delincuencia informática allí referida se centraba en el ataque a

17 Véase Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 (BOE núm. 226, de 17 de septiembre de 2010). Dicho Convenio entró en vigor para España el 1 de octubre de 2010, de conformidad con lo establecido en su artículo 36.4.

18 Otras normas europeas sectoriales que deben ser citadas son 2001/413/JAI del Consejo, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo; Decisión marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la

*ISSN 2255-1824

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

cualquier sistema de información, entendido este como todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento[19]. En este sentido, se interesaba la regulación nacional para sancionar el acceso ilegal en los sistemas de información (art. 2); la intromisión ilegal en sistemas de información (art. 3), destacando los daños como resultado típico; intromisión ilegal de datos (art. 4), y poco más, sobre todo en consideraciones derecho penal general (inducción, complicidad tentativa, circunstancias agravantes o responsabilidad penal de las personas jurídicas).

Esta normativa europea hizo que el legislador español[20], a través de la LO 5/210 de reforma del código penal, decidiera incardinar las conductas punibles que se sugerían en dos apartados diferentes, al tratarse de bienes jurídicos diversos. El primero, relativo a los daños, donde quedarían incluidas las consistentes en dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos o programas informáticos ajenos, así como obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno; y, el segundo, el referido al descubrimiento y revelación de secretos, donde estaría comprendido el acceso sin autorización vulnerando las medidas de seguridad a datos o programas informáticos contenidos en un sistema o en parte del mismo.

*ISSN 2255-1824

Lo sorprendente es que el legislador español, en ese intento fallido de estar a la "vanguardia", transpone la decisión marco en el mismo año que Europa había propuesto una Directiva[21] para derogar, precisamente, esa Decisión Marco. No es de extrañar, puesto que la decisión marco era de 2005 y la reforma del código penal tuvo lugar cinco años después. Afortunadamente para el legislador español, esta Directiva no fue aprobada hasta el año 2013, mediante 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.

Sin embargo, ya desde el año 2010 se estaba trabajando en la derogación de la Decisión marco 2005/222/JAI y, por tanto, sobre la mesa del legislador europeo existían nuevos criterios y nuevas fórmulas para tratar, jurídicamente, la delincuencia informática. No será hasta la reforma del código penal del 2015 cuando el legislador español traspusiera la Directiva 2013/40/UE[22]. La misión de esta reforma fue la de pretender superar las limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la normativa europea (preámbulo, punto XIII LO 1/2015).

Como se afirmaba en la primera propuesta de directiva (2010), en un informe de la Comisión, de fecha 14 de julio de 2008, *desde la adopción de la Decisión marco, los re-*

pornografía infantil y Decisión Marco 2008/913/JAI del Consejo, de 28 de noviembre de 2008, relativa a la lucha contra determinadas formas y manifestaciones de racismo y xenofobia mediante el Derecho penal.

19 Artículo 1 a) Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información

20 Véase la exposición de motivos, apartado XIV, de la LO 5/2010 de Reforma del Código Penal.

21 Propuesta de Directiva del Parlamento Europeo y del Consejo (Bruselas, 30.9.2010) relativa a los ataques contra los sistemas de información, por la que se deroga la Decisión marco 2005/222/JAI del Consejo

22 Puede leerse en la LO 1/2015, de Reforma del Código Penal, y concretamente en su Preámbulo, punto XIII: La reforma lleva a cabo la transposición de la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal.

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

cientes ataques sufridos en toda Europa han puesto de manifiesto las diversas amenazas que están apareciendo y, en particular, los ataques simultáneos y masivos contra los sistemas de información y la creciente utilización delictiva de los denominados botnets[23]». Ataque estos tan nuevos, que, como seguía indicando el informe contenido en la propuesta de Directiva, *no estaban en el centro de atención de la Decisión Marco de 2005*.

A pesar de todos estos avances normativos supranacionales, hoy en día no resulta pacífico establecer un concepto de delito informático. *Las definiciones que a lo largo de los últimos cuarenta años se han aportado del concepto de delito informático van necesariamente unidas a la evolución que ha sufrido la implantación de las TICs en la sociedad y a las propias conductas delictivas, o merecedoras de serlo, vinculadas con las nuevas tecnologías de la información y de la comunicación* (HERNÁNDEZ DÍAZ[24]).

En el código penal español no queda definido, con claridad y nitidez, qué deba ser considerado un delito informático. Dicha categoría delictiva no existe, ni consta así denominada en ninguna parte de la norma. Lo que sí existe, por el contrario, son modalidades delictivas en las que se incluye el fenómeno informático o tecnológico[25] (desde las tradicionales estafas y daños, hasta las más actuales sexting, child grooming, stalking, hacking, etc.).

Por tanto, en el código penal español no se define una categoría estricta de cibercriminalidad, ni de delito informático en general, optando el legislador por ubicar los distintos fenómenos delictivos de naturaleza informática, dentro de la sistemática propia del código penal, en función del bien jurídico afectado y, por tanto, ubicándolo en el título correspondiente del libro II. De ahí que pueda criticarse la desacertada regulación del código penal en torno a la ciberdelincuencia, ya que pone solo el acento en figuras típicas tradicionales, a las que se añade el medio informático en su ejecución, y no regulando, de manera autónoma, la realidad distinta que poseen, ni previendo la existencia de un posible bien jurídico independiente a los tradicionales. Se trataría, en definitiva, de regular la naturaleza tecnológica como algo que irroga un carácter especial, autónomo e independiente al delito informático (como insoslayable fenómeno social de nuevo cuño).

La actual regulación de la realidad informática, adaptada a los cánones tradicionales, defiende la tesis contraria. En efecto, el legislador entiende, o parece entender, que lo informático es tan solo un medio comisivo, que nada cambia el fenómeno delictivo concreto. Es decir, una estafa podrá ser cometida por muchos medios, entre ellos el medio

23 Señala el informe de la European Union Agency for Cybersecurity (ENISA), de 2019, que *una botnet es una red de equipos conectados infectados por programas de malware. Estos equipos los suelen usar atacantes para lanzar ataques distribuidos de denegación de servicio (DDoS). Las botnets operan en modo peer-to-peer (P2P) o desde un centro de mando y control (C2), y las controla de forma remota un agente malintencionado que opera de forma sincronizada para obtener un resultado determinado. Los avances tecnológicos en la informática distribuida y automatización han creado una oportunidad para que los atacantes exploren nuevas técnicas y mejoren sus herramientas y métodos de ataque. Gracias a ello, estas botnets operan de formas mucho más distribuidas y automatizadas, y se pueden conseguir a través de distribuidores de autoservicio y listas para usar. Estas botnets, a las que en inglés también llaman «bad bots» no solo evolucionan constantemente sino que tanto el conocimiento de las personas como el nivel de desarrollo de las «bots» se están especializado mucho en determinadas aplicaciones, como las de los proveedores de defensa o incluso técnicas de evasión. Desde una perspectiva distinta, las botnets proporcionan un vector que permite a los ciberdelincuentes lanzar varias operaciones, desde estafas de banca electrónica a programas de ransomware, minería de criptomonedas y ataques DDoS* (informe recuperado de etl2020-botnet-ebook-en-es.pdf (europa.eu)

24 HERNÁNDEZ DÍAZ, L. *El delito informático*… Op. Cit. P. 230.

25 Modalidades que, a lo largo de los tiempos, han permitido la distinción entre el delito informático, como categoría amplia, y el ciberdelito.

*ISSN 2255-1824

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

*ISSN 2255-1824

informático o tecnológico, pero eso nada distinto añade o quita, penalmente, a la estafa[26]. En este entendimiento, el autor se ha movido en los últimos años, si bien, y a partir de algunas concretas conductas, presentes en la red, ve necesario el cambio de parecer, al menos, en lo que se refiere a algunas modalidades concretas[27].

Es obvio que el sucesivo incremento de los inventos tecnológicos, y el casi preocupante (ab)uso de las nuevas tecnologías (hasta para las cosas más básicas), ha convertido lo cibernético en un nuevo mundo, con reglas nuevas y riesgos y/o peligros desconocidos. Solo ha de pensarse en la datos personales que cada individuo *entrega* a la red, y en la posibilidad de uso, por terceros anónimos, de tales datos, incluso sin el conocimiento directo ni indirecto de la víctima. Es evidente que este nuevo mundo (esa *nueva modernidad* a la que se refería BECK)[28] arroja un cúmulo de nuevos riesgos, que merecen, al menos teóricamente -no necesariamente en términos legislativos- un estudio y tratamiento especializado, que tenga en cuenta todas las variables que confluyen en este, cada vez más expandido, fenómeno social de redes (o, dicho de otro modo, en esta nueva sociedad cibernética, que se impone sobre la ya denominada sociedad tradicional o antigua).

Y es en ese nuevo mundo del ciberespacio donde se sitúa la diferencia entre el delito informático y el cibercrimen. Como ha señalado MIRÓ LINARES[29], *en la raíz de este cambio de denominación está la evolución, desde una perspectiva criminológica, de los comportamientos ilícitos en la Red y la preocupación legal en relación con ellos, concretamente, el hecho de que pasara de ser el centro del riesgo la información del sistema informático, a serlo las redes telemáticas a las que los sistemas empezaron a estar conectados y los intereses personales y sociales que se ponen en juego en las mismas*.

Siguiendo a LÓPEZ MUÑOZ[30], *diferenciamos, por tanto, "delincuencia informática" y delincuencia cibernética". La informática será la que se lleve a cabo sobre sistemas informáticos, aquí las redes son inexistentes o tienen poca relevancia respecto a la conducta delictiva que las afecta; sin embargo, la cibernética atacará a las redes electrónicas o telemáticas, siendo los sistemas informáticos menos relevantes*.

III. CIBERCRIMINALIDAD

La cuestión de si hoy debemos englobar bajo la etiqueta de cibercriminalidad todos los delitos informáticos, más otros fenómenos criminales específicos o si, por el contrario, debemos dejar, bajo aquella etiqueta, solo los delitos de redes, es algo que todavía no es pacífico en la doctrina penal. Ni siquiera existe consenso en si hay una diferencia neta y nítida entre el delito informático y el ciberdelito.

Se ha señalado que *existe, de manera consolidada,* una *distinción del objeto de agresión del medio utilizado para la comisión de estos delitos informáticos. Cuando el*

26 De ahí que, a lo sumo, se añada un tipo especifico incluyendo el medio comisivo informático.

27 Como luego se dirá, para el común -y resto- de las modalidades delictivas informáticas, seguimos pensando que todo queda limitado a un mero medio comisivo específico de la conducta general tradicional, pero es cierto que hay otras conductas (por ejemplo, el secuestro de datos o ransomware) que precisarían un tipo autónomo e independiente para evitar la insegura interpretación extensiva de los delitos tradicionales.

28 BECK, U. *Sociedad de riesgo. Hacía una nueva modernidad*.

29 MIRÓ LINARES, F. La criminalidad en el ciberespacio: la cibercriminalidad. Madrid. 2012. P. 37

30 LÓPEZ-MUÑOZ, J. *Cibercriminalidad e investigación tecnológicas*. Madrid. 2020 PP. 23-24

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

objeto de agresión son la integridad y el funcionamiento del sistema automatizado de procesamiento de datos, se habla de delitos cibernéticos propios o en sentido estricto, mientras que cuando el uso de la computadora representa un mero instrumento para llevar adelante acciones disvaliosas contra bienes jurídicos individuales o colectivos, se habla de manera más apropiada de delitos cibernéticos impropios o en sentido amplio (EDUARDO ABOSO[31]).

Con todo, la ciberdelincuencia no es necesariamente un término jurídico técnico, sino un término genérico para referirse a un conjunto de hechos cometidos en contra o a través del uso de datos o sistemas informáticos. Otros enfoques se centran en los delitos contra la información computadorizada o el uso de recursos de información con fines ilícitos (A/CONF.222/12[32]).

Mas allá de la etiqueta que, en un futuro, decida utilizar el legislador penal español, lo cierto es que en la actualidad esta forma de criminalidad (se llame cibercriminalidad, ciberdelincuencia o delincuencia informática) no constituye una categoría normativa y su uso, por tanto, no permite un concepto unívoco. Esto hace que el término sea más usado en criminología (o por profesionales de la informática y seguridad tecnológica) que, en sentido estricto, por juristas.

Ello no obsta a que, gradualmente, la cibercriminalidad comienza a integrar una serie de conceptos y supuestos bien definidos que, con el tiempo, terminarán por constituir una categoría delictiva, más o menos nítida, como hoy lo puede ser el delito informático (y ello, a pesar de que esta última denominación tampoco haya sido aceptada jamás por el código penal español). Como se ha señalado, el término ciberdelincuencia permite ya un *concepto académico* (A/CONF.222/12[33]). Es el caso de WALL[34] .

En 1994, en el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos se señaló que el potencial de la delincuencia informática es tan amplio como el de los propios sistemas internacionales de telecomunicaciones. Como era de esperar, la palabra "Internet" aparecía solo una vez en el Manual y la palabra "ciberdelincuencia" no se utilizó; sin embargo, las conclusiones demostraron una gran visión de futuro. Si bien el Manual centró su atención en el concepto de "delito informático", es bien sabido que hoy en día la "ciberdelincuencia" recurre efectivamente a las tecnologías globalizadas de la información y las comunicaciones, en particular a Internet, para la comisión de actos delictivos de alcance transnacional (A/CONF.222/12[35]).

Partiendo de esto, se acepta que la cibercriminalidad es el conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas[36].

31 EDUARDO ABOSO, G. *Derecho Penal Cibernético*... Op. Cit. P. 17

32 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Seminario 3: El fortalecimiento de las respuestas de prevención del delito y justicia pena frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional, celebrado el 2 de febrero de 2015)

33 Ibídem. P. 6

34 Wall, D. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge. 2007

35 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal… Op. Cit. P. 6

36 Siguiendo la Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional, Capítulo 2.

*ISSN 2255-1824

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

IV. TRATAMIENTO JURÍDICO PENAL DE LA CIBERCRIMINALIDAD

No guardaría coherencia, por mucho que sigamos discrepando[37], que el legislador penal decidiera incluir a la persona jurídica como sujeto penalmente responsable, y ahora no aceptara que existen sujetos virtuales, cuyo autor real (la máquina no puede ser perseguida), se encuentra detrás, moviendo -o similar- a ese sujeto virtual tras la red. Un sujeto que, en la mayoría de las ocasiones, no actúa sino a través de una programación informática predefinida, activada con intención criminal, pero sin objetivo personalizado. Es decir, sin victima determinada ni determinable, sino algorítmica con multitud de variables que la propia víctima puede modificar, sin saberlo, el día que se convierte -o no- en diana del sistema binario.

Esta nueva forma de actuar, no física, altera no solo el concepto tradicional y clásico de autoría del artículo 28 CP (y que, al tiempo, cuando la investigación jurídica cibernética avance, veremos si termina inspirando a nuestro legislador para introducir la autoría cibernética[38]), sino también la regla general de forma de culpabilidad (el dolo eventual pasaría a ser la categoría general, por encima del dolo directo), del fenómeno criminal, y de víctima (que pasa a ser víctima algorítmica variable). Es más, la propia víctima ha podido ser la que ejecute el propio delito activándolo mediante los datos que ella misma ofrece a la red (incluso mediante su voz a un smartphone), generando una autentica víctima provocadora y/o propiciatoria, sin que ello afecte, en nada, a la responsabilidad penal de quien obtiene el beneficio o genera el resultado final lesivo.

Más aún, los permisos concedidos a los micrófonos de los apartados inteligentes -a través de las famosas aplicaciones- pueden hacer que sea un tercero el que, sin saberlo, solo por hablar cerca de la víctima, sea grabado diciendo alguna palabra (que el algoritmo detecta como palabra clave), y termine activando la diana de la víctima. En este caso, además, ni tan siquiera la víctima habría propiciado o provocado el delito, lo que convierte a la ciberdelincuencia en un auténtico laberinto negro. Pero desde la perspectiva del autor tampoco el problema es simple. La inteligencia artificial convierte la conducta final lesiva en una mera probabilidad (desde la óptica del autor), de ahí que indicáramos que el dolo eventual terminará convirtiéndose en la forma de culpabilidad general en los ciberdelitos. El autor arranca un algoritmo que crece, aprende y se expande por la red, en función de parámetros comunicativos artificiales (sistema y lenguaje binario) que escaparán, en la mayoría de las veces, a la imaginación (que no intención) del autor.

Como recuerda el informe del 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal[39], algunos instrumentos de ciberdelincuencia como las redes robot o zombi ("botnets" -término derivado de las palabras "robot" y "network"), pueden constituir redes globales de decenas o centenares de miles de dispositivos infectados con programas informáticos maliciosos controlados a distancia por delincuentes. Las

37 Buena prueba de nuestra discrepancia queda plasmada, entre otras, en PÉREZ ARIAS, J. *Sistema de atribución de la responsabilidad penal de las personas jurídicas*. Madrid. 2014

38 Parece claro que el código penal sí debe modificar su planteamiento sobre el fenómeno cibernético, aunque la autoría no sea uno de estos planteamientos.

39 ONU. (A/CONF.222/12) 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Seminario 3: El fortalecimiento de las respuestas de prevención del delito y justicia pena frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional, celebrado el 2 de febrero de 2015. PP. 7-8

*ISSN 2255-1824

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

páginas web de los medios sociales pueden utilizarse para cometer actos de hostigamiento, incitación al odio, amenazas de violencia, extorsión, o para la difusión de información privada a escala global en cuestión de segundos. Como los delincuentes intentan también extender sus actividades a la "Internet de los objetos", también existe la posibilidad de que las actividades delictivas a escala mundial aumenten aún más.

La enorme cotidianeidad de lo digital es la verdadera causa de exposición. Como señala MIRÓ LINARES[40] *la hipótesis de que el mayor uso de los servicios de internet, debido al mayor tiempo en casa, derivará en un incremento de la cibercriminalidad se fundamenta en la relación entre cotidianeidad, oportunidad y delincuencia: si es en internet donde pasan tiempo será allí donde surjan las oportunidades que interaccionarán con sus motivaciones delictivas; y lo mismo se podría decir para las víctimas, que será en el ciberespacio donde les ataquen*.

De ahí que los profesionales de la seguridad cibernética estén centrados no solo en herramientas pasivas de defensa, sino en activas y preventivas. Y no solo los profesionales de las nuevas tecnologías, también aquellos que estudian el fenómeno desde una perspectiva jurídica y/o social. Como se ha señalado, *de forma vertiginosa han surgido nuevos intereses sociales en peligro y nuevas formas de comisión de delitos tradicionales, frente a lo cual en muy poco tiempo han tenido que reinterpretarse las normas sustantivas y procesales, así como crearse otras nuevas* (PÉREZ GIL[41]).

Lo que no parece posible, de momento, es partir de que el fenómeno cibernético escapa del todo al fenómeno humano (autor de la conducta), de ahí que, hoy por hoy, no resulte necesario poner la vista y la atención en la categoría dogmática del autor[42], sino en la ubicación de la barrera de protección que debe plantear el legislador con la tipificación de la conducta cibercriminal. Si en el resultado es difícil determinar al autor (por esa inteligencia artificial algorítmica que crece al margen de su decisión), quizás lo único posible sea criminalizar el riesgo y el peligro abstracto que determinadas conductas cibernéticas pueden provocar en un hipotético y futuro resultado.

Cuando el ataque -la conducta criminal- afecta a bienes jurídicos tradicionales (patrimonio, honor, intimidad, etc.) ningún problema existe para pedir que el código penal, tal y como ya hace, trate ese delito como mera modalidad (en su caso) de la que le es propia en términos tradicionales. Por ejemplo, una injuria cometida a través de las redes sociales, lo único que modificaría es el medio y el alcance de la publicidad, pero el ataque estricto al bien jurídico es exactamente el mismo que si se cometiera a través de un medio de comunicación o por carta.

40 MIRÓ LINARES, F. *Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos*, en Revista de Internet, Derecho y Política. UOC. IDP Núm. 32, ISSN 1699-8154. Marzo, 2021. P. 5

41 PÉREZ GIL, J. Recensión del libro de Fernando Miró Llinares, el cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Revista Electrónica de Ciencia Penal y Criminología REFLEXIONES (Recensión). RECPC 15. 2013. P. 1

42 En el mismo sentido, MIRÓ LINARES indica que todo el contexto es otorgado por los seres humanos quienes, con la información que le brindan (por acción y por omisión) y los algoritmos que crean para relacionar las variables, determinan completamente el actuar de la máquina, no requiere, a mi parecer, de ningún tipo de cambio en el sistema de atribución de responsabilidad pensado para los seres humanos como sí podría requerir en el futuro algún sistema de IA que tuviera rasgos de autonomía (MIRÓ LINARES, F. *Inteligencia artificial y justicia penal: Más allá de los resultados lesivos causados por robots*, en UNED. Revista de Derecho Penal y Criminología, 3ª Época, núm. 20. 2018. P. 95

*ISSN 2255-1824

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

Ahora bien, en ciertos casos, el medio comisivo añade un plus de antijuridicidad, ya que el atacante pretende alcanzar, con el uso de determinadas redes sociales (nacidas para crear información viral), una resonancia en la difamación, que impide, per se, que la víctima (incluso con instrumentos judiciales), pueda eliminar esa información que afecta a su honor (mediante el llamado derecho al olvido, por ejemplo). Ese público indeterminado se convierte en el verdadero instrumento de resonancia. Y ese efecto eco no solo puede ser considerado un medio comisivo, se convierte claramente en el fundamento de lo que no es sino un elemento subjetivo del tipo (es el propósito más específico del autor, que va indisolublemente ligado al arranque de la conducta y al ánimo de difamar). Por tanto, el medio comisivo generaría, en el ejemplo citado, un añadido de trascendencia porque, cuando concurre, agrava el injusto de la conduta típica. Verdaderamente esa intencionalidad subjetiva se convierte en elemento subjetivo, entendido este, con carácter general, como *un componente de naturaleza subjetiva, que va referido a fines y propósitos específicos del sujeto* (MORILLAS CUEVA[43]). En estos casos, como luego se ahondará, el medio comisivo informático es algo más que un mero medio comisivo, y sí merece una respuesta autónoma y específica del Código Penal.

Respecto a los sujetos, y como se decía más arriba, es evidente que la ciencia penal debe abordar y ahondar en su estudio. Estamos ante un nuevo modelo de sujeto que actúa controlando una máquina, con inteligencia artificial, que aprende hábitos y genera respuestas artificiales ante determinada situación. Inteligencia que, por artificial, no puede ser tenida en cuenta más que como medio comisivo directo, pero que, en todo caso, ha de tenerse en cuenta, ya que su artificialidad es, en numerosas ocasiones, difícilmente perfectible para la inteligencia humana. La situación actual nos recomienda, ante todo, generar seguridad preventiva, ya que el enjuiciamiento de estas conductas difusas y, en muchos casos, desterritorializadas[44], no resulta nada fácil en la práctica.

A ello le debemos unir la dificultad que conlleva cualquier investigación científica o policial de tales conductas. Dificultad que genera un grave problema, al tratarse de una tecnología que está centrada en *el anonimato, el bajo costo, la vulnerabilidad de los sistemas y redes telemáticas, la naturaleza de los delitos a distancia y los conflictos interjurisdiccionales que se plantean tanto en su prevención como represión* (EDUARDO ABOSO[45])

Cuando el código penal español regula o intenta tratar la ciberdelincuencia (o lo relacionado con ella) lo hace recurriendo a términos típicos[46] como *sistema informático* o *tecnología de la información y la comunicación*. Son muchos los delitos que, en el código penal, regulan este fenómeno. Así, sin ánimo exhaustivo, lo encontramos en el delito de fomento del suicidio (art. 143 bis); Delito de fomento autolítico (art. 156 ter); delitos contra la Indemnidad sexual: Child Grooming (art. 183 ter. 1 CP) y Pornografía infantil (arts. 183 ter. 2, 189.5 ,189 bis CP); Delitos contra la intimidad (arts. 197 y ss.): acceso no autorizado a sistemas, registros o archivos informáticos, apoderamiento de secretos, pro-

43 MORILLAS CUEVA, L. *Sistema de Derecho Penal*. Parte general. Madrid. 2018. P. 454

44 En muchos de estos casos, además, se consigue la desterritorialización a través de herramientas informáticas como los proxy, VPN, red Tor, etc.

45 EDUARDO ABOSO, G. Derecho Penal Cibernético... Op. Cit. P. 534

46 En la mayoría de las ocasiones previstos como medios comisivos típicos, sin añadir ninguna relevancia adicional al delito.

*ISSN 2255-1824

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

gramas ilegales para acceder a sistemas de manera no autorizada, etc.; Delito de estafa: Estafa informática (estafa impropia, art. 248.2 a y b); Delitos de daños: Daños informáticos (Arts. 264, 264 bis. 264 ter CP); Delitos de secreto industrial (art. 278 CP); Delito de alteración de cotización de valores o materias primas (Art. 284 CP); Delito de prestación de servicios de acceso condicional (art. 286 CP); Delitos contra la salud pública (Art. 361 bis); Delito de falsificación de tarjetas (crédito y débito) y cheques de viaje (Art. 400 CP); Delitos contra los derechos fundamentales (Art. 510 CP); Delito de organización y grupo criminal (Art. 570 bis. 2 CP); Delito de terrorismo (Art. 573.2 CP).

Es evidente que el legislador penal, de lege ferenda, tiene varias opciones para hacer un tratamiento de la cibercriminalidad: la primera de ellas, como hace ahora, es ir formulando tipos concretos en los que, de manera autónoma y taxativa, regule el fenómeno cibernético que merezca protección penal. Esta posibilidad, quizás la que mayor dota de seguridad jurídica, genera, sin embargo, una evidente redundancia en el código penal. En efecto, en la mayoría de los casos, lo informático no será más que un medio comisivo, por lo que reiterar un tipo para añadir solo un medio comisivo haría casi interminable la redacción de tipos específicos en la norma. Esta posibilidad trataría el medio informático como medio comisivo más, por lo que la necesidad de su tipificación también podría ser discutible. Piénsese, por ejemplo, que en el delito de homicidio se generaran tantos tipos específicos de agravación como longitudes de arma blancas existieran en el mercado (como medio comisivo). Sería redundante y poco trascendente.

La segunda opción sería crear un título autónomo en el que el legislador tratara de manera conjunta el fenómeno de la cibercriminalidad, con la posibilidad incluso de establecer disposiciones comunes. Evidentemente en este caso habría que trasladar los tipos actuales que regulan lo informático (que se convertirían así en delitos pluriofensivos) con el consiguiente problema de sistematización. Esta posibilidad procede si se considerara que la seguridad en el ciberespacio tiene entidad autónoma y suficiente, como para erigirse en bien jurídico protegido independiente.

La tercera de las posibilidades sería establecer una circunstancia modificativa de la responsabilidad (agravante) con el fenómeno cibernético, de tal forma que el libro II no deba, salvo excepciones, regular de manera autónoma y específica cada una de las modalidades delictivas en las que cabe imaginar la cibercriminalidad. Esta última de las posibilidades es, posiblemente, la que mejor pueda funcionar en un código ya de por sí sobrecargado de delitos. Sin embargo, también es cierto que hay modalidades que, por su gravedad, no obtendrían una pena proporcional (al injusto realizado) solo con la aplicación de una circunstancia agravante. Por ello y, en función de los casos, es evidente que se hace necesaria la tipificación específica de algunos delitos. El ejemplo más evidente de esta necesaria tipificación autónoma delictiva es el conocido como ransomware[47] (o secuestro de datos); se trata de un figura que no tiene una respuesta nítida en el código penal, aunque el cúmulo de conductas que integran este especifico secuestro se encuentra tipificado a través de delitos independientes (apoderamiento de datos, secuestro, rescate, finalidad económica, etc.). Al final, pues, se deja en manos de la interpretación judicial; una interpretación que, en muchos casos, pudiera ser tildada incluso de extensiva.

47 Para que se vea la importancia del problema, en el año 2021, El ransomware crece un 93% en un año (https://emad.defensa.gob.es/Galerias/unidades/mccd/files/newsletter_09-2021.pdf)

*ISSN 2255-1824

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

Dentro del tratamiento jurídico de la cibercriminalidad resultan de especial interés práctico las Circulares[48] de la Fiscalía General del Estado número 1/2019, 2/2019, 3/2019, 4/2019 y 5/2019, aunque su estudio pormenorizado escapa a la extensión y objetivo del presente trabajo.

V. CONDUCTAS ALGORÍTMICAS: PELIGRO ABSTRACTO

Cuando estos factores (riesgo y dificultad para atribuir el resultado) confluyen, el Derecho Penal debe intentar anticipar la barrera de protección allá donde sea posible para facilitar la prevención de la lesión del bien jurídico. Así ocurrió no solo con el tráfico de drogas, sino también, entre otros, con la protección del medio ambiente. Son, todos ellos, fenómenos que provienen de conductas arriesgadas, peligrosas, inciertas, pero socialmente -si se encuentran bien controladas- necesarias para el progreso.

Sin embargo, esta incertidumbre no es nueva, ni será la última. *Todo ingenio humano de amplia repercusión ha generado incertidumbre y ha colocado a los ciudadanos y al poder público ante esa inseguridad y la decisión sobre el control de estos medios* (MATA Y MARTÍN[49]).

Como hemos indicado más arriba, el problema fundamental de estas conductas radica en la difícil conexión entre el resultado lesivo y la conducta concreta del autor. Esta dificultad encuentra su causa en dos factores principalmente: En primer lugar, y desde perspectivas procesales, en la desterritorialización y anonimato[50] de las conductas, características esenciales en la ciberdelincuencia; pero, en segundo lugar, y desde perspectivas penales, en la difícil conexión causal entre la conducta del autor y el algoritmo en el que finalmente se desencadena la conducta ideada. La trascendencia de la ciberdelincuencia radica en esto, precisamente: No es un sujeto que dirige desde un sistema informático a otro un malware. El problema se complica cuando lo que entra en la red es una aplicación (algoritmo), cuya programación lo hace crecer para buscar víctimas propiciatorias utilizando métodos de engaño, aprendidos a partir de la información que facilita la propia víctima en su navegación por internet. Todo ello, no entra en la imaginación directa del autor, aunque sí en su juicio de probabilidad. El resultado, de obtenerse, será devuelto, es-

*ISSN 2255-1824

48 Concretamente: CC FGE 1/2019 sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológicas en la Ley de Enjuiciamiento Criminal.; 2/2019 obre interceptación de comunicaciones telefónicas y telemáticas; 3/2019 sobre captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; 4/2019 sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización; y 5/2019 obre registro de dispositivos y equipos informáticos.

49 MATA Y MARTÍN, RM. Criminalidad informática… O. Cit. P. 936

50 Aunque, como se señala por la ONU, En los primeros tiempos se daba por sentado que Internet era en gran medida un medio anónimo, por lo menos a juicio de sus usuarios, que no comprendían que era posible técnicamente rastrear la actividad en línea de una persona. Sin embargo, en los últimos años los sistemas de justicia penal se han venido familiarizando más con los conceptos de direcciones IP y registros de conexión, así como con el uso de órdenes judiciales para obtener datos de proveedores de servicios electrónicos. Como resultado de ello, las huellas electrónicas que dejan los usuarios de Internet resultan cada vez más accesibles para los investigadores, aunque la obtención de datos de Internet puede requerir mucho tiempo y esfuerzo. Asimismo, los avances con respecto a los instrumentos forenses digitales, como la creación de dispositivos forenses de instalación automática ("plug and play") y sencillos de utilizar, han facilitado el análisis rutinario de los datos almacenados en dispositivos digitales como computadoras y teléfonos inteligentes (ONU. (A/CONF.222/12) 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal… Op. Cit. P. 8)

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

tilo boomerang, al destino seleccionado por el autor, que es cuando tomará conocimiento de la efectividad o no de su conducta, y de su alcance y contenido concreto.

Por tanto, hay mucho de probabilidad e intención, y muy poco -a veces nada- de conexión directa (objetiva y subjetiva) con un resultado concreto (en términos naturalísticos). Mas aún, en la mayoría de los casos, la conducta final lesiva y el resultado ni siquiera será conocido, ni esperado, ni imaginado, con carácter previo por el autor. La peligrosidad del ciberdelincuente estriba en que este lanza un producto (que busca solo y crece solo), y solo tiene que esperar el resultado (si lo hay). Es, en realidad, una caza con red.

Se trataría de tipificar una conducta de peligro hipotético o potencial, donde el objeto de investigación e imputación fuera la idoneidad de la conducta cibernética para originar un riesgo grave en el bien jurídico protegido. Se trata de un *delito de actividad cuyo merecimiento de pena descansa sobre la peligrosidad general de la acción típica para determinados bienes jurídicos* (JESCHECK/WEIGEND[51]).

De ahí, que resulte interesante normativizar la seguridad en la red como valor digno de protección en el ámbito penal. En definitiva, lo importante es definir qué conducta es la que puede criminalizarse y cómo articular su redacción taxativa, sin perjuicio de su abstracción conceptual. Por ello, solo el delito que configure una conducta en base al peligro abstracto podría generar un resultado preventivo y evitar la impunidad: De un lado, porque si tal peligro se configura -de ser posible- como abstracto, haría innecesaria la vinculación causal -concreta- del resultado con la conducta (lo que a todas luces facilitaría la investigación criminal en estos delitos) y, de otro lado, porque tal previsión delictiva permitiría luchar contra la ciberdelincuencia anticipándose a un resultado que, por ser masivamente lesivo, sería, en la mayoría de las ocasiones, inmune al derecho penal (al menos a ese derecho penal que, actualmente, y dentro de esa ciberdelincuencia, se ha convertido en un riesgo asumible para el delincuente, dada la monetización que le genera).

Quizás se deba ampliar la perspectiva del código penal y sistematizar la ciberdelincuencia en base a esos factores comunes que concurren, incluyendo esa protección a la seguridad de la vida en la red, que debería añadirse como nuevo bien jurídico, distinto del tradicional (y ello por mucho que también este pueda quedar afectado por la concreta modalidad delictiva).

VI. ASPECTOS CRIMINOLÓGICOS

Tampoco la criminología está exenta de cierto desorden teórico respecto de la cibercriminalidad. Existe cierto consenso en que la cibercriminalidad ha generado un nuevo paradigma de la criminología, y que no estamos ante un fenómeno criminal que pueda ser abordado solo con los parámetros científicos tradicionales, y mucho menos individuales (sino a nivel multidisciplinar[52]). Muy al contrario, nos encontramos ante una criminolo-

51 JESCHECK/WEIGEND. *Tratado de Derecho Penal. Parte General* (trad. OLMEDO CARDENETE). Granada. 2002. P. 283

52 Como se afirma en el estudio sobre la cibercriminalidad en España, del año 2019, la ciberdelincuencia como fenómeno complejo y global requiere un enfoque multidisciplinar para abordar cualquier planteamiento de respuesta contra la misma (Gabinete de Coordinación y estudios. Secretaría de Estado de Seguridad del Ministerio del Interior del Gobierno de España. *Estudio sobre la cibercriminalidad en España*. 2019. P. 2)

*ISSN 2255-1824

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

gía específica o alternativa que, como ha señalado CÁMARA ARROYO[53], *debe tratar el estudio de una determinada sección de la realidad y su relación con la criminalidad, las tipologías delictivas, etc. Se trata de especializaciones por razón de la materia dentro del objeto de estudio de la Criminología*.

Son muchos los factores que se analizan para hallar, o explicar, el origen o el riesgo que incentiva esta ciberdelincuencia. Factores que, en muchos casos, quieren ser explicados a través de las teorías tradicionales[54] (a las que se le añaden pequeñas variaciones o reinterpretaciones), o mediante la formulación de nuevas hipótesis[55], nacidas precisamente desde el problema cibernético para explicar las conductas cibernéticas. Estas últimas, quizás, sean las que, en un futuro, terminen por exponer con mayor claridad, o al menos profundidad, el problema que en el presente estudio estamos analizando. Y ello por una razón evidente, la variación de lo tradicional no sirve para explicar una fenómeno como la ciberdelincuencia, por mucho que nos ayude, inicialmente, como punto de arranque hipotético.

Pero, sin duda de ningún tipo, una de las cuestiones en las que más está incidiendo la cibercriminología (término acuñado por JAISHANKAR[56]) es en la búsqueda del perfil de ciberdelincuente; en efecto, se parte de que conocer quién es potencialmente el sujeto activo de estos delitos ayudará a estudiar no solo el fenómeno, sino los efectos que produce y la naturaleza de la víctima. En esto tampoco hay excesivo consenso, pudiendo encontrar desde clasificaciones generales de posibles perfiles, a quien, desde instancias más institucionales (como la ONU[57]), niega que exista un perfil determinado ni determinable de ciberdelincuente, al menos en la actualidad.

Como señala, y acertadamente clasifica, CÁMARA ARROYO[58], la primera distinción que se hace, por parte de quienes buscan este perfil, es entre *ciberdelincuentes especializados y ciberdelincuentes no especializados*. Entre los primeros, se encontrarían 1. *los Hacker; 2. Cracker, phreakers y cyberpunks; 3. Viruckers; 4. Traficante de armas (traficante de malware, spyware, virus, etc.); 4. Banquero; 5. Contratista o hackers for hire; 6. Agente especial; 7. Ninjas e information Warriors; 8. Ciber-soldados; 9. Spammer; 10. Domainer; 11. Espías informáticos; 12. Sniffer; 13. Terrorista informático o cyberterrorist; 14. Phisher; 15. Hoaxer; 16. Hacktivista o anarquista.* Entre los ciberdelincuentes del segundo grupo, esto es, los no especializados encontraríamos a: *1. Emugger;*

53 CÁMARA ARROYO, S. *Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente*, en Derecho y Cambio Social. ISSN: 2224-4131. Núm. 60, Abril-junio 2020 P. 471

54 Por ejemplo, la teoría del aprendizaje social y la asociación diferencial de SUTHERLAND y AKERS o teoría del control social, de los vínculos sociales y del autocontrol de GOTTFREDSON & HIRSCHI (Vid. CÁMARA ARROYO, S. Estudios criminológicos contemporáneos… Op. Cit. PP 474-477)

55 Por ejemplo, Teoría de la Acción Situacional revisada para Internet o Ciber Teoría de las Actividades Cotidianas (Vid. CÁMARA ARROYO, S. Estudios criminológicos contemporáneos… Op. Cit. P. 477)

56 Considerado el fundador de esta específica rama de la criminología, este autor entiende que la cibercriminología una materia multidisciplinar que abarca diversos campos, tales como la Criminología, la Victimología, la Sociología, la Ciencia de Internet y las Ciencias de la computación (así lo recuerda CÁMARA ARROYO, S. *Estudios criminológicos contemporáneos (IX): La Cibercriminología… Op. Cit.* PP. 471-472

57 Concretamente, se afirma que Un número relativamente reducido de programadores y piratas informáticos altamente cualificados pueden impulsar la innovación en el terreno de la ciberdelincuencia
y ofrecer sus aptitudes como un servicio delictivo. Sin embargo, la facilidad de acceso a los exploits y los programas maliciosos implica que en muchos casos los autores ya no requieren conocimientos avanzados. Por otra parte, es posible que algunas formas de ciberdelincuencia dependan cada vez más de la presencia de un gran número de "soldados rasos" (ONU. (A/CONF.222/12) 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal… Op. Cit. PP. 10-11)

58 CÁMARA ARROYO, S. *Estudios criminológicos contemporáneos*… Op. Cit. PP 492-508

*ISSN 2255-1824

2. Wannabe; 3. Poseur; 4. Newbie y lammer; 5 Script kiddie. Junto a esta clasificación, coexisten en la doctrina otras muchas[59] .

En definitiva, aunque se pudiera pensar que el ciberdelincuente es, sobre todo, un sujeto con grandes conocimientos en informática y en el uso y creación de nuevas tecnologías, lo cierto es que, en la actualidad, se duda que este perfil sea correcto. De hecho, lo que mayor confusión genera en la criminología es precisamente, que ese perfil, propio de sujeto especial, con cualidades muy específicas, es discutible en la actualidad. Esto no significa que estos sujetos no especializados hayan apartado a un lado a los temidos profesionales del hacking. Todo lo contrario, lo más significativo de la cuestión es que hoy conviven tanto profesionales como meros aficionados del cibercrimen, produciendo, aún más si cabe, enormes dificultades para la investigación. La problemática es evidente, no se sabe a quién buscar. Esto, además, resulta aún más confuso cuando son muchas las disciplinas que estudian el cibercrimen, y el lenguaje dispar, a veces incomprensible, incentiva poco el avance cooperativo en la materia.

Posiblemente, lo que más dificulta la creación de un perfil de ciberdelincuente, y con ello la facilidad de su captura o al menos de su investigación, es que no hablamos de un perfil estandarizado de delincuente técnico o cualificado. Hoy en día, en el que todo el mundo tiene nivel de usuario en lo tecnológico, es relativamente fácil encontrar programas o aplicaciones que, con una pequeña guía, permiten realizar miles de conductas criminales en la red. Es decir, hoy en día no se buscan solo a organizaciones criminales, más o menos profesionales, ya que cualquier persona, desde adolescentes a personas de edad avanzada, sin mayor estructura, que un dispositivo inteligente y una conexión, puede entrar en el ciberespacio con intención criminal. Y figúrese ese problema que genera el anonimato cuando hablamos no de los usuarios de España (el 93,2% de la población de 16 a 74 años ha usado Internet en los tres últimos meses[60]), sino de los usuarios de todo el mundo.

Y ello por no entrar en el sistema de protección/inmunidad que algunos Estados ofrecen para determinados usos, y que impide la aplicación de convenios internacionales para facilitar la investigación internacional del cibercrimen.

Si se quiere llegar a una categorización del cibercrimen es importante asimilar las características que posee ese nuevo fenómeno. Se ha dicho que *entre todas las características que podrían desarrollarse sobre las tecnologías de la información y la comunicación (TIC), nos concentraremos en tres: 1. la inmediatez de las comunicaciones a distancia, 2. la posibilidad de la realización de acciones masivas (automatizadas o no) y 3. la posibilidad de realizar acciones con un determinado nivel de anonimato* (TEMPERINI[61]).

El gran problema de la cibercriminalidad y de la cibercriminología, se deriva de las implicaciones profundas de las tecnologías, que plantean la cuestión de cómo lograr que las respuestas de las autoridades se mantengan a la par con el ritmo de innovación de la ciberdelincuencia (ONU [62]).

59 Véase, por ejemplo, MIRÓ LINARES, F. el cibercrimen Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid. 2012.

60 Según Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares, en el año 2020, del Instituto Nacional de Estadística (Informe de 16 de noviembre de 2020)

61 TEMPERINI, M. Delitos informáticos y cibercrimen: Alcances, conceptos y características, en *Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet.* Erreius. 2018. P. 52

62 ONU. (A/CONF.222/12) 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal… Op. Cit. P. 8

*ISSN 2255-1824

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

VII. CONCLUSIONES

Quizás, y aunque pueda ser tenido por contradictorio, la primera conclusión a la que se debería llegar en esta materia es que solo se pueden plantear premisas ciertas, para conseguir, algún día, generar conclusiones fiables. Estamos ante un fenómeno que, hoy por hoy, es difícil de definir, mediante estándares estancos; no es posible perfilar conductas, ni tampoco sujetos (activos y pasivos). Lo único conocido, y es el problema, es el resultado, esto es, la exposición al riesgo constante e indiscriminado por parte de víctimas anónimas, y la facilidad para atacar bienes de enorme valor personal individual (intimidad, patrimonio, etc.).

Posiblemente, sea más necesario formular preguntas que improvisar respuestas. Preguntas, cuyas respuestas futuras, pueden generar algo de luz a este fenómeno criminal. Desde el punto de vista penal, ¿estamos tan solo ante un mero medio comisivo más (delito informático) o ante una realidad nueva, con tratamiento jurídico diferenciado (sujetos (v.g. bots), bienes jurídicos afectados (v.g. seguridad ciberespacial), conductas, víctimas, finalidades etc.)? Es evidente que aquí hay dos tendencias claramente: Aquella que podríamos tildar de regla general, que considera que el fenómeno informático no es más que un medio comisivo, y que los delitos afectados siguen siendo los tradicionales, sin que el medio comisivo cambie o afecte el tratamiento penal tradicional de la figura. La otra tendencia es considerar que estamos ante una nueva realidad, esto es, ante nuevos delitos, no tratados específicamente (aunque pudieran encajar de manera alambicada en alguna modalidad concreta) en el código penal. Es el caso, por ejemplo, del secuestro de datos (ransomware) o del falso antivirus (Scareware). Decidir si estamos ante una tendencia u otra, haría variar no solo el estudio y la sistemática del fenómeno, sino también la tarea del legislador.

Pero existe un segundo interrogante más; desde un punto de vista más general, la cibercriminalidad ¿es un problema jurídico penal o solo criminológico? Y dentro de esta pregunta, sería necesario analizar tres sub-cuestiones, a saber: Si es materia penal estricta, ¿estaría hoy por hoy huérfana, sin tratamiento normativo, o es una manera de tratar el fenómeno criminal regulado ya (la llamada cibercriminología)? Y, por último, ¿es, en realidad, una rama científica multidisciplinar que busca el perfil estándar de ciberdelincuente como fenómeno social?

Por tanto, estamos ante un nuevo fenómeno en el que, de momento, es mejor formular preguntas que respuestas categóricas. Es importante por ello evitar la fácil investigación que pretende crear respuestas de moda, sin contenido alguno, que quizás solo sirvan para ralentizar el avance de las investigaciones. Empecemos, como en la filosofía clásica, por preguntarnos qué es la cibercriminalidad. El tiempo, los estudios serios (que avancen en ideas y no solo recopilen anglicismos) y la experiencia, nos darán respuesta categórica a nuestros interrogantes. Solo con un conocimiento serio previo, la legislación será estable, y las opiniones conseguirán ser tendencias intelectuales y no meras modas lingüísticas.

VIII. BIBLIOGRAFÍA

AAVV. (Gabinete de Coordinación y estudios. Secretaría de Estado de Seguridad del Ministerio del Interior del Gobierno de España). Estudio sobre la cibercriminalidad en España. 2019.

Cámara Arroyo, S. Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente, en Derecho y Cambio Social. ISSN: 2224-4131. Núm. 60, Abril-junio 2020.

*ISSN 2255-1824

Universidad de Almería - Edificio Departamental de Ciencias Jurídicas - (Edif. D) Planta. 2, Despacho: 2.210
Ctra. Sacramento s/n - La Cañada de San Urbano 04120 Almería

Eduardo Aboso, G. Derecho Penal Cibernético. La cibercriminalidad y el Derecho Penal en la moderna sociedad de la información y la tecnología de la comunicación. Buenos Aires. 2017.

Hernández Díaz, L. El delito informático, en EGUZKILORE, núm. 23, San Sebastián, diciembre 2009.

Jescheck/Weigend. Tratado de Derecho Penal. Parte General (trad. OLMEDO CARDENETE). Granada. 2002.

López-Muñoz, J. Cibercriminalidad e investigación tecnológicas. Madrid. 2020.

Mata y Martín, R.m. Criminalidad informática: una introducción al cibercrimen. Actualidad Penal, Núm. 37, Sección Doctrina, Semana del 6 al 12 Oct. 2003, Ref. XXXVI, tomo 3, Editorial LA LEY.

Miró Linares, F. Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos, en Revista de Internet, Derecho y Política. UOC. IDP Núm. 32, ISSN 1699-8154. Marzo, 2021.

Miró Linares, F. Inteligencia artificial y justicia penal: Más allá de los resultados lesivos causados por robots, en UNED. Revista de Derecho Penal y Criminología, 3ª Época, núm. 20. 2018.

Miró Linares, F. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid. 2012.

Miró Linares, F. La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Revista Electrónica de Ciencia Penal y Criminología. RECPC 13-07 (2011).

Morillas Cueva, L. Sistema de Derecho Penal. Parte general. Madrid. 2018.

ONU. (A/CONF.222/12). 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Seminario 3: El fortalecimiento de las respuestas de prevención del delito y justicia pena frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional, celebrado el 2 de febrero de 2015.

Pérez Arias, J. Sistema de atribución de la responsabilidad penal de las personas jurídicas. Madrid. 2014.

Pérez Gil, J. Recensión del libro de Fernando Miró Llinares, el cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Revista Electrónica de Ciencia Penal y Criminología REFLEXIONES (Recensión). RECPC 15. 2013.

Romeo Casabona, C.M. Poder informático y seguridad jurídica. la función tutelar del derecho penal ante las nuevas tecnologías de la información. Madrid. 1988.

Wall, D. Cybercrime: The Transformation of Crime in the Information Age. Cambridge. 2007.

Wiener, N. Cibernética y Sociedad (trad. Novo Cerro). Buenos Aires. 1958.

*ISSN 2255-1824