Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido

Cybercrime and cybervictimization in Europe: Institutions involved in cybercrime prevention in the United Kingdom

Cibercrime e cibervictimização em Europa: instituições envolvidas na prevenção do cibercrime no Reino Unido

Fecha de recepción: 2015/02/03 Fecha concepto evaluación: 2015/03/20 Fecha de aprobación: 2015/03/30

Marta María Aguilar Cárceles
Doctora en Derecho.
Profesora Asociada de Derecho Penal y Criminología,
Facultad de Derecho, Universidad de Murcia,
Murcia, España.
maguilarcarceles@um.es

Para citar este artículo / To reference this article / Para citar este artigo: Aguilar, M. M. (2015). Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. *Revista Criminalidad*, 57 (1): 121-135.

Resumen

El objetivo es realizar una revisión en materia de prevención del cibercrimen en el ámbito europeo. De acuerdo con los datos estadísticos, Europa es el segundo territorio con mayor número de ciberusuarios a nivel mundial; se destaca el Reino Unido, por ser uno de los países que han destinado más entidades a la prevención del ciberdelito. Por este motivo, por ser el segundo país de la Unión Europea con mayor número de ciberusuarios en la red –y el primero en relación con Facebook–, se ha decidido realizar un exhaustivo análisis sobre los organismos y entidades que orientan sus fines a evitar la cibervictimización, y se hace mención de los menores como víctimas especialmente vulnerables.

Palabras clave

Prevención del crimen, delito informático, cibercrimen, víctima, criminalidad mediante computadoras (fuente: Tesauro de política criminal latinoamericana - ILANUD).

Abstract

The objective consists of carrying out a review of the cybercrime prevention issue in the European sphere. According to statistical data, Europe is the second territory with the highest number of cyber-users worldwide. The United Kingdom stands out since it is one of the countries having devoted more entities to cybercrime prevention. For this reason, and because, as already said, is the second country in the European Union with the largest number of network users—and the first with relation to Facebook—it has been decided that an exhaustive analysis should be carried out on agencies and entities that are currently guiding their purposes and efforts toward preventing cybervictimization, with respect to which special mention is to be made to minors as the most specifically vulnerable group of victims.

Key words

Crime prevention, cybercrime, computer crime, victim, criminality, criminality through the use of computers (Source: Tesauro de política criminal latinoamericana - ILANUD).

Resumo

O objetivo é fazer uma revisão na matéria da prevenção do cibercrime no âmbito europeu. De acordo com os dados estatísticos, Europa é o segundo território com maior número de ciberusuários ao nível mundial; destaca-se o Reino Unido, porque é um dos países que tem destinado mais organizações à prevenção do cibercrime. Para esta razão, para ser o segundo país da União Europeia com maior número de ciberusuários na rede –e primeiramente com relação ao Facebook– decidiu-se fazer uma análise exaustiva dos organismos e das organizações que orientam seus alvos para evitar a cibervictimização, e fornce-se uma menção especial dos menores como as vítimas especialmente vulneráveis.

Palavras-chave

Prevenção do crime, crime informático, cibercrime, vítima, criminalidade por meio dos computadores (fonte: Tesauro de política criminal latinoamericana - ILANUD).

I. "Ciberseguridad": demanda social ante un nuevo fenómeno criminal

1. Aspectos preliminares

No cabe duda de los beneficios aportados por parte de los nuevos medios de información y comunicación a la sociedad moderna, pero igual que las ventajas son innumerables, los efectos negativos adheridos a su desarrollo y proliferación también son notorios.

Partiendo de la afirmación realizada por Quintero (2001) cuando refiere que "internet no es una simple progresión en la evolución tecnológica, sino un cambio revolucionario en los modelos de las relaciones sociales que sirve a la fluidez de los intercambios comerciales y de todo tipo" (p. 369), habría que ser crítico al comprender la acepción "revolucionario", no solo como innovación y avance prosocial, sino también como un hecho transformador y modificador de la vida en sociedad, que ha permitido al delincuente disponer de nuevas formas de actuación e incluso crear tipos delictivos ausentes años atrás.

La posibilidad de realizar comportamientos criminales al margen del espacio físico se hace presente con el desarrollo de las nuevas tecnologías, y se crea de este modo una compleja problemática en el ámbito jurisdiccional. En esta línea, para hacer frente a esta nueva ola de comportamientos típicos, no es baladí la necesaria adopción y entrada en vigor

de normativas adecuadas (indispensable cometido para su prevención, cuya esencia descansa en la cooperación internacional).

De este modo, la justificación del presente análisis se basa en sus implicaciones sociales, y se demuestra cuantitativamente que se trata de un fenómeno creciente, cuyos fines últimos debieran orientarse a la prevención; aspecto deducible del número de usuarios con acceso a las Tecnologías de la Información y la Comunicación (TIC), y que delimita, en última instancia, la motivación y modalidad de actuación del ciberdelincuente.

En la misma línea, ya las propias características de estos delitos los hacen especiales respecto de otros, sobre todo en lo que atañe a la accesibilidad y ubicuidad –particularidad relativa a la localización del ilícito–, lo cual hace su persecución más compleja en comparación con otras tipologías penales que no tuvieran internet como medio de comisión del delito o de lesión del bien jurídico. Al mismo tiempo, una característica fundamental del *modus operandi* radicaría en el anonimato, que se presume en el sujeto activo, pues es más fácil que dicho agente pase inadvertido.

Por otro lado, un aspecto muy significativo de todo lo referido atañe a la figura de la víctima, colectivo que ha hecho posible que la demanda social en ciberseguridad haya tenido efecto en los últimos años. Dicha posibilidad de ser sujeto pasivo en los delitos cibernéticos se relacionaría de manera directa con lo que se entiende que podría denominarse como "cibervulnerabilidad", donde la probabilidad de victimización se vería incrementada exponencialmente, dependiendo de un conjunto de factores de riesgo (externos e internos) que delimitarán la asunción de tal papel. Se trata de un aspecto notorio en determinados grupos poblacionales, como sería el caso de los menores de edad o mujeres, pero que al unísono podría recaer en cualquier individuo, dependiendo de la motivación y objeto del agresor (e. g., acceder al número de cuenta para su uso posterior, venta de billetes de avión falsos a modo de estafa, etc.).

Siguiendo la postura ambientalista de Cohen & Felson (1979), efectivamente la conducta criminal sería la confluencia en el espacio-tiempo de tres factores interrelacionados; esto es, la presencia de delincuentes motivados que atentarían contra víctimas propicias en ausencia de medidas de protección eficaces, fórmula que justificaría la realización del delito. Unido a lo anterior, y extrapolando la noción que atañe a la confluencia espacio-temporal de los elementos indicados, la vulnerabilidad del sujeto se verá incrementada cuando dicha interacción se produce en el entorno no físico. Ahora bien, la cuestión para plantear se centraría en valorar la efectiva correspondencia espacio-temporal de la acción del delincuente cuando actúa en el entorno cibernético, pues precisamente una de sus ventajas se sostendría en la innecesaria coincidencia en espacio y tiempo (e. g., programar un ciberataque desde un país concreto a otro para que se haga efectivo a los dos días, huyendo a su vez el delincuente a un tercer país). De este modo, se entiende que las ventajas de actuación en el ciberespacio superarían las formas tradicionales de perpetración del delito, más aún cuando ya es conocida la porción presumiblemente amplia del denominado "internet profundo o invisible", espacio que hará todavía más difícil de rastrear la huella del delincuente.

En definitiva, papel muy relevante dentro de este ámbito tendrá la motivación del autor en cuanto directriz de dicha oportunidad, pues se verá incrementada ante el conocimiento de las características típicas delimitadoras de los ciberdelitos. Así pues, añadido a lo previamente indicado, entre los aspectos que beneficiarían la producción del ciberdelito y su resultado lesivo se encontrarían: i) la escala o número de usuarios con acceso a internet; ii) el anonimato del ciberdelincuente; iii) la distribución o movilidad indiscriminada y veloz de los datos; iv) la innecesaria confluencia entre los sujetos, o v) la localización global y la ausencia de autoridades que disuadan al ciberdelincuente (Clough, 2010).

Además de ello, la escasez de medidas preventivas se hace evidente debido al origen mismo del ciberataque, pues el desconocimiento de muchas de las nuevas tecnologías, su rápida evolución y propagación, hacen que la intervención no se pueda obstaculizar hasta que se conozcan esas nuevas herramientas de actuación empleadas por el delincuente; esto es, en la etapa posdelictual podrán entonces diseñarse esos medios de disuasión y prevención.

Por todo ello, la necesidad de dar cobertura a la ciberseguridad se instaura como uno de los principales cometidos de los organismos gubernamentales a nivel mundial. De este modo, la efectividad de la seguridad en el ámbito cibernético exclusivamente será plausible sobre la base de la alianza, coordinación y cooperación transfronteriza, lo cual llevará aparejado el problema intrínseco de la materialización de la prevención. Así, e. g., resultaría mucho más complicada la determinación del lugar de la realización de los hechos o la concreción del sujeto que efectivamente realizó la conducta, donde la "indeterminación del ámbito geográfico o inexistencia

de fronteras reales sería una variable favorecedora de dichas actividades" (Díaz, 2010, p. 173). Todo ello afectaría de manera directa la competencia jurisdiccional, ley penal aplicable y procedimiento judicial de actuación, de manera que si bien es cierto que aquellos delitos en los que la acción y resultado se producen en un mismo Estado, ya serían complejos de enjuiciar cuando se alude al ámbito cibernético, cuánto más lo será cuando el delito es perpetrado a distancia, cuando la acción y el resultado se produzcan en diferentes países (Rayón & Gómez, 2014).

En consonancia con lo anterior, a sabiendas de que en otros ámbitos el derecho europeo o internacional viene a armonizar las legislaciones y prácticas nacionales preexistentes, indica Pavón (2003) que "en el ámbito de la cibercriminalidad es el derecho internacional el que viene a impulsar la adopción de medidas nacionales, muchas veces inexistentes o desfasadas en relación al propio progreso técnico", a lo que continúa diciendo que "ello explica por qué a defecto de respuesta internacional coordinada cada Estado individual poco puede hacer" (p. 203).

A su vez, uno de los inconvenientes principales alude al hecho de ser grupos criminales organizados los que actúan por medio de la red, pues si bien es cierto que ya de por sí se requiere de un alto grado de especialización en la lucha contra la cibercriminalidad, cuánto más lo será cuando se trata de colectivos organizados. En esta línea, internet sería el medio que permite su perfecta conexión y coordinación desde diversas áreas geográficas, lo que lleva a admitir que "lo que los individuos pueden hacer, las organizaciones lo pueden hacer incluso mejor" (Broadhurst, Grabosky, Alazab, & Chon, 2014, p. 2).

La problemática de la ciberseguridad concierne directamente al planteamiento sobre la capacidad disuasoria y preventiva de las entidades públicas, mediante la posibilidad práctica de atribuir el hecho a su autor y de localizar la iniciativa criminal. Especial relevancia se le ha otorgado a este aspecto desde importantes organizaciones internacionales, como sería el caso de la OTAN (Organización del Tratado del Atlántico Norte), que dota de especial trascendencia la lucha contra la cibercriminalidad, y lo hace patente mediante la creación de un centro específico en gestión de ciberdefensa. De esta forma, el denominado Centro de Excelencia para la Ciberdefensa Cooperativa permite dar respuesta a la creciente amenaza de la seguridad en la red (Sánchez de Rojas, 2010).

De igual forma, a modo de ilustración, una de las nuevas estrategias llevadas a cabo en materia de ciberseguridad atañe al gobierno de los Estados Unidos, el cual ha creado recientemente una nueva agencia en la lucha contra los ataques cibernéticos, que tiene su base en la centralización de toda aquella información recibida consecuente de una ciberamenaza. En este sentido, el *Cyber Threat Intelligence Integration Center (CTIIC)* ayuda a monitorizar dicha información, sobre la base de las organizaciones encargadas de la ciberseguridad, como sería el caso de la recepción de información de la *National Security Agency (NSA)*, entre otras.

Evidentemente, la necesidad de controlar los ataques cibernéticos refleja el propio derecho de libertad del ciudadano en sus actividades diarias en la red, libertad que se ve limitada, reprimida y coaccionada –normalmente de forma enmascarada–, "gracias" a la sofisticación de los instrumentos y medios empleados por los ciberdelincuentes.

En definitiva, la ciberseguridad se define como un mecanismo de prevención y actuación en la red, dirigido a suprimir –o, mejor dicho, disminuir– el número de delitos perpetrados por medio de internet o contra las nuevas tecnologías, todo ello como consecuencia de la alarma social generada por la era cibernética. Consecuente con ello resulta la demanda del control de su uso y la prevención de sus efectos, pero no solo por tratarse de una nueva forma de actuación del delincuente, sino, y sobre todo, por la incertidumbre que supone el desconocimiento de la amplia e inimaginable gama de objetos materiales y consecuencias derivados del espacio cibernético.

2. Justificación estadística del fenómeno

Habiendo realizado una breve introducción en materia de ciberseguridad, lo cierto es que el verdadero motivo de su estudio no podría justificarse de otro modo sino por medio de cifras reales. En este sentido, no es posible examinar en cifras la efectiva actuación preventiva, sino por medio del análisis del número de cibervíctimas y de la información recibida por diversos organismos que, tanto en el ámbito público como en el privado, intervienen en la disminución de las tasas de incidencia del ciberdelito. No obstante, lo que sí queda claro es el incremento del número de ciberusuarios a nivel mundial, tal y como puede apreciarse en la gráfica 1, donde se observa que el número de ciberusuarios no ha dejado de crecer en los últimos veinte años.

El incremento del número de ciberusuarios amplía la posibilidad de la comisión de ilícitos a través de las TIC y, por tanto, la actuación de los ciberde-

ISSN 1794-3108. Rev. crim., Volumen 57, número 1, enero-abril 2015, Bogotá, D. C., Colombia

lincuentes, motivo por el que puede afirmarse que dicho aumento mantendrá una vinculación directa y positiva con la cibercriminalidad.

Centrando la cuestión en el ámbito europeo, el argumento que justifica el análisis de este fenómeno responde a las propias estadísticas, pues tal y como puede apreciarse en la gráfica 2, dicho territorio sería, en términos porcentuales, el que mayor número de usuarios con acceso a internet presentaría, después de Asia. De este modo, Europa sería el segundo territorio geográfico con mayor número de ciberusuarios (aproximadamente un quinto de la totalidad mundial, tal como se observa en la figura 2).

Además, en consonancia con lo anterior, debiera destacarse lo siguiente:

1) Pese al elevado número de usuarios a nivel mundial, dicha cifra, en cuanto a la localización geográfica de acceso del ciberusuario, se ha visto modificada. Así, e. g., mientras en el año 2012 territorios como Europa y América del Norte representaban, a nivel mundial, un porcentaje mayor que el especificado para el año 2014, en situación contraria se situarían Asia y América Latina, cuyas cifras sí han aumentado desde entonces (Aguilar, 2013).

2) La distribución del número de usuarios varía considerablemente dentro de cada una de las zonas geográficas representadas en la gráfica 2. A modo de aclaración, dentro del espacio europeo, Rusia y Alemania serían los países con mayor número de usuarios, con unas cifras de 87,5 y 71,7 millones, respectivamente, y el tercer lugar lo ocupa el Reino

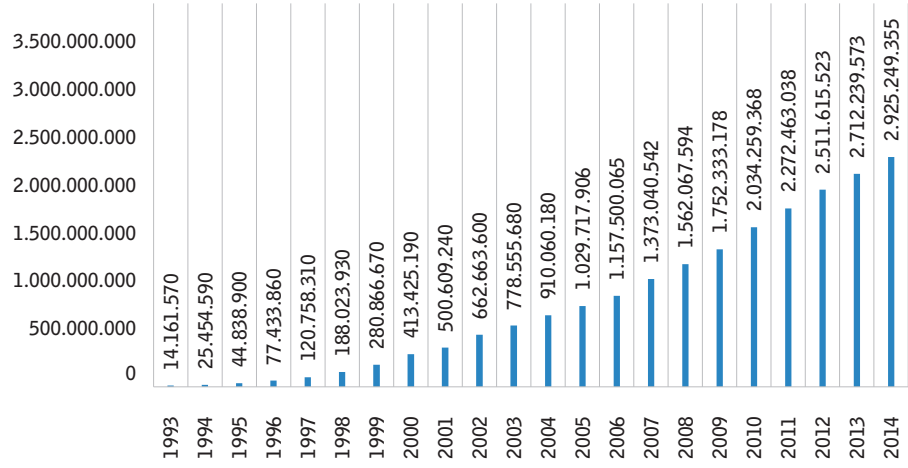

Figura 1. Evolución del número de usuarios en internet (N = millones)

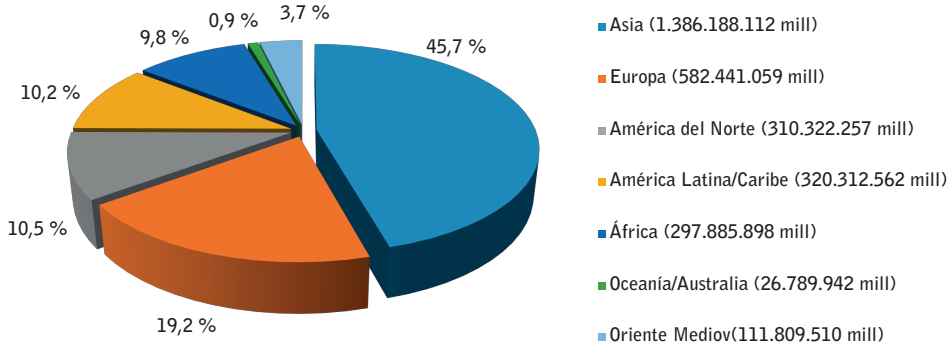

Figura 2. Número de usuarios en internet según la zona geográfica (%)[1]

1 Información obtenida del portal web "World Internet Users Statistics", en la siguiente dirección web: http://www.internetworldstats.com/stats.htm. Actualizada a 15 de febrero del 2015.

Unido, con una tasa que sobrepasa los 57 millones. Habría que señalar que estos datos no son tan dispares como los hallados en otras zonas geográficas, como sería el caso de los países de América Latina, donde se destaca Brasil, con 109,8 millones de usuarios, los cuales casi cuadruplican las cifras estimadas para Argentina y Colombia (32,3 y 28,5 millones de usuarios, respectivamente).

Centrando la cuestión en Europa, el objetivo esencial del trabajo focaliza su interés en el análisis de aquellas entidades que, tanto públicas como privadas, actúan en la erradicación del ciberdelito en el Reino Unido, selección justificada por tratarse de uno de los primeros territorios en abordar el delito cibernético y dotar al mismo de una cobertura multidisciplinar y coordinada.

Así pues, a pesar de haber indicado que Rusia y Alemania presentan tasas mayores de ciberusuarios, la justificación de estudiar el Reino Unido y tomarlo como ejemplo se establece con base en las siguientes premisas: i) pertenecer o ser miembro de la Unión Europea, y ii) utilizar el sistema jurídico *Common Law*, el cual dista mucho de semejarse al actualmente en vigor en España –país cuyos orígenes en este ámbito se remontan al país germano–.

II. Instituciones específicas de intervención

Uno de los problemas fundamentales ligados al desarrollo y evolución de las nuevas tecnologías atañe a la necesidad de implementar programas de actuación en la erradicación de todos aquellos delitos relacionados con las redes. En este sentido, son distintos los aspectos objeto de tratamiento; esto es, desde los organismos encargados de intervenir en la lucha contra el crimen, o las políticas de prevención que se deben llevar a cabo, hasta aquellos colectivos de especial vulnerabilidad, los cuales, entiendo, debieran gozar de un tipo de protección especial.

Conforme a ello, dada la extensión del trabajo, no es posible analizar de manera detallada cada uno de los indicadores que sería pertinente incluir en un programa de prevención, debido, entre otros motivos, a la variabilidad de las tipologías delictivas; por ello, lo que se ha hecho es centrar la cuestión en los organismos que, en la práctica, lidian a diario con el ciberdelito, focalizando la atención en el Reino Unido por los motivos ya aludidos.

1. Principales organismos de actuación

1.1. Europa

Una de las más recientes incorporaciones en el ámbito europeo responde a la creación del European Cybercrime Centre (EC3), encargado de luchar no solo contra la ciberdelincuencia, sino también de aportar análisis de investigación y movilizar los recursos pertinentes en la lucha contra la criminalidad informática. Desde el propio centro se enfatiza la necesidad de unión de fuerzas, la cooperación y colaboración entre las autoridades de los diferentes países en la captura de los ciberdelincuentes, entendiendo que se trata de un delito de carácter transfronterizo, sin límites.

Para tal finalidad, el EC3 cuenta con el apoyo de diferentes organismos, como serían el Grupo de Trabajo de la Unión Europea en la Lucha contra la Ciberdelincuencia (*European Union Cybercrime Taskforce*, EUCTF), la Agencia Europea de Seguridad en Redes e Información (*European Network and Information Security Agency*, ENISA), la Unidad de Cooperación Judicial de la Unión Europea (*European Union's Judicial Cooperation Unit*, EUROJUST) o la Organización Internacional de Policía Criminal (*International Criminal Police Organization*, INTERPOL).

El objetivo en la erradicación de los delitos cibernéticos se establece conforme a los principios instauradores del Convenio de Budapest (2001), el cual, si bien centra su atención en la erradicación de diversas formas de cibercriminalidad, resalta fundamentalmente su interés en la detección de grupos organizados –e. g., atentar contra estructuras críticas del sistema gubernativo–, en aquellos delitos que tienen como objeto a los menores de edad –e. g., abuso o explotación sexual–, y en los relativos al fraude por internet tras el pago con tarjeta de crédito[1].

Por lo que respecta a las medidas de actuación, uno de los aspectos más sobresalientes del EC3 lo presenta su programa de prevención, así como las estrategias adoptadas en la lucha contra la ciberdelincuencia. En esta línea, argumenta la trascendencia de aumentar la comprensión, conocimiento y sensibilización, tanto de los ciudadanos como de las propias empresas de la Unión Europea, siendo la clave contra los ataques cibernéticos el propio asesoramiento. De este modo, defiende que la evolución del cibercrimen es constante, lo que favorece

1 En relación con el fraude, confirma el Centro Europeo que se trata de un negocio altamente rentable para grupos criminales, por suponer, dentro de la Unión Europea y de manera anual, un ingreso aproximado de 1,5 millones de euros a favor del mencionado colectivo.

ISSN 1794-3108. Rev. crim., Volumen 57, número 1, enero-abril 2015, Bogotá, D. C., Colombia

tanto que se constituyan nuevos entornos y modos de perpetración del delito, como que se incremente el número de víctimas potenciales, motivo por el cual los mecanismos de prevención se centran en el seguimiento de dichas tecnologías emergentes.

En definitiva, su estrategia y mecanismo de prevención se basa en el Proyecto 2020, fundamentado en la Alianza Internacional de Protección para la Ciberseguridad (denominado ICSPA, por las siglas en inglés: *"International Cyber Security Protection Alliance"*). Se trata de un estudio dirigido por la Europol, que tiene como objeto adelantar la visión gubernativa y de las fuerzas oficiales a las posibles consecuencias que, en materia penal y criminal, pudieran resultar del avance de las nuevas tecnologías.

Por último, cabría destacar que, efectivamente, los fines previstos resultarán coherentes con el país receptor cuando su propia normativa interna ya establezca modos concretos de actuación o, dicho de otro modo, la citada cooperación quedará limitada a la regulación normativa en materia de criminalidad informática. En el caso de España, desde una perspectiva jurídico-penal, la terminología "delincuencia informática" carecería de relevancia, pues, a efectos penales, no existe una incriminación o tipo concreto que castigue tal conducta, cuestión sí contemplada por terceros países (Morillas, 2005).

1.2. Reino Unido

El continuo desarrollo de las nuevas tecnologías hace que determinados ilícitos vean favorecido su *modus operandi*, propiciando de este modo una actuación delictiva más sofisticada y efectiva por medio de internet. Se trata de un importante hándicap al que han de enfrentarse los organismos gubernamentales, debiendo adaptar los mecanismos de prevención y detección a las nuevas necesidades sociales.

Son diversas las asociaciones, organismos e instituciones que, de un modo u otro, ayudan en la lucha contra los crímenes en la red. Concretamente, en el Reino Unido son diferentes las entidades que, de una manera interdisciplinar, colaboran desde el ámbito internacional, con el objetivo de disminuir la incidencia de tales delitos.

Conforme a ello, siguiendo el documento del 2010 elaborado por el propio Departamento gubernamental del Reino Unido en la lucha contra el crimen informático, y las estrategias frente al mismo, se detallan seguidamente casi una veintena de los organismos que colaboran con dicho Estado para la persecución de los delitos cibernéticos. Un listado general englobaría las siguientes instituciones:

i) *The Association of Chief Police Officers (*ACPO). Asociación integrada por los jefes de policía de Inglaterra, Gales e Irlanda del Norte, la cual firma la denominada "e-crime Strategy" en el 2009, con una duración de 18 meses; sus principales cometidos se orientaban a la ayuda y coordinación efectiva en la lucha contra los delitos cibernéticos. Se trata de una guía de buenas prácticas y asesoramiento para gerentes de las investigaciones del crimen mediante internet.

ii) *Action Fraud* es el centro de informes del Reino Unido sobre la comisión de fraudes, los cuales pasan a formar parte de la Oficina de Inteligencia Nacional del Fraude. Este tipo de ejercicio quedaría complementado con la denominada "Acción contra el Fraude Financiero del Reino Unido", mediante la cual la industria de servicios financieros coordina su actividad frente al fraude y sus consecuencias, tratándose sobre todo de una medida preventiva.

iii) *Cybercirme Forensics Specialist Group*. Colectivo cualificado de profesionales informáticos, abogados, agentes del orden público y otros cargos que, siendo miembros de la *British Computer Society* (BCS), colaboran en el análisis forense del cibercrimen y establecen medidas de actuación contra la ciberdelincuencia. Uno de los medios empleados para promover dicha concienciación social lo constituyen los propios debates, eventos o *blogs* realizados por estos profesionales, donde aportan, desde la perspectiva de un programa independiente pero especializado, apoyo a las propuestas estatales.

iv) *Department for Business, Innovation and Skills* (BIS). El Departamento de Negocios, Innovación y Habilidades desarrolla el programa de seguridad cibernética para el gobierno del Reino Unido en todas aquellas actividades relacionadas con el comercio y la industria, y asegura que dichos colectivos quedan garantizados en cuanto a la prevención del crimen mediante el empleo de las nuevas tecnologías.

Conforme al mismo, uno de los primeros proyectos fue el denominado "Proyecto sobre la Confianza en el Sistema Informático y Prevención de la Delincuencia" (*Cyber Trust and Crime Prevention Project*, CTCP), el cual, apoyado por el propio Ministerio del Interior y orientando sus principales objetivos a la aplicación e implicación de las próximas generaciones de comunicación y nuevas tecnologías, expuso sus principales conclusiones en el año 2004, en lo relativo a aspectos tan diversos como la identidad, autenticidad, vigilancia, seguridad o sistemas de aseguramiento de la información.

v) *The Child Explotation and Online Protection* (CEOP). Este organismo se caracteriza tanto por su

objeto de protección como por el modo de erradicar los ilícitos. Respecto al primero de los aspectos, su objeto de protección y actuación se centraría en un colectivo especialmente vulnerable, los menores de edad, mientras que, con relación al modo de actuación, su principal táctica sería la redirección de la cuenta electrónica del presunto infractor a las de los propios policías, tratándose, por tanto, de un tipo de centro dependiente de la propia autoridad oficial del Reino Unido.

Uno de sus últimos cometidos responde al análisis realizado en dicho Estado bajo la rúbrica *Threat Assessment on Child Sexual Explotation and Abuse* (TACSEA); esto es, para evaluar la probabilidad de sufrir abusos o explotación sexual durante la infancia, siendo su objetivo proporcionar una imagen verídica sobre la magnitud de tales delitos a partir de los aspectos señalados por el CEOP.

En relación con su repercusión en menores durante el año 2011 (y en la proliferación desde el 2009), podría decirse que el denominado "vídeo chat", o sesiones con webcam, ha visto considerablemente aumentado su número de denuncias; todo ello impulsado por redes sociales, como "*Facebook*" –seis veces más visitado que su seguidor "*Twitter*"–. A su vez, cabría destacar que, en su conjunto, se estima que las redes sociales representarían más del 20 % del tiempo dedicado a estar conectado, característica que favorecería la comisión del ilícito conforme aumentase la vulnerabilidad del menor (deficiente supervisión parental, más tiempo conectado, etc.), de manera que llegan a establecerse vínculos de amistad cada vez más estrechos, hasta incitar al menor a la realización de algún tipo de actividad sexual.

vi) *The Cyber Security Operation Centre* (CSOC). El Centro de Operaciones de Seguridad Cibernética, levantado en el año 2009, es responsable de proporcionar análisis sobre el ciberdelito y la situación de concienciación social contra tales amenazas, de manera que actuaría a nivel preventivo, ofreciendo asesoramiento e información sobre los posibles riesgos, tanto para las empresas como para los ciudadanos. Aquí destacaría la creación de la primera "Estrategia de Seguridad Cibernética" en el Reino Unido en el 2009 (*UK Cyber Security Strategy*, CSS), la cual aludiría a la "necesidad de un enfoque coherente sobre seguridad cibernética", incluyendo el apoyo gubernativo, industrial, o a los interlocutores públicos e internacionales, siempre con la finalidad de compartir las responsabilidades. A partir de esta nueva "estrategia" tiene cabida el desarrollo del "Programa Nacional de Seguridad Cibernética" del año 2010 (*National Cyber Security Programme*, PACN), el cual clasificaría los ataques hostiles realizados por medio del ciberespacio contra el Reino Unido como uno de los riesgos prioritarios, junto con el terrorismo, habiendo desembolsado, respecto a aquellos, una totalidad de 650 millones de dólares durante la fecha citada (Downing, 2011, p. 1).

vii) *Department for Children, Schools and Families* (DCSF). A través de este departamento se apoya, mediante el empleo de mecanismos de control social de tipo informal, la prevención de aquellos delitos que tienen como objetivo los menores, incluyendo en este caso las detecciones por parte de la propia escuela y familiares. Se trata de un departamento actualmente suplantado por el Departamento de Educación, en vigor desde el 2010.

viii) *Get Safe Online*. Lanzado en el 2005, destaca por tratarse de una campaña con respaldo gubernamental, fundamentada en la necesidad de que tanto los propios ciudadanos como las empresas supieran defenderse por sí mismas de las amenazas de posibles delitos informáticos.

ix) *Home Office*. Entidad encargada de que la respuesta policial contra el cibercrimen sea efectiva, comprendida a su vez como la entidad organizadora de las estrategias gubernamentales contra los citados delitos.

x) *The Internet Corporation for Assigned Names and Numbers* (ICANN). La Corporación para la Asignación de Nombres y Números en Internet establece direcciones *únicas* por ordenadores, de manera que con base en esta identificación sea posible la coordinación de diferentes ordenadores desde distintas partes del mundo. Pero no solo la coordinación, sino también la localización exacta de los mismos, aspecto que, evidentemente, da nombre al conocido fenómeno "globalización de internet", y que, en definitiva, también viene a auxiliar a las entidades gubernativas para precisar la ubicación del delito.

xi) The *Internet Watch Foundation* (IWF). Organización benéfica instalada en la ciudad de Cambridgeshire (Inglaterra), que tiene como finalidad principal disminuir la probabilidad del empleo de internet como medio de comisión de un ilícito. Para garantizar esta finalidad, se facilita un sistema de conexión directa con el ciudadano, a fin de que denuncie de manera segura y confidencial el posible delito del que ha conocido o ha sido víctima.

xii) *The Medicines and Healthcare products Regulatory Agency* (MHRA). Si bien aparentemente pudiera parecer no tener conexión directa con la cibercriminalidad, la agencia que regula los productos que atañen al ámbito sanitario en el Reino Unido trata de asegurar que ningún producto médico sea distribuido de manera ilegal. En este sentido, la re-

ISSN 1794-3108. Rev. crim., Volumen 57, número 1, enero-abril 2015, Bogotá, D. C., Colombia

lación con la citada temática deviene por entender que internet actuaría como una fuente importante de difusión y venta de tales productos, motivo por el cual a partir de esta fuente se podría favorecer la venta fraudulenta de medicamentos o productos manipulados ilegalmente.

xiii) *The National Fraud Intelligence Bureau* (NFIB). Servicio a cargo de la Autoridad Nacional contra el Fraude, establecida a partir del año 2010 en el Reino Unido. La Oficina de Inteligencia Nacional tiene su sede en Londres, y su objetivo es combatir el delito informático en coordinación con otras entidades, sobre todo aquellas pertenecientes al sector económico.

xiv) *The Office of Cyber Security* (OCS). Oficina de Seguridad Cibernética, encargada de proporcionar liderazgo estratégico y coordinación a todos los poderes públicos en asuntos cibernéticos, mediante la supervisión de distintos programas transversales cuyo objetivo radica en fomentar la ciberseguridad. En definitiva, la también denominada como "*The Office of Cyber Security and Information Assurance* (OCSIA)" se presenta como una unidad de dirección que proporciona tanto seguridad informática como de la información.

xv) *The Office of Fair Trading* (OFT). En línea con lo referido para la MHRA, la Oficina de Comercio Justo tiene como objetivo proteger a los consumidores de la distribución y venta ilegal, así como de aquellas conductas que fuesen contrarias a los principios de libre y justa competencia –en este caso por medio de la red–.

xvi) *The Police Central e-crime Unit* (PCeU). Unidad policial metropolitana de actuación, creada para proporcionar una intervención más efectiva contra los delitos cibernéticos más violentos, así como para mejorar la respuesta frente a las víctimas de tales atentados. Se define como un centro nacional de excelencia, encargado de combatir la delincuencia electrónica tanto en Inglaterra como en Gales e Irlanda del Norte.

xvii) *The Serious Organised Crime Agency* (SOCA). Agencia que centraría su foco de interés en la detección y supresión de todos aquellos delitos cuyo agente o sujeto activo lo constituirían individuos integrados en grupos delictivos organizados. Su objeto de interés recaería principalmente en la detección de los delitos de gran envergadura social, como sería el caso del tráfico de drogas, el contrabando de personas, el fraude, la delincuencia informática o el blanqueo de dinero, entre otros. Se trata de una agencia de aplicación de la Ley, creada en el año 2006 en el Reino Unido, y que: a) colabora con oficinas internacionales en la aplicación de leyes extranjeras, y b) guarda conexión directa con diferentes agencias de inteligencia.

xviii) *The UK Council for Child Internet Safety* (UKCCIS). Como se acaba de ver, si bien existen dispositivos específicos en la actuación contra el crimen organizado a través de internet, el gobierno del Reino Unido también desarrolla planes de actuación específicos en relación con los menores de edad. En este sentido, el Consejo del Reino Unido para la Seguridad Infantil en Internet reúne a organizaciones de la industria, entidades benéficas y del sector público, para trabajar con el gobierno con base en las recomendaciones del Informe Byron 2008 "*Safer Children in a Digital World*". Igualmente, propuesta desde el 2008, se estableció para el año 2009 la primera Estrategia de Seguridad en Internet para Niños en el Reino Unido ("*The first UK Child Internet Safety Strategy*"), conformada por empresas, departamentos gubernamentales y agencias, policía, instituciones, grupos de padres y expertos académicos, que orienta su finalidad a la cooperación a largo plazo en la lucha contra los ciberdelitos.

xix) Por su parte, la *Agencia Europea para la Seguridad de la Información y de las Redes* (*European Information Network Security Agency*, EINSA) ha identificado desde el 2011 al Reino Unido como uno de los principales Estados que, dentro de la Unión Europea, se ocupan de todos aquellos casos relacionados con internet, y reconoce su sofisticación y coordinación en la lucha contra los ataques cibernéticos, así como en la promoción de la seguridad cibernética. En este sentido, podría decirse que la primera estrategia de seguridad cibernética del Reino Unido se produjo en el 2009, que creó la capacidad central de seguridad cibernética en torno a dos vertientes fundamentales. Por un lado, la Oficina de Seguridad Cibernética para coordinar las políticas entre el gobierno y los servicios policiales y de seguridad, y por otro, el Centro de Operaciones de Seguridad, con la finalidad de coordinar la protección de los principales sistemas de tecnologías de la información del país. Conforme a este, las amenazas informáticas para la seguridad podrían clasificarse en: i) códigos informáticos maliciosos cuya finalidad es atentar contra los sistemas de gobierno (*worms*); ii) técnicas cibernéticas de una nación sobre otra para ejercer presión política o económica, y iii) robo de la propiedad intelectual con consecuencias tanto para la seguridad comercial como nacional.

A tenor de lo anterior, habría que resaltar que una de las líneas de investigación de mayor preocupación en la ENISA atañe fundamentalmente a los menores de edad, la cual orienta sus fines a la concienciación sobre protección de datos personales

ISSN 1794-3108. Rev. crim., Volumen 57, número 1, enero-abril 2015, Bogotá, D. C., Colombia

o de aquel material que pudiera afectar a la propia imagen, lo cual incidiría de manera directa en la prevención del *cyberbullying* o del *child grooming*, entre otros ilícitos perpetrados por la red y que afectan a menores.

En definitiva, este organismo surge con la finalidad de controlar los ataques cometidos a través de la red, apoyado en todo caso en la legislación vigente que, sobre delitos cibernéticos, caracteriza al Reino Unido.

Por último, antes de finalizar con el presente epígrafe, habría que destacar una de las medidas más novedosas llevadas a cabo en el Reino Unido en materia de erradicación del ciberdelito, a saber, las "cibercondenas"[2].

Distando mucho de lo que pudiera considerarse en España en la tipificación de ciertos delitos informáticos –que, como ya ha sido dicho antes, está ausente como tipo específico–, las "cibercondenas" en el Reino Unido se han propuesto como una alternativa para aquellos condenados por este tipo de delitos, y una de las finalidades es restringir el acceso a internet, así como limitar la utilización de redes sociales, servicios de correo electrónico o determinados dispositivos de conexión a internet. Se establecen como un conjunto de limitaciones, que de no llevarse a término serían puestas en conocimiento de las autoridades pertinentes, gracias a la identificación del sujeto pasivo con una "ciberetiqueta" específica. Se trata de un tipo de limitación ya empleado como medida cautelar en el acceso ilícito a sistemas de datos (*hacking*), pero que el gobierno intenta ampliar para considerarla parte de la pena, admitiendo incluso su aplicabilidad para evitar la reincidencia, a través de internet, de personas condenadas por delitos contra la indemnidad e integridad sexual. Todo ello se vincularía con los propios fines de la prevención terciaria en dicho ámbito para el tratamiento de víctimas y ofensores (Agustina, 2014).

Sería interesante poder estudiar con detenimiento esta alternativa y realizar alguna implantación dentro la organización del sistema penitenciario español, pues tal y como refiere el art. 25.2 de la Constitución española, todos los programas habrán de orientarse a la reeducación y reinserción del delincuente, tarea imposible si no se tiene en consideración el tipo de tratamiento específico que debiera de recibir cada de delincuente atendiendo al ilícito cometido.

De esta forma, adentrándome hacia una vertiente más criminológica, la necesidad de analizar la relación entre las características del delincuente y el tipo de delito se hace imprescindible para la erradicación del delito –o, mejor dicho, la disminución de sus tasas de incidencia–, por lo que, con base en la propuesta del Reino Unido, considero conveniente que los ciberdelincuentes reciban una modalidad de intervención psicoeducativa específica y adecuada a la (ciber)tipología. Así, no solo sería conveniente evitar el contacto con internet, es decir, su acceso o empleo a través redes sociales, chats (…), sino que lo más importante sería favorecer conductas alternativas, que sustituyan las motivaciones del sujeto que le llevaron a cometer determinadas conductas típicas. Así pues, si, e. g., como medida cautelar se le impone al sujeto una "cibercondena" que prohíbe el empleo de los citados medios, no solo una "ciberetiqueta" valdrá para evitar la comisión de ilícitos (bien porque cambia su contraseña, lo hace a partir de terceras persona o se conecta desde otros ordenadores con un IP distinto), sino que lo importante sería actuar sobre las motivaciones que llevaron al sujeto a realizar dichos comportamientos, para que, una vez cumplida la medida penal, sea capaz de acceder a internet mediante un dispositivo electrónico sin la tentativa de cometer actos delictivos, esto es, sin reincidir.

Por tanto, sería necesario actuar para rebajar la oportunidad delictiva, tarea complicada si se tiene en cuenta que la motivación del agresor quedaría favorecida por su difícil identificación, por su anonimato o por tratarse de ilícitos con un componente transfronterizo esencial, entre otros aspectos. A este respecto, afirma Miró (2011) que "no solo se trata de la identificación de la dirección IP, sino de la posterior concreción del usuario concreto" (pp. 25-26), aspecto fundamental respecto a la responsabilidad penal y posterior en la imputación de un determinado ilícito al "usuario" en cuestión y, en consecuencia, de la sanción y medida de reinserción social correspondiente.

Lo que planteo en líneas anteriores haría alusión al trabajo dentro del ámbito penitenciario con los medios que favorecieron en el sujeto la comisión de un determinado hecho criminal, pues entiendo que en este caso la sola intervención psicoeducativa no sería suficiente si no se contemplan otras conductas alternativas; es decir, al estar inmersos en la era de la información, el sujeto que haya cometido un delito cibernético se verá rodeado continuamente de este tipo de medios cuando haya cumplido la sanción penal impuesta, motivo por el que enfatizo aún más la necesidad de trabajar con este tipo de

2 En este sentido destaca el titular de Europa Press: "*Reino Unido piensa introducir cibercondenas para delitos informáticos. Ciberetiquetas*", 25 de noviembre de 2011. Referencia en http://www.europapress.es/portaltic/internet.

recursos, para asegurar el desarrollo de conductas prosociales antes de dar por terminada la medida señalada. Un ejemplo de ello sería la actuación para evitar la explotación sexual on-line, pues no solo se han de trabajar las motivaciones que llevaron a realizar la conducta, sino que, dado el elevado número de menores de edad que actualmente tienen conexión a internet (o poseen cuenta en distintas redes sociales y participan en chat), entiendo que una buena medida preventiva, que no la única, sería trabajar con este tipo de ciberdelincuentes cuando aparecen imágenes de tal colectivo en las propias redes, es decir, ante el foco de riesgo –para enseñarles entonces a evitar la tentación y, en consecuencia, la infracción–.

En esta línea, uno de los medios para incrementar la ciberseguridad podría ser el contemplar, dentro de los programas diseñados para trabajar con ciberdelincuentes, el manejo adecuado de las nuevas tecnologías, sin descartar, como ya se ha dicho, el empleo de otras campañas preventivas que pudieran llevarse a cabo en colectivos de especial vulnerabilidad (menores en las redes sociales, ancianos en sus primeras compras on-line…) y que, en todo caso, complementarían los mecanismos anteriores.

2. Menores en la red: cibervíctimas especialmente vulnerables

A pesar de que internet brinda a los más jóvenes una amplia gama de oportunidades, tanto de entretenimiento como de comunicación y educación, también son conocidos los riesgos que dichas redes podrían suponer, sea a partir del daño intencionado de terceros, como de la exposición inadecuada de contenido en la propia red. En este sentido, el Consejo del Reino Unido para la Seguridad Infantil en Internet (UKCCIS) entiende que al mismo tiempo que los menores crecen se produce un simultáneo incremento en el mundo digital, por lo que necesitarían conocer dichos medios para estar a salvo de todos los riesgos que podrían tener que enfrentar vía online[3]. Sería la sociedad en su conjunto la que podría formar parte y participar en mantener a los menores a salvo de este tipo de ilícitos, de la "industria de internet", la cual tiene una especial y particular responsabilidad en la creación de herramientas para ayudar a la prevención de los delitos que a partir de dichas redes se originan. En esta línea, considerando el informe "*Safer Children in a Digital World*" como la clave fundamental del UKCCIS, por lo que procedo a analizar seguidamente algunas de sus características fundamentales.

En este informe, redactado por Byron en el año 2008 y cuya traducción respondería a "Niños más seguros en un mundo digital", la autora elabora un análisis sobre los riesgos que tienen los menores tras su exposición continua a internet y durante el empleo de los videojuegos. En este sentido, alude a la Oficina de Comunicaciones del Reino Unido (OFCOM), e indica que si bien es cierto que aproximadamente el 99 % de los menores entre los 8 y los 17 años tienen acceso a internet, no todos ellos desconocen los riesgos que su empleo pudiera conllevar. Así, afirma que las principales preocupaciones, de las que advierten los menores, recaen en el miedo a encontrarse en forma accidental con información de contenido grosero, el no saber diferenciar qué tipo de información de la que se presenta es verídica, el posible contacto no deseado con otros usuarios o el problema del *cyberbullying*, entre otros aspectos (Byron, 2008).

Del mismo modo, refiere cuáles serían aquellas áreas objeto de una mejor y mayor regulación gubernativa en la lucha contra los ciberatentados hacia menores, y advierte que "ni el gobierno ni la industria podrán hacer de internet algo completamente seguro (…). Internet significa que siempre habrá riesgos" (Byron, 2008, p. 81). Así, completando lo anterior, habría que trabajar dos áreas concretas para una mejor regulación de internet en este colectivo: i) la reducción de la disponibilidad, y ii) la restricción del acceso.

Respecto a la primera de las áreas referidas, una de las características más sobresalientes de internet reside en la facilidad con que los usuarios pueden disponer de información y permanecer en contacto unos con otros, lo que supondría un importante riesgo en menores, cuya indefensión quedaría expuesta a futuros cibernautas (visualización de contenido inadecuado, establecimiento de contactos impropios, etc.). En este sentido, con el objetivo de hacer frente a estos peligros, el Ministro del Interior publicó una serie de directrices de buenas prácticas, con el fin de lograr un adecuado manejo de la información de la red por parte de los menores, como serían la moderación de las salas de chat y mensajería instantánea (2003), el empleo de servicios interactivos (2005) y las redes sociales (2008). En todo caso, se trataría de un conjunto de características que el

3 El gobierno del Reino Unido, en la página web del propio Departamento de Educación, refiere la trascendencia de salvaguardar y advertir a los más jóvenes de los riesgos que supone internet, así como de la necesidad de prevenir este tipo de delitos. Referencia: http://www.education.gov.uk/childrenandyoungpeople/safeguardingchildren/b00222029/child-internet-safety.

usuario debiera de respetar para garantizar el uso seguro de determinados productos, así como si es o no aceptable su registro en un determinado lugar, aspecto que enlazaría directamente con la segunda de las áreas mencionadas.

El problema de todo lo anterior radicaría en proporcionar mecanismos de prevención que en realidad fuesen efectivos en la detección del usuario que se adentra en la red; es decir, ¿de qué manera podría restringirse el acceso a determinados individuos, y en virtud de qué aspectos? ¿Cómo podría reducirse la disponibilidad de ciertos materiales y con base en qué criterios personales?

Resulta difícil dar una respuesta a cada una de las preguntas planteadas, no solo por no poder ofrecer una contestación unívoca, sino por la necesidad de adecuar multitud de variables para acertar en la solución; así, e. g., si bien sería infructuoso pretender ausentar los riesgos de internet, también sería una utopía intentar homogeneizar criterios que pudieran filtrar el acceso a determinados contenidos de internet, dependiendo de las cualidades del usuario. En esta línea, indica Miró (2013) que el elemento clave sería la víctima, pues la producción del delito dependerá del riesgo creado, sea tanto al incorporar determinados bienes como al interaccionar con terceros, pudiendo decir que dicho riesgo de victimización quedará además condicionado a la tipología delictiva concreta (Morillas, Patró & Aguilar, 2014).

Además, en lo que atañe a la esfera internacional, no solo las políticas de actuación son diversas, sino también la tipificación de determinados comportamientos y su consecuencia jurídica. Tal es el caso de la variable de edad, por comprender que ciertas conductas antisociales pudieran considerarse delito en un país, pero no en otro, cuando el sujeto activo es menor de edad.

Pero dicha cautela debiera extenderse al sentido opuesto, a la cibervulnerabilidad en menores de edad y su especial protección; esto es, cuando incurren de manera inconsciente en posibles riesgos futuros. Ejemplo de ello sería la acción deliberada de registrarse en determinadas páginas web o redes sociales, donde la exigencia de un requisito específico carece de verificación oficial –como sucede con los menores que se registran en *Facebook* falseando su edad–.

Ante ello, se plantea la cuestión de lo que se entiende por edad mínima de acceso, a lo que se suma si sería posible sancionar dicha actitud del menor cuando conoce y voluntariamente realiza una acción no permitida.

Por otro lado, dejando al margen el empleo de la mentira deliberada con un fin concreto, ¿cómo podría controlarse el acceso de los menores de edad a las redes sociales, a los chats, así como a otros medios, donde ciertamente su acceso estaría prohibido?

Centrando la atención en lo concerniente al ámbito criminológico y a las primeras etapas del desarrollo como cruciales en la demarcación de una trayectoria futura, el papel de los medios de control social de tipo informal se establece como un delimitador fundamental de tales comportamientos[4]. En este sentido, la familia y el grupo de iguales serían los principales ámbitos de referencia para el menor en dicha edad, los cuales favorecen el aprendizaje y consolidación de determinados comportamientos en el sujeto, sean estos o no delictivos. Así, autores como Lösel & Farrington (2012) informan que variables como la relación emocional que se mantenga con los padres o sus estilos educativos, la presencia de patologías en los progenitores, el nivel socioeconómico (…), podrían considerarse factores que, en un sentido u otro, bien como elementos de riesgo, bien como factores de protección, delimitarán positiva o negativamente el desarrollo de la carrera delincuencial.

Un ejemplo de lo anterior, aplicado al campo del cibercrimen, podría encontrarse en el menor con unas inadecuadas relaciones parentales, o incluso con su grupo de amigos, y que busca amistades por medio de las redes sociales, no siendo consciente de los peligros que ello pudiera conllevar; esto es, ante un estado de malestar personal, infravaloración y baja autoestima, la propia persona busca la comprensión y apoyo en terceros, pudiendo llegar a respaldarse en estos medios y acceder a las propuestas de otros individuos. Todo ello sucederá principalmente en determinadas etapas del desarrollo, de manera que si un desconocido comienza a responder a todos los deseos del menor, podría conducirlo a realizar actos inconscientes o sujetos a un nivel muy elevado de manipulación psicológica –de ahí la especial vulnerabilidad de dicho colectivo–[5]. Tal es el caso de la menor que se desnuda y exhibe por medio de una *webcam* a un tercer individuo, sin llegar a conocer el alcance o repercusión

4 A diferencia de los medios de control social informales, se entienden por medios de control social formales aquellos que están delimitados por la ley, que especifican las medidas y sanciones objeto de aplicación por aquellos individuos dedicados en su profesión al cuidado, control y salvaguarda de los derechos de los ciudadanos. Por su parte, el control social informal permite inhibir y disuadir dichos actos delictivos de una manera más activa y comprometida a largo plazo, pues el sujeto recibe las prohibiciones en su entorno cultural y desde personas más cercanas (Redondo & Garrido, 2013, p. 68).

5 De un modo u otro, refiere Miró (2012) que "el acceso y utilización de redes sociales conlleva, de algún modo, la realización de actividades que pueden incidir en una potencial victimización", y describe el estudio de Lenhart & Madden, por medio del cual se observa que más del 93 % de estos menores revela información personal, como su edad o su domicilio (pp. 278 y 279).

ISSN 1794-3108. Rev. crim., Volumen 57, número 1, enero-abril 2015, Bogotá, D. C., Colombia

de su comportamiento, lo que podría llegar a considerarse producto del conocido como *grooming*[6], o incluso sin necesidad de internet, pero haciendo alusión directa a las nuevas tecnologías, como sería el caso del *sexting* (envío de material pornográfico por medio de mensajería móvil, siendo muy posible que acabe en la red)[7].

Por su parte, siguiendo ahora con la revisión del año 2010 del Informe Byron, destaca la autora el papel fundamental no solo de los menores, sino también de sus familias, y se confirma nuevamente el rol de los progenitores como principales instrumentos de aprendizaje en las edades más tempranas. De este modo, el medio familiar se configura como un entorno que pudiera evitar el aumento de menores cibervíctimas.

La autora destaca cuatro fases fundamentales para el fomento de acciones y políticas que auxilien tanto a niños y adolescentes como a sus familias, en la lucha contra la cibercriminalidad (Byron, 2010):

El aumento de la concienciación pública. La campaña de sensibilización social se constituye como un elemento fundamental de las medidas de prevención para la disminución de los índices de cualquier comportamiento que pudiera resultar contrario a las normas o valores, o incluso adverso a las condiciones de salud que caracterizarían a una comunidad. Respecto a la conexión de los menores en internet, la campaña en el Reino Unido se formalizó con un *screening* evaluativo, para analizar en qué medida dicho colectivo emplea la tecnología digital y su concienciación acerca de los riesgos que ello podría soportar.

La mejora en el sistema educativo. Se trata de una fase centrada en la pretensión de cómo enseñar a los menores y jóvenes, desde su centro de estudios, a acceder y gestionar de un modo más seguro el espacio digital, enlazando dicha intervención con los principios de calidad pedagógica[8].

La importancia del papel de las empresas y los proveedores. El desarrollo de un código de prácticas de autorregulación permite a estos colectivos guiar su buena praxis para no verter contenido inapropiado en la red, que pudiera ser accesible por menores de edad.

La función de los videojuegos y dispositivos multimedia. Refiere la autora que han existido grandes progresos en el contenido de los videojuegos desde el año en que se realizó el primer informe, particularmente en la clasificación por edades de su accesibilidad. Indica, a su vez, el compromiso de los propios fabricantes en el desarrollo de controles para garantizar el conocimiento de los padres y su observancia en todos los dispositivos habilitados y vinculados a internet.

Así pues, retomando de nuevo la trascendencia de las redes sociales en cuanto medio favorecedor de la tipificación de ilícitos que atañen a internet, podría decirse que el Reino Unido constituye el país europeo con más entradas de usuarios a este tipo de red social, donde un total de 32.950.400 usuarios en el 2012 tenían su cuenta para acceder a *Facebook,* seguido de Turquía y Francia (porcentajes en relación con el resto de Europa del 13,13 %, 12,8 % y 10,21 %, respectivamente)[9].

Ante ello, desde el EC3 se advierte sobre uno de los principales problemas de este colectivo, el ya nombrado delito de explotación sexual en menores, teniendo como objetivo la identificación tanto de las propias cibervíctimas como de los ciberdelincuentes; esto es, por un lado evitar que la potencial explotación se lleve a término, con la dotación de los medios de auxilio pertinentes, y por otro lado, identificar el *modus operandi* de los perpetradores, a partir del apoyo entre los Estados miembros.

Por último, aun fuera del ámbito de tratamiento expuesto (Unión Europea), Vuanello destaca cómo en materia de normas legales son muchos los países de América Latina que se han concienciado sobre la necesidad de aplicar nuevas coberturas normativas para dicho modo comisivo (2011), lo que, entiendo, ha llevado paralelamente a la instauración de una política-criminal basada en la prevención –lo que de nuevo viene a confirmar el riesgo del ciberdelito como hecho presente a nivel mundial–.

6 Denominado también *cybergrooming*, en términos generales, haría alusión al contacto que establece el pederasta con un menor por medio de la red y con la finalidad de acosarlo sexualmente. Extorsión y chantaje a menores, que facilita a los acosadores la accesibilidad a los menores gracias al empleo de internet; no obstante, cabría resaltar que esta conducta podría incluso darse entre los propios menores de edad (Pardo, 2010, p. 58).

7 En España, la Policía alertó de esta nueva modalidad delictiva entre los más jóvenes, de lo que entiendo que las consecuencias que de ello pudieran desprenderse podrían llegar a ser muy dramáticas para la propia víctima. Vid. http://www.hoy.es/v/20121020/badajoz/policia-alerta-aumento-delitos-20121020.html.

8 Cabría decir que desde el Instituto Nacional de Tecnologías de la Comunicación (INTECO, 2009) se añade además un conjunto de recomendaciones y pautas, no solo para menores sino también para sus padres.

9 Estadística del portal de internet World Stats, actualizada a 31 de diciembre del 2012. Información disponible en http://www.internetworldstats.com/stats9.htm.

III. Consideraciones finales

La delincuencia cibernética constituye uno de los mayores retos de la sociedad actual, objetivo ambicioso si no es por la cooperación y colaboración internacional de diversos organismos gubernamentales y privados.

Estadísticamente, el número de usuarios en la red no ha cesado de crecer; Asia y Europa son los territorios que mayor número de ciberusuarios presentan a escala mundial, y se puede decir que, en la práctica, el 65 % de los usuarios pertenecerían a alguno de esos territorios.

Inevitablemente, hablar del número de ciberusuarios lleva, en forma paralela, a plantear la cuestión del riesgo de criminalidad en el ciberespacio, de manera que, por relación directa y positiva, las probabilidades de que un ciudadano de los presentes en dicho 65 % sea víctima de un delito cibernético es mayor que en el resto del mundo.

Habiendo centrado la cuestión en Europa, el ejemplo tomado como referente en este análisis ha sido precisamente el Reino Unido, que al ser definido por su elevado número de ciberusuarios, se trata de uno de los países que mayor número de recursos han destinado a la erradicación del cibercrimen –en especial hacia la prevención de aquellos tipos que atañen a menores de edad–. Así, tomado como ejemplo gubernativo en materia de cibercriminalidad, lo cierto es que cada una de las entidades destinadas a la erradicación del ciberdelito –sean públicas o privadas–, basan sus fines esenciales en una política-preventiva de actuación –al igual que se hace desde el ámbito internacional–.

En este sentido, la existencia de un grupo de entidades coordinadas y orientadas hacia la consecución de un mismo fin no desmerece la necesaria especialización en las diversas tipologías delictivas que pudieran quedar relacionadas con el ciberdelito, sino que precisamente sería el conocimiento de esa propia especialización el que favorecería la reducción de las tasas de ciberdelincuencia.

Ante esta situación, la prevención no solo debiera de establecerse en la detección de futuros delincuentes –o en el impedimento del desarrollo de ciertos actos delictivos–, sino que, igualmente, debiera orientarse en dos sentido: a) evitar segundas y posteriores victimizaciones, y b) intervenir sobre aquellos colectivos que presenten un elevado grado de cibervulnerabilidad.

En definitiva, la trascendencia de definir un marco de actuación contra el ciberdelito basado en la cooperación internacional no puede pasar por alto: 1) que en la propia normativa interna del país ya se prevean mecanismos de actuación, de manera que ello respaldará una lucha globalizada contra el cibercrimen; 2) que la prevención no solo se basa en evitar la reincidencia, sino en la implementación de estrategias que protejan de la producción del ciberdelito sobre población especialmente vulnerable, y 3) que en la actualidad el ciberdelito es uno de los riesgos prioritarios al que tienen que hacer frente los organismos públicos y privados, para garantizar la ciberseguridad internacional.

Referencias

Aguilar, M. M. (2013). Los delitos informáticos: cuantificación y análisis legislativo en el Reino Unido. *Cuadernos de Política Criminal*, 109 (I): 217-242.

Agustina, J. R. (2014). Victimología y victimodogmática en el uso de las TIC. Desfragmentación del yo en la era digital: "desinhibition effect", esquizofrenia digital e ingenuidad en el ciberespacio. En J. M. Tamarit & N. Pereda (Coords.). *La respuesta de la victimología ante las nuevas formas de victimización*. Madrid: Dykinson.

Barker, R. (1963). *The stream of behavior*. New York: Appleton-Century-Crofts.

Barrio, M. (2011). Los delitos cometidos en internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010. *La Ley Penal*, 86.

Broadhurst, R., Grabosky, P., Alazab, M. & Chon, S. (2014). Organizations and Cyber Crime: An analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, 8 (1): 1-20.

Byron, T. (2008). Safer Children in a Digital Word. A summary for children and young people. Children and New Technology, p. 4. Consultado en http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews.

Byron, T. (2010). Do we have to safer children in a Digital Word? A review of progress since the 2008 Byron Review. *Children and New Technology*. Consultado en http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews.

Clough, J. (2010). *Principles of Cybercrime*. Cambridge: Cambridge University Press.

Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review*, 44: 588-608.

ISSN 1794-3108. Rev. crim., Volumen 57, número 1, enero-abril 2015, Bogotá, D. C., Colombia

Díaz, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest. *Revista Electrónica de Derecho de la Universidad de La Rioja* (REDUR), 8: 173.

Downing, E. (2011). Cyber security - A new national programme. Science and Environment Section, House of Commons, 3-9.

INTECO (2009). *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres.* Madrid: Observatorio de la Seguridad de la Información.

Lösel, F. & Farrington, D. (2012). Direct protective and buffering protective factors in the development of youth violence. *American Journal of Preventing Medicine,* 43 (2): 8-23.

Miró, F. (2011). 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: 25-26.

Miró, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

Miró, F. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. *Revista Española de Investigación Criminológica* (REIC), 11: 1-35.

Morillas, D. L. (2005). *Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comisivas relacionadas con internet.* Madrid: Dykinson.

Morillas, D. L., Patró, R. M. & Aguilar, M. M. (2014). *Victimología: un estudio sobre la víctima y los procesos de victimización*. Madrid: Dykinson.

Pardo, J. (2010). Ciberacoso: cyberbullying, grooming, redes sociales y otros peligros. En J. García González. *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en internet*. Valencia: Tirant lo Blanch.

Pavón, J. (2003). Derecho Internacional Público. La labor del Consejo de Europa en la lucha contra la cibercriminalidad: el Protocolo Adicional al Convenio N.° 185 sobre cibercriminalidad relativo a la incriminación de actos de naturaleza racista y xenófobos cometidos a través de los sistemas informáticos. *Anuario de la Facultad de Derecho*, XXI: 187-204.

Quintero, G. (2001). Internet y propiedad intelectual. Internet y Derecho Penal. *Cuadernos de Derecho Judicial*, 369-370.

Rayón, M. C. & Gómez, J. A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*, XLVII: 209-234.

Redondo, S. & Garrido, V. (2013). *Principios de criminología*. Valencia: Tirant lo Blanch.

Sánchez de Rojas, E. (2010). La ciberseguridad: retos, riesgos y amenazas. *Revista Ejército*, 837: 136-143.

Smith, R. G., Grabosky, P. & Urbas, G. (2004). *Cyber Criminals on Trial*. Cambridge: Cambridge University Press.

Vuanello, R. (2011). La criminalidad como atentado a los derechos de los más jóvenes. *Revista Criminalidad*, 53 (1): 249-260.

ISSN 1794-3108. Rev. crim., Volumen 57, número 1, enero-abril 2015, Bogotá, D. C., Colombia