Universidad Internacional de La Rioja
Grado en Criminología

Enfoque criminológico del cibercrimen

Trabajo de fin de grado presentado por: Juan Antonio Iglesias Gómez

Titulación: Criminología.

Director/a: Beatriz Romero Flores

Ciudad: Madrid.

11/03/2019

Firmado por: Juan Antonio Iglesias Gómez

A mi mujer, Raquel, y a mis hijos; Alejandro y Javier

Índice

1. AGRADECIMIENTOS

Es innegable que, en los momentos de mayor dificultad, siempre surgen con un valor especial las personas que con su inestimable ayuda posibilitan los proyectos en nuestra vida. En este apartado de agradecimientos tratare de recordar a todas las personas que de una manera u otra me han ayudado a culminar el presente Trabajo de Fin de Grado.

Deseo comenzar agradeciendo a Beatriz Romero Flores, mi directora de este TFG, su inestimable ayuda y comprensión. Gracias por orientarme, gracias por tus sabios consejos, y sobre todo gracias por sacrificar el poco tiempo que me consta que posees, en ayudarme, detrayéndolo incluso de aquel que reservas para tus seres más queridos, guiándome en la consecución de esta meta.

Especialmente influyente, para la elección del tema elegido en este trabajo, fue la impartición de la asignatura de Delincuencia Tecnológica por la profesora Gema Martínez Galindo, a la cual aprovecho la ocasión para agradecerla su dedicación y actitud, siempre positiva. Dicha elección se debe, en gran medida, a la fortuna que supuso haber podido asistir a sus clases.

Con el presente trabajo cierro un ciclo en mi vida con un cierto sabor agridulce, provocado, por un lado, por la enorme satisfacción de completar el Grado en Criminología de la UNIR, tras años de constancia, esfuerzo y privaciones personales y, por otro lado, debido a la amarga realidad de las pérdidas familiares, de aquellos que lamentablemente se fueron y con los cuales no voy a poder compartir este momento especial. Desde donde estéis os hago participes, con una emoción desbordada, especialmente a ti Carmen, que desgraciadamente nos dejaste tan pronto, y a ti Antonio, que nos has dejado recientemente sin poderlo celebrar juntos.

También deseo expresar mi eterna gratitud, una vez más, a mis padres, especialmente relevantes, ahora y siempre, en este logro y en todos aquellos que me han acompañado a lo largo de mi vida, espero y deseo que este también os haga sentir igual de orgullosos que los anteriores.

Termino este apartado, destacando y agradeciendo, por encima del resto, a Raquel, que siempre me apoya en todo de manera incondicional, que siempre se queda en último lugar, con un inmutable y perenne sacrificio por nuestra familia, pensando primero en Alejandro, en Javier y en mí muchísimo antes que en ella. Sin tu total apoyo este trabajo difícilmente se hubiese materializado, te prometo tomarme un largo descanso y no “complicarme tanto la vida” como me repites tantas y tantas veces con razón, al menos durante un tiempo…Gracias amor.

2. ACRÓNIMOS:

AEPD; Agencia Española de Protección de Datos.

CCN; Centro Criptológico Nacional, dependiente del CNI.

CIS; Centro de Investigaciones Sociológicas dependiente del Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad.

CNI; Centro Nacional de Inteligencia.

CNP; Cuerpo Nacional de Policía.

CNPIC; Centro Nacional de Protección de Infraestructuras y Ciberseguridad.

DLE; Diccionario de la Lengua Española.

DSN; Departamento de Seguridad Nacional.

DGOJ; Dirección General de Ordenación del Juego.

EC3; European Cybercrime Centre (El Centro Europeo para la Ciberdelincuencia).

ENISA; European Union Agency for Network and Information Security (Agencia Europea de Seguridad de las Redes y de la Información).

Eurojust; European Union Agency for Criminal Justice Cooperation (Agencia de la Unión Europea para la Cooperación en Justicia Criminal).

Europol; Agencia Europea de Cooperación Policial.

FGE; Fiscalía General del Estado.

GC; Guardia Civil.

GDT; Grupo de Delitos Telemáticos de la Guardia Civil.

GSM; se derivan del término inglés Global System for Mobile communications. Es un programa estándar de telefonía móvil, establecido por medio de una combinación de antenas terrestres y satélites.

ICANN; Internet Corporation for Asigned Names and Numbers (Corporación para la Asignación de Nombres y Números en Internet).

INE; Instituto Nacional de Estadística.

Interpol; Organización Internacional de Policía Criminal.

IOCTA; Internet Organised Crime Threat Assessment (Evaluación de la Amenaza de la Delincuencia Organizada en Internet).

IPC3; Intellectual Property Crime Coordination Centre (Coalición Coordinada para Delitos contra la propiedad intelectual).

IS4K; Internet Segura for Kids.

J-CAT; Joint Cybercrime Action Taskforce (El Grupo de Acción Conjunta sobre Ciberdelincuencia).

KiVa; Kiusaamista Vastaan (Programa contra el acoso escolar creado en la Universidad de Turku en Finlandia).

MCCD; Mando Conjunto de Ciberdefensa

NIST: National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología, del Departamento de Comercio de los Estados Unidos).

ONG; Organización no gubernamental.

ONIF; Oficina Nacional de Investigación del Fraude.

ONTSI; Observatorio Español de la Economía y la Sociedad Digital de la entidad pública red.es perteneciente al Ministerio de Economía y Empresa.

OSI; Oficina de Seguridad del Internauta OSI.

SEC; Sistema Estadístico de Criminalidad.

SOCTA; Serious and Organised Crime Threat Assessment (Evaluación de la Amenaza de Delincuencia Organizada y Grave de la UE).

TE-SAT; EU Terrorism Situation and Trend Report (Informe de Situación y Tendencia del Terrorismo de la UE).

UIT; Unidad de Investigación Tecnológica del CNP.

UNODOC; United Nations Office on Drugs and Crime (Oficina de las Naciones Unidas contra la Droga y el Delito).

3. RESUMEN:

En el presente Trabajo de Fin de Grado de Criminología se tratará de analizar el riesgo real y permanente que supone cotidianamente para la mayor parte de la población estar conectado a Internet. La interrelación que se produce en el ciberespacio trae consigo aspectos indiscutiblemente positivos en nuestras vidas, a todos los niveles; personal, familiar, laboral y social, pero también genera aspectos negativos debido a los potenciales riesgos delictivos y victímales que se encuentran muy presentes en el mundo virtual.

Partiendo de la reformulación teórica de Miró (2013), respecto a la Teoría de las Actividades Rutinarias de Cohen y Felson (1979), se analizarán dichos riesgos *online* sobre la base de la importancia que tienen las conductas, los actos y los hábitos de las víctimas en relación al aumento o la disminución de la probabilidad de recibir un ataque a través del ciberespacio.

Palabras clave; cibercrimen, cibercriminalidad, ciberespacio, cibervíctima.

SUMMARY:

In this Final Degree Project of Criminology, we will try to analyze the real and permanent risk that it is daily for most of the population to be connected to the Internet. The interrelation that occurs in cyberspace brings with it indisputably positive aspects in our lives, at all levels; personal, family, work and social, but also generates negative aspects due to the potential criminal and victim risks that are very present in the virtual world.

Starting from the theoretical reformulation of Miró (2013), regarding the Theory of Routine Activities of Cohen and Felson (1979), these risks will be analyzed online based on the importance of behaviors, acts and habits of victims in relation to the increase or decrease in the probability of receiving an attack through cyberspace.

Keywords; cybercrime, cybercriminality, cyberspace, cybervictim.

4. INTRODUCCIÓN

Resulta una obviedad afirmar que el desarrollo tecnológico está transformando de forma permanente la sociedad actual afectando a múltiples áreas; la industria aeronáutica, militar, automovilística, médica, farmacéutica, la robótica, etc. Dentro del contexto de expansión tecnológica en el que nos encontramos merece mención especial el desarrollo de las tecnologías de la información y la comunicación (TIC), que verdaderamente esta alcanzado cotas impensables de repercusión social, desconocidas hasta la fecha, debido principalmente a un factor fundamental; el aumento de nuestra capacidad para comunicarnos y para relacionarnos en cualquier tiempo y lugar, produciéndose, como consecuencia de ello, una verdadera transmutación de nuestro modelo de sociedad.

En la era digital en la que estamos inmersos y seguiremos estando inmersos, sine die, la accesibilidad a la información se sitúa a la velocidad a la que golpeamos una tecla, tal es la dependencia tecnológica generada que cada vez queremos tener más capacidad para poder almacenar la información, más velocidad para interconectarnos y dispositivos más agiles y reducidos en peso y tamaño para poder tener la mayor funcionalidad posible. En dicho contexto; ¿Cómo nos planteamos nuestra seguridad personal?, ¿Somos conscientes verdaderamente de los riesgos y peligros existentes cuando nos conectamos a la red?, ¿Cuándo tenemos un problema relacionado con dicha seguridad como lo resolvemos?, ¿Dónde y cuándo informamos o denunciamos un problema de seguridad relacionado con las TIC?, ¿Tenemos el grado de adaptación necesario, en términos de prevención delictiva, para la era digital?, ¿Cómo solucionamos la brecha digital existente entre los padres y los hijos de cara a su seguridad personal?, estas son algunas de las cuestiones principales que tratarán de abordarse en este trabajo de fin de grado.

Las problemáticas asociadas al uso inapropiado de las tecnologías tienen como protagonistas principales el uso de la telefonía móvil y de las redes sociales, situación que afecta no solo a la población adulta, sino también y especialmente a la población adolescente e incluso preadolescente (motivado sobre todo por la necesidad de sentimiento de pertenencia al grupo y a la falta de madurez, a las que habría que sumar las carencias de información y formación específica de los más jóvenes).

El teléfono inteligente es un buen ejemplo para evidenciar el ritmo vertiginoso al que avanzan estas tecnologías y como su influencia se está transmitiendo, exponencialmente, en nuestras relaciones personales, familiares y sociales. Desde la irrupción en el mercado de los primeros *smartphones* ¿qué ha ocurrido?, la respuesta la encontramos en el informe anual Mobile Economy,

que publica cada año la GSMA[1], y no deja lugar a dudas; actualmente es el dispositivo más extendido del mundo y lo seguirá siendo en el futuro más próximo (la población que posee un smartphone alcanzó en 2018 el 57% y supondrá el 79% en el 2025 a nivel mundial). En el informe también se destacan las cifras siguientes; el número de usuarios únicos de telefonía móvil alcanzó los 5.100 millones y el número de líneas (tarjetas SIM) los 7.900 millones, con una previsión de 5.800 y 9.200 millones respectivamente para el año 2025; los usuarios de internet móvil pasarán de 3.600 millones en 2018 a 5.000 millones en 2025; las conexiones relacionadas con el Internet de las cosas, pasarán de 9.100 millones en 2018 a 25.200 millones en 2025 (…)

Otro aspecto que se considera importante analizar es el aporte de la Criminología respecto al estudio de un fenómeno tan amplio y complejo como el cibercrimen, el cual se abordará con un sentido crítico, dada la escasa implicación científica que se está aportando desde la misma. Con este TFG se tratará de poner de manifiesto la apremiante necesidad de que surjan contribuciones empíricas al saber criminológico sobre este fenómeno, que empieza a no ser tan nuevo, y cuya previsión futura apunta a un incremento exponencial del mismo, relacionado con el enorme aumento del internet de las cosas en general y de las TIC en particular.

En suma, se tratará de abordar, desde el punto de vista preventivo, el análisis sobre la repercusión que la revolución tecnológica está teniendo sobre nuestra seguridad, tanto a nivel público como privado, debido al aumento y evolución de las denominadas formas tradicionales de delincuencia que han crecido de forma superlativa a la par que las nuevas tecnologías. A tal fin, sobre la base teórica de la reformulación de la teoría de las actividades rutinarias, se analizará el especial protagonismo que cobra la víctima en el ciberespacio y como su conducta y sus actividades online marcan la clara diferencia, en términos referidos a la oportunidad delictiva, de convertirse o no en el blanco de los ciberdelincuentes.

5. PLANTEMIENTO DEL TRABAJO Y FINALIDAD:

La justificación del presente trabajo se fundamenta en la apremiante necesidad de aumentar los conocimientos, no solo, sobre los riesgos que entraña el uso de las TIC, sino también, sobre los comportamientos que desarrollamos cuando interactuamos en *Internet* y la trascendencia que los

[1] La GSMA representa los intereses de los operadores móviles de todo el mundo, reuniendo a casi 800 operadores y más de 300 compañías del ecosistema móvil en general. La GSMA también organiza el Mobile World Congress, el Mobile World Congress de Shanghai, Mobile World Congress Américas, y la serie de Conferencias Mobile 360.)

mismos pueden tener en relación al evento criminal. La urgencia se basa en el déficit actual que existe respecto al grado de adaptación necesario al nuevo mundo virtual que nos rodea, en el cual deben incluirse, no solo, a los cibernautas particulares, sino también a los institucionales.

En relación a los objetivos del presente TFG se persiguen dos tipos de objetivos; generales y específicos, los cuales, se exponen a continuación de forma breve:

- Objetivos generales;
  - Analizar desde un punto de vista criminológico los entornos digitales en los que se producen los ciberataques.
  - Analizar la problemática que origina la ciberdelincuencia respecto a la determinación de la jurisdicción y competencia de los tribunales penales.
  - Efectuar un análisis criminológico sobre la dimensión real de la amenaza del cibercrimen, con especial referencia a la cifra negra del cibercrimen, y la repercusión que tiene sobre su prevención.
- Objetivos específicos;
  - Efectuar una nueva definición del concepto cibercrimen y con base en la misma una nueva clasificación de los tipos de cibercrimen.
  - Analizar el perfil victimológico de la víctima *online*, en relación al perfil victimológico de la víctima *offline.*
  - Analizar el perfil criminológico del ciberdelincuente efectuando la necesaria distinción entre el hacker y el cibercriminal.
  - Determinar las líneas de actuación para la prevención del cibercrimen desde el enfoque teórico de las actividades cotidianas.

Se afronta este trabajo desde un enfoque criminológico, dada la complejidad del tema objeto de estudio, para tratar de ampliar la perspectiva respecto al auge de la ciberdelincuencia, así como de los diferentes instrumentos y recursos preventivos necesarios para amortiguar su impacto en la sociedad. Para la consecución de los objetivos anteriormente referidos se va a emplear un método de investigación mixto, con una carga mayor respecto a la investigación teórica que respecto a la investigación empírica, dado que esta última se empleará principalmente en relación a los datos estadísticos existentes actualmente sobre la ciberdelincuencia. En relación al tipo de fuentes empleadas se utilizarán; referencias bibliográficas de autores expertos en el campo objeto de estudio

propuesto; el cibercrimen. Además, se emplearán fuentes normativas y otra serie de fuentes que contendrán información procedente de; páginas Web, revistas electrónicas, periódicos en línea e informes procedentes de organismos relacionados con el marco teórico expuesto en el presente TFG.

6. DESARROLLO:

Se puede definir la criminología como; "*la ciencia empírica e interdisciplinaria que tiene por objeto el crimen, el delincuente, la víctima y el control social del comportamiento delictivo; y que aporta una información válida, contrastada y fiable sobre la génesis, dinámica y variables del crimen; contemplando éste como fenómeno individual y como problema social; así como su prevención eficaz, las formas y estrategias de reacción al mismo y las técnicas de intervención positiva en el infractor y la víctima."*(GARCÍA-PABLOS 2009, p. 53)

Partiendo de esta definición se tratará de efectuar un análisis criminológico del objeto de estudio de esta ciencia trasladándolo al nuevo contexto virtual surgido en el ciberespacio. La primera reflexión que surge al respecto es referente a la dificultad que, tradicionalmente, ha tenido que superar el análisis multidisciplinar y científico de la criminología, debido a que no ha gozado del consenso deseable respecto a su definición, método, objeto o funciones. Pues bien, si en el "mundo físico" el aporte de información valida, contrastada y fiable sobre la génesis, dinámica y variables del crimen ha resultado y sigue resultando complejo, en el "mundo virtual" este aspecto se complica, de forma exponencial, por diversas razones que se intentarán abordar a lo largo de este trabajo.

La segunda reflexión surge respecto a la consecución de las metas y logros que persigue la criminología, no solo, desde el punto de vista intervencionista (lucha contra el delito y resocialización del delincuente), sino también, desde el punto de vista de la prevención contra el crimen (control y estrategias de neutralización frente al mismo). Su análisis nos lleva también, irremediablemente, a la misma conclusión respecto al incremento de la dificultad que supone su estudio, debido a las nuevas características que presenta la criminalidad en el ciberespacio y que también serán objeto de análisis en el presente TFG.

Ambas reflexiones iniciales nacen con una dosis importante de escepticismo, debido a que la Criminología, apenas ha explotado el estudio sobre la relación existente entre la evolución tecnológica y la modificación actual de la delincuencia. No obstante, si efectuamos un repaso estadístico sobre los datos que existen al respecto de esta cuestión, puede resultar paradójico y

contradictorio efectuar dicha afirmación, dado que son ingentes las cifras y datos que se han publicado y se siguen publicando respecto a esta nueva forma de criminalidad.

Durante el desarrollo de este trabajo se tratará de analizar porqué desde la Criminología prácticamente se ha obviado y se está obviando este nuevo fenómeno. Con dicha finalidad, se efectuará una aproximación sobre su verdadera repercusión tanto a nivel particular como a nivel institucional, es decir, respecto a si la percepción de esta nueva forma de criminalidad tiene la relevancia de una verdadera amenaza a la seguridad, o si por el contrario dicha amenaza está siendo exagerada, principalmente, desde un ámbito mediático en unos casos y empresarial en otros (concretamente determinadas empresas tecnológicas que obtienen cuantiosos réditos económicos relacionados con la ciberseguridad).

6.1. Cibercrimen; análisis de su verdadera repercusión

Tal y como se apuntaba en el apartado anterior resulta necesario, como cuestión inicial, contextualizar este fenómeno, no solo, desde un punto de vista terminológico, sino también desde el punto de vista de su verdadera dimensión, cuestiones ambas que se tratan, seguidamente, en este apartado:

6.1.1 Aproximación conceptual del cibercrimen:

El motivo por el cual surge la necesidad de delimitar esta nueva forma de delincuencia, llevada a cabo en el ciberespacio, es doble; en primer lugar, para poder efectuar un análisis criminológico lo más riguroso posible; en segundo lugar, para utilizar un término que pueda condensar con la mayor precisión posible el alcance de este problema con el mayor número de matices posible, evitando así la dispersión terminológica existente, lo que provoca que se utilicen de manera confusa los términos; delito informático, cibercrimen, delito tecnológico, ciberdelito, criminalidad informática, ciberdelincuencia o cibercriminalidad. Cabe señalar al respecto que la Comisión Europea en una Comunicación[2], del año 2007, denominada; "Hacia una política general de lucha contra la Ciberdelincuencia", abordó esta cuestión, ante la falta de una definición consensuada del término, ofreciendo la siguiente definición de cibercrimen; "*actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas*"

[2] COM (2007)267 final, de 22 de mayo de 2007.

Para efectuar el análisis de este fenómeno, desde un enfoque criminológico, se empleará en el presente trabajo el término cibercrimen, dado el amplio uso que se viene efectuando del mismo por las ciencias sociales, en un amplio número de países, que utilizan el término *cybercrime* (MIRÓ 2012, p. 33), cuya definición en español no es establecida por el Diccionario de la Lengua Española (tampoco recoge el término cibercriminología), no obstante, si recoge *ciber-,* que indica relación con redes informáticas y el término *crimen*, que significa delito grave. Conviene especificar qué, existen diversas definiciones al respecto del concepto cibercrimen, aunque atendiendo al objeto de estudio del presente trabajo, y a falta de una definición admitida doctrinalmente se propone una nueva definición, surgida de la necesaria reflexión criminológica que estará presente a lo largo de este TFG, por consiguiente, se entiende por cibercrimen; *Toda conducta delictiva, cuya intencionalidad se sustenta en el daño o perjuicio de tipo personal, social, político o económico, generada o favorecida mediante el uso de las TIC en el ciberespacio.* Reseñar respecto al término cibercriminalidad y su analogía con el término cibercrimen que, dado que viene siendo utilizado generalmente para referirse al fenómeno de la criminalidad en el ciberespacio, en este trabajo se utilizaran ambos conceptos con un carácter sinónimo (dado su carácter indistinto).

6.1.2 Clasificación de los Tipos de cibercrimen:

Para ilustrar mejor la delimitación terminológica efectuada y atendiendo al propósito que persigue la criminología, se sugiere, a continuación, una nueva clasificación de los tipos de cibercrimen que se reflejan en la tabla siguiente:

Cibercrímenes personales	**Cibercrímenes Sociales**	**Cibercrímenes económicos**	**Cibercrímenes políticos**
• Ciberinducción al suicidio • Ciberinducción al daño físico • Retos virales que atentan contra la vida, contra la integridad física, y moral. • La práctica del *happy slapping*	• *Cyberbullying* o acoso escolar al menor en Internet • *Cyberstalking* o *Cyberharassment* • *Sexting* • *Cybergrooming* u *online grooming.*	• Ciberfraudes • Ciberblanqueo de capitales • Ciberespionaje de empresa • Robos de identidad • Suplantación de identidad • Ciberextorsión • Ciberpiratería industrial • Ciberpiratería intelectual • Cibercomercio de datos personales • Cibertráfico de drogas • Distribución de pornografía infantil en Internet • Ciberocupación • Juegos de azar online ilegales.	• Ciberguerra • Ciberespionaje • Ciberactivismo político en la red • *Cyberwarfare* • Ciberterrorismo • Ciberactivismo ideológico en la red • *Cyberhate speech u online hate speech*

Tabla de elaboración propia con una nueva sugerencia de clasificación del cibercrimen actual.

Reconociendo las limitaciones de dicha clasificación, y siendo consciente de que el aporte criminológico, si realmente llega a alcanzar tal consideración, es muy modesto, se efectúa con el objetivo de mejorar la comprensión del fenómeno cibercrimen al incluir las últimas tendencias criminales surgidas en el ciberespacio, muchas de las cuales se terminan materializando en el mundo real. Por esta razón se introduce un apartado referido a los cibercrímenes personales, para distinguir aquellas conductas que se originan en la Red y que atentan contra la vida, la integridad física y moral de las personas.

La clasificación propuesta se configura desde una óptica criminológica abierta, es decir, trata de condensar los fenómenos delictivos que se producen en la actualidad a través de internet, toda vez que siguen surgiendo y seguirán surgiendo nuevas modalidades criminales en el ciberespacio. Se efectúa dicha clasificación, por tanto, con una perspectiva amplia, en contra del criterio mantenido por MIRÓ, que considera que su clasificación del cibercrimen enumera todas las formas de ataque existentes en el ciberespacio. Precisamente, el carácter cambiante que se le otorga, no solo, al mundo online, sino también, al comportamiento online, provoca que se produzcan con asiduidad conductas que modifican las tipologías criminales en el ciberespacio (algunas de las cuales se configuran como formas de ataque evolucionadas de las ya existentes) como, por ejemplo; las APT, o Amenazas Persistentes y Avanzadas, las cuales precisan un estudio y enfoque distinto para su detección y prevención (FRIEDBERG, SKOPIK, SETTANNI, Y FIEDLER, 2015).

Siguiendo con el análisis, sobre el surgimiento de conductas online que pueden incluirse en la clasificación del cibercrimen, podríamos citar también como ejemplo el fenómeno del *oversharing o sharenting,* que se produce cuando los padres publican y comparten en las redes sociales, de forma profusa, información e imágenes de sus hijos cuando son menores de edad. Esta conducta, que ya está teniendo consecuencias legales significativas en países de nuestro entorno, como Italia y Francia, (VOLPATO, 2016) trae una serie de riesgos y peligros asociados que pueden terminar victimizando a los menores de edad. Es un fenómeno que va en aumento y que afecta también a las relaciones familiares, como demuestran las noticias publicadas sobre casos de menores que han denunciado a sus progenitores por la cantidad y el tipo de imágenes que compartían sobre ellos en las redes sociales (circunstancia que se ve potenciada en los casos de separación de los padres).

Por consiguiente, continuando con la reflexión sobre la clasificación de los tipos de cibercrimen, se considera que tiene una dudosa utilidad, desde el punto de vista criminológico, establecer

clasificaciones cerradas sobre las modalidades de cibercrimen, debido principalmente al contexto virtual en el que se desarrolla dicha intención criminal. Al respecto, también habría que sumar a este análisis la irrupción en nuestras vidas del denominado internet de las cosas que puede conllevar el aumento de nuevas amenazas potenciales, tal y como se apunta en el informe sobre Ciberamenazas y Tendencias, de 2019, del Centro Criptológico Nacional (en adelante CCN). Asimismo, determinados autores (YONCK, 2013), ya pronosticaron la posibilidad del primer asesinato en línea a través de Wifi en los dispositivos médicos implantables (IMD) como marcapasos, dispositivos ventriculares y bombas de insulina. Además, también indicaba que los delincuentes podrían utilizar otros dispositivos conectados a la red (como los automóviles sin conductor) dando lugar a nuevos tipos de cibercriminalidad. El CCN, en su referido informe, también recoge dicha posibilidad y apunta la existencia de un incremento progresivo en el desarrollo de dispositivos médicos que se conectan a Internet, los cuales facilitan no solo la labor de los médicos, sino también, la labor de los ciberdelincuentes debido a que estos dispositivos presentan puntos vulnerables a ciberataques, al priorizarse en su fabricación su funcionalidad en detrimento de su seguridad[3].

6.1.3 Análisis de las nuevas formas de criminalidad *online*:

A continuación, se efectúa, en relación a la clasificación del cibercrimen propuesta en este TFG, un breve análisis criminológico de las nuevas formas de criminalidad *online* consignadas en el mismo, al considerarlas más graves desde el punto de vista del resultado lesivo que pueden suponer, concretamente, respecto a la vida y a la integridad física o moral:

- **Ciberacoso;** quizás es la tipología menos novedosa, pero se cree conveniente su análisis al constituirse en una especie de macrocategoria que aglutina todas aquellas conductas dirigidas contra la libertad y la dignidad de la víctima, efectuadas en la Red, por medio de las TIC, con una finalidad que puede ser de índole laboral, sexual o personal. Seguidamente se efectúa un breve repaso de las formas más comunes de ciberacoso, sin un ánimo exhaustivo motivado por las reglas de extensión que limitan este trabajo, las cuales han dado lugar a categorías propias como son;

[3] Varias pruebas en laboratorio, realizadas en los Estados Unidos, han demostrado que una porción de dispositivos médicos (marcapasos, desfibriladores, respiradores, bombas de infusión) son vulnerables a ciberataques sería posible obtener acceso no autorizado y manipular el dispositivo sin el conocimiento del paciente. Por ejemplo, un desfibrilador se pudo controlar y reprogramar de forma remota para liberar electricidad no deseada.

- *El cyberbullying o acoso escolar a menores en internet:* consistente en el acoso psicológico entre iguales por medio del ciberespacio. Existen numerosos estudios relacionados con el *bullying* y el *ciberbullying*, no obstante, se considera necesario distinguir aquellos en los que se analiza la accesibilidad de los menores a las TIC, especialmente al uso diario de la telefonía móvil, y los riesgos asociados al mismo como son las conductas de uso adictivo, y el *cyberbullying* (ARNAIZ, CEREZO, GIMENEZ y MAQUILÓN 2016). En el mismo sentido, existen estudios que relacionan el uso cotidiano de las redes sociales en el ciberespacio y la violencia escolar, cuyos resultados muestran que las adolescentes son más proclives a utilizar de manera abusiva dichas redes, provocando una mayor expresión de conductas violentas en la escuela hacia sus iguales (MARTÍNEZ-FERRER Y MORENO 2017). Reseñar que, desde el punto de vista criminológico, este tipo de estudios cobran un especial valor de cara a poder detectar y prevenir de forma más precoz este tipo de conductas.
- *El cyberstalking,* podría entenderse como el uso de las TIC para acosar, perseguir o amenazar a alguien de forma más o menos continuada, aspecto que diferencia este tipo de conductas en relación al *cyberharassment* (también denominado *online harassment*), que es el término utilizado para referirse a los actos concretos y no continuados de *bullying o stalking* en el ciberespacio. Cabe efectuar una serie de matizaciones respecto a esta categoría de acoso tras establecer un paralelismo con el *stalking*; siguiendo a VILLACAMPA y PUJOLS (2019), se constata la escasa incidencia judicial respecto a las denuncias de las víctimas de *stalking*, a pesar de la inclusión penal de este tipo delictivo tras la reforma operada por la LO 1/2015 (art. 172 ter CP). Los argumentos que constatan este hecho son sobradamente referidos por dichas autoras y no serán reiteradas en este trabajo por las razones, ya mantenidas, relacionadas con las normas de extensión del mismo, pudiendo destacarse, entre otras, la desconfianza de las víctimas respecto a la eficacia de la actuación judicial en este tipo de procedimientos. La reflexión criminológica pretendida en este apartado, por tanto, es referida a que apenas existen estudios empíricos sobre este tipo de acoso offline, entre otros motivos por su escasa incidencia judicial, circunstancia que se agrava en el caso del *cyberstalking,* no solo, respecto a su casuística, sino también, respecto a su prevención.
- *El ciberacoso sexual; el sexting y el online grooming; el sexting* consiste en la realización, por parte de menores de edad, de fotografías propias de desnudos completos o parciales y su envió a otros,

generalmente mediante el teléfono móvil, incluyendo textos obscenos cuyo fin es conocer a otras personas o enviar mensajes de amor y odio. *El online grooming o cybergrooming* es otra forma de ciberacoso sexual pero más grave que la anterior, y consiste en contactar con menores de edad, por medio de las redes sociales, salas de chat, etc. ganándose su confianza para poder acercarse a estos e intentar posteriormente un contacto sexual. Ambas conductas se caracterizan por atentar contra la libertad e indemnidad sexual de menores de edad. Respecto al riesgo y la gravedad que pueden suponer este tipo de conductas es interesante considerar el trabajo empírico efectuado por algunos autores, pudiendo destacarse la investigación de VILLACAMPA Y GÓMEZ (2016, p. 24) que, abogan para la prevención de tales formas de victimización, ante la reducida gravedad de tales conductas, por una mayor actuación en el terreno educativo y formativo de los menores en el uso seguro y responsable de las TIC y una menor actuación penal. En relación al ciberacoso, desde el punto de vista criminológico, debe profundizarse en el estudio de la relación entre el uso de las TIC y como el mismo puede incidir en los perfiles de los sujetos activos y pasivos de este fenómeno. Respecto a la prevención de este fenómeno es necesario ahondar en la cifra negra del ciberacoso para poder conocer su verdadera dimensión; ¿es realmente un problema a escala mundial como se afirma desde hace años?, o ¿se ha generado una alarma infundada en relación al número de casos y a la gravedad de los mismos? Estas y otras cuestiones relacionadas con la cifra negra del cibercrimen se analizarán también más adelante en el presente TFG.

- **Ciberinducción al daño físico**, tiene su origen en las interacciones personales surgidas a través de las redes sociales, y consiste en inducir a determinados usuarios de las mismas, generalmente niños, niñas y adolescentes, a autolesionarse convenciéndoles para que formen parte de determinados juegos online como *"el reto de Momo"*[4], que consiste en cumplir una serie de pruebas algunas de ellas de carácter autolesivo, y que ha provocado, tras extenderse por *Whatsapp*, que desde diferentes cuerpos policiales se advierta del riesgo que puede suponer para los menores de edad. A tal fin, la Policía Nacional de Colombia publicó, en su página oficial, una

[4] Su terrorífica imagen pertenece a la escultura de una mujer-pájaro que se expuso en 2016 en una galería de arte alternativo en Ginza (Tokio). Su imagen se ha hecho famosa a través de WhatsApp en forma de reto viral. Pero las autoridades advierten de que podría tratarse de algo mucho más serio que un juego online

serie de recomendaciones para prevenir la ciberinducción al daño físico en niñas, niños y adolescentes, y para evitar riesgos y navegar seguros en Internet. El CNP y la GC también han informado en sus cuentas de Twitter, respectivamente, sobre el peligro de la reaparición de este juego en vídeos de *Peppa Pig y Fortnite en YouTube* y acerca de no aceptar los desafíos del juego *"Momo Challenge"*.

- **Retos virales que atentan contra la vida, contra la integridad física, y moral**: en este apartado se refleja una breve muestra de los retos virales que se han popularizado mediante las redes sociales, concretamente aquellos que pueden suponer un riesgo mayor para las personas en general y para los menores en particular. La intencionalidad de este tipo de conductas online se fundamenta en varias razones; desafiar a la autoridad, el desafío de los limites personales, por diversión, curiosidad etc., no obstante, cuando estas conductas se comparten en las redes sociales todas confluyen en un mismo fin; lograr popularidad social con un desmedido afán de protagonismo. Esta razón puede explicar porque muchos de los videos son protagonizados por menores de edad, que se encuentran en plena fase de su desarrollo personal y social, los cuales sienten muchas veces la necesidad de destacar socialmente para ser aceptados, en ocasiones, a cualquier precio. Los videos subidos a las redes sociales demuestran como sus protagonistas no dudan en poner en riesgo, no solo, su vida, su integridad física y su integridad moral, sino también, la de los demás. Seguidamente se analizan de forma breve algunos de los retos virales más mediáticos:
  - *Rompe cráneos*: se realiza entre tres personas, generalmente adolescentes, y consiste en saltar al mismo tiempo y los dos situados en los extremos golpean con sus pies los pies del que se encuentra situado en medio cuando están todos en el aire, para que caiga hacia atrás, logrando que se golpee la parte trasera del cráneo, de ahí el nombre de “rompe cráneos” o “cráneo roto”. Esta peligrosa conducta ha llevado a varios jóvenes a subir videos a redes sociales y a la aplicación *Tik Tok* mostrando las caídas de las que son objeto, en las que se pueden producir lesiones graves en el cuello e incluso la muerte.
  - *El rompebocas*; es uno de los últimos retos virales que se han popularizado, también a través de *Tik Tok*, el cual consiste en pasarle a la víctima una bufanda o prenda similar alrededor de los tobillos para hacerle perder el equilibrio al tirar fuertemente de la misma. Normalmente,

la víctima, que no se lo espera, cae de frente y suele sufrir algún traumatismo importante en la cara y en la boca, de ahí su nombre.

- *Tide Pod Challenge*; El reto surgió tras aparecer un anuncio de la marca de detergente estadounidense *Tide* donde un hombre simulaba comerse una cápsula de detergente. El reto saltó de la pequeña pantalla a la realidad y los videos de usuarios comiendo detergente comenzaron a dejarse ver en internet, produciéndose numerosas intoxicaciones. Otros retos similares que provocan un peligro grave para la salud, debido a las intoxicaciones que pueden provocar, son el *reto de canela* y el reto denominado *Shell on*; que consiste en comer huevos con cáscara, fruta sin pelar y hasta envases de plástico.
- *El desafío*; consiste en que un menor desaparece voluntariamente entre 48 y 72 horas, sin poder responder al móvil, ni a las llamadas ni a mensajes de *WhatsApp* o similares. Debe aislarse de todo tipo de comunicación con sus contactos y tampoco puede publicar nada en las redes sociales ni alertar a nadie de dónde se encuentra. Gana el que más entradas tiene en sus cuentas de Instagram, *Facebook o Twitter* preguntando sobre su paradero. Cada mensaje en redes sociales relacionado con la desaparición del autor del desafío suma puntos y reputación en el mundo virtual. Tras finalizar el reto el menor aparece como si no hubiera pasado nada.
- *Outlet Challenge* (o el reto del enchufe); este reto viral consiste en enchufar un cargador del móvil o similar y colocar una moneda en el espacio que queda entre este y el enchufe de la pared, lo que provoca desde un chispazo hasta un cortocircuito o, en el peor de los casos, un incendio. Se ha vuelto viral en Estados Unidos a través de Tik Tok y está protagonizado principalmente por adolescentes.
- *Cha Cha Slide*; entre los retos virales más absurdos y peligrosos, sin duda, se encuentran aquellos que ponen en riesgo la seguridad vial. El *Cha Cha Slide* es una canción del cantante *MR C The Slide* y el reto consiste en que el conductor siga el estribillo de la canción haciendo maniobras de forma súbita, en zigzag, de derecha a izquierda, con el peligro evidente que ello conlleva para el resto de usuarios de la via. Las maniobras son grabadas y subidas a TikTok. En línea con lo anterior, en su día la DGT, se vio obligada a alertar del riesgo del reto conocido con el nombre de la canción *In my feelings* interpretada por el cantante *Drake*.

Consistía en salir de un coche en marcha cantando y bailando esta canción, mientras el coche seguía avanzando sin conductor, para volver a subir también en marcha.

- La lista de retos virales empieza a ser incontable, muchos de los mismos no tienen un componente criminógeno al ser conductas de riesgo efectuadas de forma individual en las que el protagonista en principio solo se pone en riesgo a sí mismo. El problema surge cuando sube su reto a la Red y se produce un efecto imitativo, sobre todo entre los menores de edad. Entre las conductas que han causado lesiones y situaciones graves para la salud podríamos citar de forma concisa; el *ice bucket challenge,* que comenzó siendo una campaña social que buscaba concienciar sobre la Esclerosis Lateral Amiotrófica (ELA), pero enseguida se hizo viral, la cual consistía en lanzarse cubos de agua helada sobre la cabeza (hay personas que sufrieron problemas de salud por el choque térmico); derivado de este, también se popularizó el *hot water challenge*, en el que la gente se tiraba agua hirviendo por encima o la bebía (hubo personas que llegaron a sufrir quemaduras muy graves); el ice and *salt challenge*, en el que se buscaba la reacción química de la sal sobre el cuerpo tras aplicarle hielo y que posteriormente sus autores subían a las redes sociales (muchas personas han sufrido quemaduras importantes); el *condom challenge*, derivado de la broma del globo de agua, consiste en lanzar sobre la cabeza de algún incauto un preservativo lleno de agua. Al no romperse, la cabeza queda atrapada dentro del condón como si alguien colocara una bolsa de plástico cerrada con el consiguiente riesgo de asfixia.

  Los retos online referidos son una minúscula muestra de los existentes en la Red, no obstante, es necesario indicar que desde el punto de vista criminológico nos interesarían solamente aquellos que derivan en conductas delictivas (con resultado de muerte, lesiones, daños, peligro para la seguridad vial, etc.)

- **La práctica del *happy slapping*** (bofetada feliz). La ONG *Save the children* alerta sobre este fenómeno que apareció por primera vez en Reino Unido en 2005. Consiste en una agresión personal (física, verbal o incluso de índole sexual) que puede ser planificada u ocasional, en la cual participan al menos dos autores, un agresor y la persona que graba la agresión. Se efectúa con el objetivo de lograr popularidad a través de los *likes* (en ocasiones puede hacerse viral, generalmente por las redes sociales y el canal Youtube). Este tipo de comportamiento criminal

tiene como finalidad lograr la obtención de éxito social, una distinción popular a cualquier precio, incluso dañando o humillando a otra persona.

Este tipo de fenómenos está provocando que los responsables de las redes sociales más importantes en Internet, como Facebook, Instagram o Twitter, estén considerando la supresión de los *Likes* en aras a mejorar el bienestar de sus usuarios. Desde la perspectiva criminológica sería conveniente saber cómo puede afectar dicha medida en la incidencia delictiva derivada del comportamiento online, si finalmente se suprime esta función de las redes sociales, especialmente respecto a los menores de edad y los adolescentes.

- **Ciberinducción al suicidio o cibersuicidio,** la Red es capaz de propiciar tipos delictivos sobre los que creíamos que su realización solo podía llevarse a cabo en el espacio físico. No obstante, la virtualidad que ofrece internet permite al sujeto activo trasladar su intención delictiva al mundo real aumentando, por tanto, su capacidad de acción al reducir el riesgo para poder ser detenido durante la misma. Este incremento de la capacidad criminal que ofrecen las TIC, permite que la inducción al suicidio pueda ser online. El medio comisivo de este tipo de conductas se efectúa, principalmente, a través de páginas web y determinados juegos online como la "Ballena Azul" (en España el caso más reciente fue el de una niña guipuzcoana que en 2018 se quitó la vida tras jugar al mismo). Cabe reseñar que las víctimas suelen ser adolescentes, existiendo también casos en niñas de corta edad (Ursulla Keogh de 11 años, Molly Russell de 14 años, Noa Pothoven de 17 años, etc.).

  Desde el punto de vista preventivo resulta necesario investigar estas conductas mediante el análisis científico de esta nueva forma de inducción al suicidio, de lo contrario seguiremos encontrándonos con la actualización permanente del denominado "efecto Werther"[5], el cual podrá verse potenciado, además, por la capacidad de difusión que tienen las TIC (sirva como ejemplo; el caso reciente de la serie "13 razones" que provocó un aumento de suicidios reseñable entre los adolescentes de Estados Unidos).

[5] Es un fenómeno surgido a partir de la novela de Goethe (Las penas del joven Werther) donde el protagonista sufre por amor hasta el punto que acaba por quitarse la vida y que causó en su época, tras su publicación en 1774, una epidemia de suicidios.

- **Cibertráfico de drogas o tráfico de drogas online**; Otro capítulo que merece un análisis criminológico riguroso, debido a la problemática que constituye a todos los niveles (personal, familiar, social y económico), es el referido al auge de las nuevas drogas y su introducción entre los jóvenes a través de Internet. La ONU en su Informe Mundial sobre Drogas de 2018 determina que se han alcanzado niveles sin precedentes de producción de drogas de origen vegetal (como, por ejemplo, el *Kratom*).

  Este problema se intensifica no solo por la facilidad que brinda la red respecto al tráfico de estas sustancias[6], especialmente la Darknet, sino también, por el hecho de que algunas de estas drogas son legales en los países de procedencia de este tipo de sustancias e ilegales en nuestro país. Al respecto también cabe indicar que se está produciendo un aumento alarmante del tráfico online de medicamentos sujetos a prescripción médica (con fines no médicos). Los profesionales sanitarios afirman desconocer el número total de variedades distintas de sustancias que están introduciéndose en España por medio de este tipo de tráfico online, cuya persecución es muy complicada desde el punto de vista policial y sanitario. Se puede afirmar que los consumidores de drogas y medicamentos, nunca han tenido a su alcance tal variedad de sustancias con la facilidad, celeridad y falta de riesgo que les otorga el ciberespacio en la actualidad.
- **Juego ilegal online:** el acceso a sitios online de juego ilegal es un fenómeno que también merece un estudio criminológico amplio para tratar de explicar las razones de su permanente expansión y la falta de datos existentes respecto a sus efectos nocivos; tanto para la salud (debido a la peligrosa adicción que provoca), como a nivel económico (por la afectación que supone en la economía del jugador y de su entorno familiar). La DGOJ, dependiente del Ministerio de Hacienda, advierte sobre los peligros del juego online ilegal en relación; al patrimonio, los datos personales, o la posibilidad de sufrir fraude, engaño o prácticas deshonestas, e incluso colaborar con organizaciones criminales. Este fenómeno se agrava especialmente entre los menores de edad que reciben a través de la TIC una oferta publicitaria masiva de juego online. Al respecto

[6] En el Informe Mundial de Drogas (UNODOC 2018: crisis de opioides, abuso de medicamentos y niveles récord de opio y cocaína. UNODOC, 2018. se indica que, en julio de 2017, las fuerzas del orden de varios países llevaron a cabo una operación conjunta para desmantelar la mayor plataforma de venta de drogas en la red oscura. Antes de su cierre, AlphaBay contenía más de 250.000 listados de drogas y sustancias químicas ilícitas y a lo largo de su existencia contó con más de 200.000 usuarios y 40.000 vendedores.

cabe matizar que la ilegalidad viene determinada por el hecho de tratarse de menores de edad, aunque la oferta en estos casos proceda principalmente de operadores de juego legales. Puede afirmarse que, si están fallando los controles en el espacio físico, en el espacio virtual podemos hablar directamente de "descontrol", en relación a este fenómeno, especialmente en algunos países como Alemania (favorecido por el efecto multiplicador que tiene internet).

6.2 Cibervíctima:

En este apartado, tal y como anticipamos al inicio, se efectúa un breve análisis criminológico de la víctima al objeto de reflejar la importancia y el protagonismo que adquiere en el evento cibercrimen. Asimismo, se efectúa el estudio de los perfiles de victimización y de la dimensión real de la amenaza que supone este fenómeno en el que se incluirá también el análisis de la cifra negra del cibercrimen.

En relación al estudio de la Cibervíctima existen dos características fundamentales a la hora de poder efectuar la prevención del cibercrimen; la primera, viene determinada por el ciberespacio, que representa un nuevo ámbito de oportunidad delictiva; la segunda, viene determinada por las interacciones personales surgidas en el mundo virtual. Ambas características tienen una repercusión directa y distinta respecto al crimen producido en el mundo físico, debido a la carga de responsabilidad y al protagonismo de los sujetos participantes, las cuales ya no recaen solo en la voluntad del agresor, sino que depende del tipo de actuación que decida tener la víctima en la Red.

6.2.1 La importancia de la víctima en el evento cibercrimen:

Hasta la consolidación de la Victimología como disciplina científica, el estudio de la víctima ha sido despreciado desde todos los ámbitos, incluido el de la criminología, que tradicionalmente, desde su origen positivista, había centrado el estudio del comportamiento criminal entorno a la persona del infractor (GARCÍA-PABLOS, 2009). Desde entonces el estudio de la víctima ha seguido teniendo un interés creciente que debería verse incrementado, aún más, como consecuencia del protagonismo que ha adquirido la víctima respecto al cibercrimen.

Entre los estudios criminológicos que han tratado de abordar la cibercriminalidad probablemente la corriente teórica que ha tenido mayor consideración es la Teoría de las Actividades Cotidianas (COHEN y FELSON, 1979). A partir de los enfoques criminológicos de la oportunidad, y especialmente de los presupuestos de la TAC, se analiza el ciberespacio como un nuevo ámbito de oportunidad criminal y se plantea si el mismo supone la necesidad de modificar las estrategias

preventivas pensadas para el delito offline. Por esta razón, principalmente, se considera que la TAC puede servir para revelar la importancia de la víctima en el delito online, porque la interdependencia espacio temporal de los delitos y las actividades humanas planteadas en la misma sigue existiendo, al igual que existe en los delitos offline, con un matiz diferenciador claro; la relación espacio-temporal se modifica en el cibercrimen y las actividades humanas que se efectúan a diario en este nuevo contexto también. Ello es debido a que será la víctima con su elección, a la hora de interactuar en el ciberespacio, la que marcará o no las posibilidades de convertirse en cibervíctima.

Al respecto, cabe destacar el enfoque criminológico (MIRÓ, 2012), en el cual efectúa la reformulación de la TAC para ajustar sus postulados al nuevo ámbito criminal surgido en el ciberespacio y que sirve para ilustrar el protagonismo que adquiere la víctima durante el cibercrimen, en el cual podemos señalar tres factores coadyuvantes; el primero tiene que ver con el nivel de riesgo que asume la victima potencial y que dependerá de los bienes que esta decida incorporar al ciberespacio (su intimidad, imagen, patrimonio, etc.); el segundo factor es el referido a la interacción de la víctima en el ciberespacio que marcará las posibilidades de éxito del agresor motivado; el tercero viene determinado por el nivel de autoprotección de la víctima al incorporar, o no, sistemas digitales de protección.

Este nuevo enfoque victimológico y multifactorial cobra un sentido especial frente a una delincuencia cuya topografía se encuentra en permanente cambio (CANO 2018). En línea con lo anterior, se efectúa un nuevo planteamiento en relación a la prevención de la ciberdelincuencia basado en el control social informal, tras comprobarse la falta de eficacia de las formas de control social formal en relación al cibercrimen, debido entre otras razones al carácter transnacional y anonimizado del ciberespacio, que sin duda limita la eficacia de la acción preventiva que trata de ejercerse a nivel institucional por medio de los cuerpos policiales y el sistema judicial y penal.

Un ejemplo que valida el planteamiento anterior, basado en el control informal, lo podemos encontrar en la *vigilancia natural de internet*. Si analizamos brevemente el caso de *Luka Rocco Magnota, aunque su verdadero nombre es Eric Clinton Kirk Newman, conocido como el "descuartizador de Montreal" o "el asesino de la generación Facebook"* podemos comprobar, de una forma empírica, el grado de eficacia que puede tener el control informal de internet, (en este caso posibilitó la captura de este asesino y su posterior condena a cadena perpetua). En 2010, este criminal subió un vídeo en internet matando a 2 gatitos, a los que ahogo en una bolsa de vacío con

un aspirador. El vídeo pronto se convirtió en viral y varios usuarios de Internet decidieron crear un grupo en *Facebook* para intentar localizar al protagonista del video y poder desvelar su identidad[7]. El documental de Netflix titulado; "No te metas con los gatos; cazar a un asesino en Internet (traducido del título original; Dont Fuck With Cats: Hunting An Internet Killer) retrata el periplo de este asesino que actuó para lograr notoriedad a través de las redes sociales (obsesionado con la repercusión y la fama). Este caso tuvo una trascendencia enorme en la Red con miles de seguidores en todo el mundo, unidos en una especie de caza común al asesino, y ha servido para escenificar los múltiples y variados roles que se generan cuando interaccionamos, a través de las redes sociales, con otras personas a las que ni siquiera llegamos a conocer. Además, también ha servido para demostrar que, paradójicamente, la vigilancia natural de internet puede resultar más eficaz que la vigilancia institucional derivada del control social formal que trata de ejercerse en el espacio virtual, circunstancia que resulta importante, desde el punto de vista preventivo, respecto al estudio de la victimología *online*.

6.2.2 Análisis criminológico de los perfiles de victimización;

Para poder efectuar un análisis criminológico del perfil de la cibervíctima tomaremos nuevamente como punto de partida la TAC, para poder valorar como las actividades cotidianas de la víctima en la Red y su interacción con otros usuarios de la misma, ciertamente, delimitarán las posibilidades de sufrir un ataque online.

Si admitimos la premisa de que el ciberespacio alberga la posibilidad de ampliar la oportunidad criminal, podemos afirmar que el mundo virtual amplía la oportunidad victimal (entendida como la posibilidad de convertirse en cibervíctima), por tanto, podemos concluir que no puede existir un único perfil de cibervíctima, porque cualquier internauta que tenga acceso a la Red podrá convertirse en cibervíctima o en cibercriminal, es decir, habrá tantos perfiles victimológicos como ámbitos de oportunidad criminal surjan en el ciberespacio (MIRO, 2012).

Por consiguiente, el estudio tradicional de la criminología, que se ha centrado sobre el agresor, ahora debe focalizarse con mayor intensidad en la víctima, y de forma especial en la cibervictimización de los jóvenes sobre la cual apenas existen estudios criminológicos[8]. La conducta

[7] Posteriormente asesinó al estudiante chino Lin Jun y grabó el crimen en un vídeo que colgó en Internet.

[8] Destacar el Estudio Nacional Sobre Cibercriminalidad en España del Centro Crimina de la Universidad 'Miguel Hernández' de Elche, en Alicante, de 2018.

de los más jóvenes aumenta el riesgo de convertirse en cibervíctimas, de un modo especial, debido a que contribuyen con sus actividades cotidianas a incrementar el riesgo de sufrir algún ciberataque, cuando navegan por internet o hacen uso de las TIC, por ejemplo, al enviar información personal a personas que no conocen a través de; las redes sociales, la mensajería instantánea, los juegos online, foros, videoblogs, canal de You Tube, correo electrónico, etc. Cabe matizar al respecto que, no solo, son víctimas potenciales de sufrir un ciberataque los usuarios "particulares", sino también, las empresas y los organismos e instituciones debido a que, en definitiva, su funcionamiento depende del factor humano.

Otro aspecto importante que, sin duda, también determinará la posibilidad de convertirse en una cibervíctima, tiene que ver con la adopción o no de las medidas de autoprotección que se adopten al utilizar las TIC (por ejemplo, programas antivirus, cortafuegos, etc.). El ciberespacio es un ámbito de comunicación paralelo al espacio físico, pero en el que los objetos, bienes y acciones tienen que ser introducidos en él. Mientras que en el espacio físico se está, en el ciberespacio se puede estar o no. Y lo mismo sucede con los derechos relativos a la intimidad, el patrimonio, el honor etc.

No obstante, cabe reseñar, que la decisión de acceder o de introducirse en el ciberespacio no siempre es voluntaria, es decir, en muchas ocasiones serán las acciones de terceros o acciones involuntarias nuestras, las que conllevarán la introducción de nuestra imagen, de nuestra privacidad, etc. (como ya anunciamos al hablar del *sharenting*). Por todo lo anterior, podemos afirmar que el primer elemento de la victimización en el ciberespacio guarda relación directa con los bienes y derechos que introducimos, de forma consciente o inconsciente, en Internet.

6.2.3 Análisis criminológico de la dimensión real del cibercrimen:

En línea con el análisis anterior referente a los factores de riesgo de victimización del cibercrimen en relación a las actividades cotidianas se efectúa seguidamente el análisis criminológico sobre la dimensión real del cibercrimen. A tal fin se analizarán los factores que pueden influir en la percepción de la amenaza online, además se efectuará un análisis sobre las posibles causas de la cifra negra del cibercrimen y finalmente se abordaran las posibles repercusiones que a nivel preventivo pueden influir en ambos aspectos.

A) Factores que intervienen en la percepción de la amenaza:

El uso masivo de las TIC, tal y como se puede constatar en el Informe del SEC de 2018, con los datos estadísticos del INE sobre la Sociedad de la Información indican una tendencia alcista

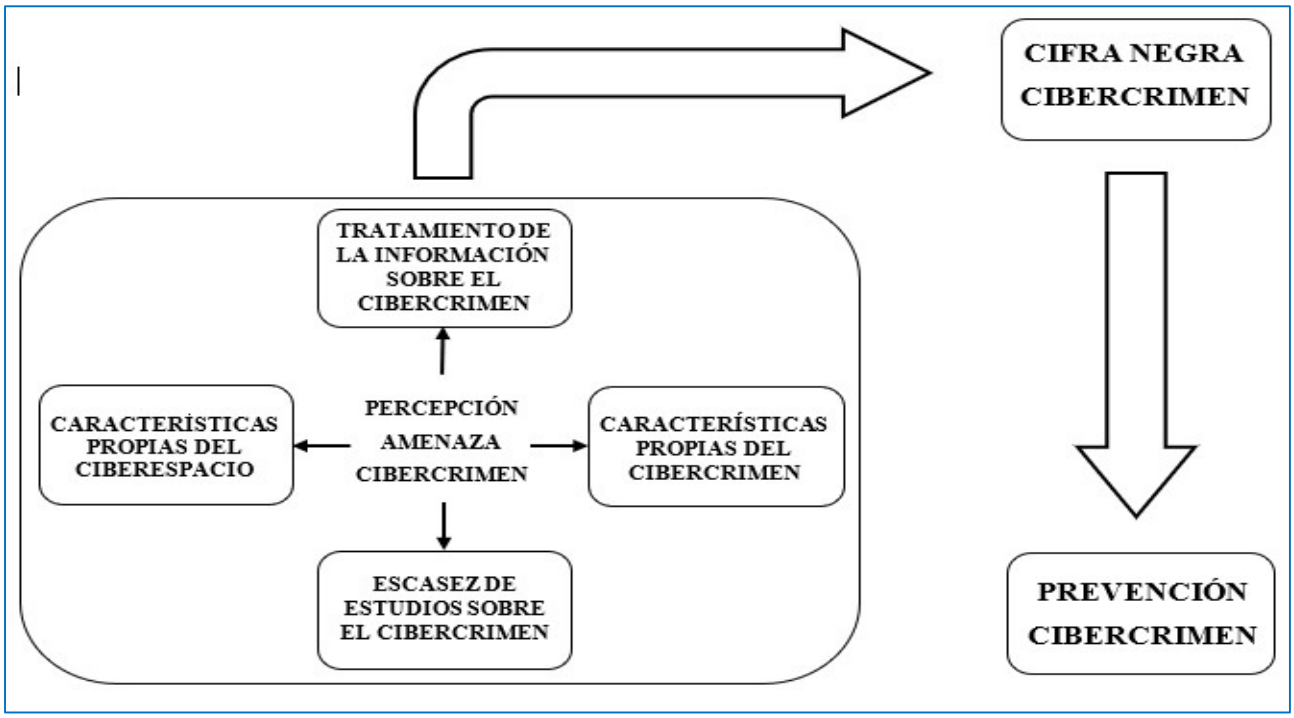
constante, desde el año 2009, en relación al porcentaje de viviendas en España con acceso a Internet. Dicha tendencia probablemente conducirá a que en los próximos años se alcance, prácticamente, la cifra del cien por cien de las viviendas con acceso a la Red. El informe también refleja una tendencia alcista del uso de Internet (sin diferencias significativas respecto a la edad o el sexo), que se ha ido incrementando permanentemente durante los últimos diez años, no solo a nivel particular, también a nivel institucional y empresarial.

A la vista de los datos referidos se podría deducir que no se percibe el ciberespacio como una amenaza dado el elevado porcentaje de la población que utiliza Internet. Sin embargo, si recurrimos al Informe de ONTSI de 2018, (Estudio sobre la Ciberseguridad y Confianza en los Hogares Españoles), podría deducirse que dicha percepción sobre la amenaza online está presente entre los internautas, con base en los datos siguientes:

- Tres de cada cinco internautas consideran que el número de incidencias de seguridad acontecidas durante los últimos 3 meses y la gravedad de las mismas se ha mantenido en similares proporciones con respecto a las observadas en los meses anteriores (61% y 62,8% respectivamente).
- Las incidencias de seguridad son referidas a; daños en los componentes del ordenador (hardware) o en los programas que utilizan (software); perjuicio económico (debido al fraude online en compras, cuentas y tarjetas bancarias); la privacidad: robo o uso de información de carácter personal sin consentimiento de su titular (fotografías, nombre, dirección).
- Se observa un incremento en la valoración de los peligros de Internet como la cesión voluntaria de datos personales (78,1%) y en la cesión de información sobre hábitos, tendencias y usos de Internet (66,9%).
- Se reafirma la alta preocupación sobre el acceso, compartición, pérdida o robo de archivos personales (83,3%) y por las infecciones de malware (85,6%).
- Casi la mitad (49,7%) de los internautas son conscientes de que cada acción llevada a cabo online tiene repercusiones sobre la ciberseguridad y también perciben que la propagación de amenazas se debe a la poca cautela de los propios usuarios (68,8%).

A los factores reseñados que inciden en la percepción de la amenaza podríamos añadir otra serie de factores que sumados a los anteriores pueden estar condicionando no solo la cifra negra del

cibercrimen, sino también y como consecuencia de esta, la prevención de dicha amenaza online, los cuales se plasman en el esquema siguiente:



Esquema de elaboración propia que analiza los factores que intervienen en la percepción del cibercrimen.

La percepción de cualquier amenaza incide en nuestro comportamiento y en nuestros hábitos, de forma que cuanto mayor sea la intensidad con la que percibimos la misma aumentaremos, en similar proporción, las medidas de seguridad y viceversa. Al analizar la percepción de la amenaza en el ciberespacio podemos afirmar que en general se "rebaja el nivel de alerta" en comparación a la amenaza física. Esta diferencia en la percepción de la amenaza online se encuentra condicionada por los factores siguientes (GIL, 2015);

- Las características propias del ciberespacio; transnacional, deslocalizado, universalizado, neutro, anonimizado, en constante cambio, no centralizado distribuido.
- Las características propias del cibercrimen; concretamente la inmaterialidad, la facilidad comisiva y la atipicidad, características cuyo análisis, se efectúa más adelante en profundidad (en otro apartado).
- El tratamiento que efectúan los medios de información en relación al cibercrimen, que en muchas ocasiones tiene un carácter sensacionalista que genera cierta alarma social, que luego no se justifica con la gravedad del mismo (si, por ejemplo, hacemos una búsqueda en

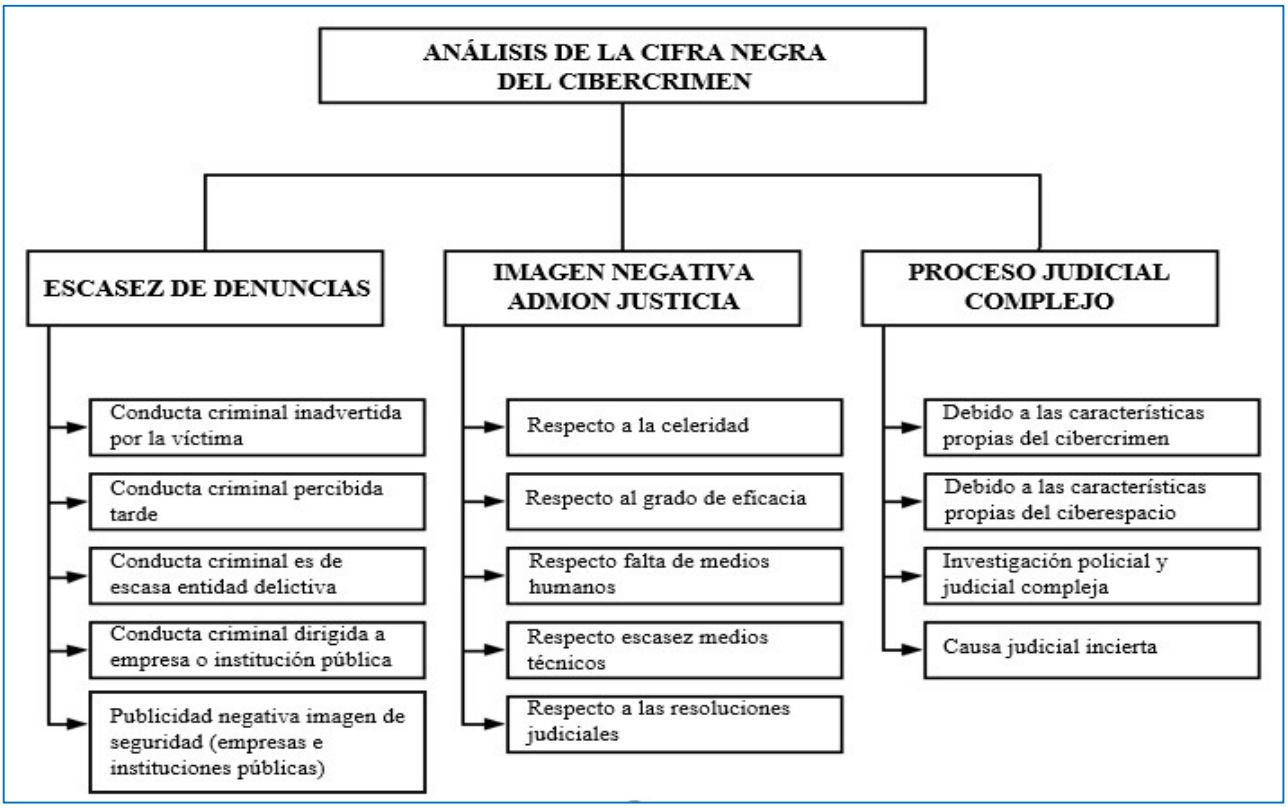
internet bajo el título; noticias sobre ataques informáticos, se puede corroborar esta afirmación).

- La falta de estudios empíricos sobre este fenómeno; es una lamentable realidad que la criminología no haya aportado, desde su saber científico y multidisciplinar, más investigaciones sobre la cibercriminalidad para explicar este fenómeno, que empieza a no ser tan nuevo.

La conjunción de los factores analizados da como resultado que la percepción de la amenaza respecto al cibercrimen se encuentre un tanto distorsionada. Esta cuestión tiene una importancia fundamental, desde el punto de vista criminológico, porque estamos anticipando en muchas ocasiones un juicio subjetivo del problema, dando como resultado que el cibercrimen sea percibido, en unas ocasiones, como una amenaza cercana y en otras como una amenaza lejana. Resulta necesario establecer, con mayor objetividad, las dimensiones reales respecto a este tipo de amenaza o, de lo contrario, la cifra negra del cibercrimen continuará situándose fuera del alcance de cualquier tipo de estimación valida y en consecuencia seguirá afectando negativamente a su prevención. En el mismo sentido se pronuncian diversos autores (MONTIEL, 2016) haciendo especial hincapié respecto a los estudios de cibervictimización y ciberdelincuencia juvenil y a la importancia de cuantificar la magnitud real del problema desde el punto de vista criminológico y victimológico.

B) La cifra negra del cibercrimen**:** en la memoria de la FGE (2019) se efectúa el análisis de las diligencias de investigación y procedimientos judiciales, incoados por el Ministerio Fiscal en 2018, enfatizándose la importancia de evitar la dispersión de información relacionada con la actividad criminal en el ciberespacio. Hay diversos autores (ROBLES, 2015), que también recalcan esta cuestión estableciendo el paralelismo con un “iceberg”, para referirse a las estadísticas oficiales y a la cuantificación de los datos relacionados con la cibercriminalidad, indicando que solo nos permiten visualizar una pequeña parte del problema en comparación a lo que existe debajo de la superficie.

En el esquema siguiente se refleja un análisis sobre las posibles causas de la cifra negra del cibercrimen, las cuales en conjunto contribuyen a que se considere como la forma de delincuencia más infradenunciada de toda la existente:



Esquema de elaboración propia sobre la cifra negra del cibercrimen

La escasez de denuncias en relación al cibercrimen viene motivada por varias razones, algunas de las cuales se tratarán de analizar en este apartado, sin embargo, cabe resaltar nuevamente la necesidad de realizar investigaciones empíricas basadas en estudios cuantitativos y cualitativos que ayuden a arrojar luz sobre dicha cifra oculta.

Entre las razones reflejadas en el esquema anterior, respecto a la escasez de denuncias, la imagen negativa de la administración de justicia, y un proceso judicial complejo, el CIS (barómetro, julio 2019) arroja una serie de datos que indican como *dicha percepción de las victimas cambia en relación a los delitos online*, por ejemplo, ante la pregunta; ¿Ha sido Ud. víctima de algún delito durante los últimos diez años? el 16,7% responde afirmativamente y el 83,1% responde de forma negativa. Cuando se pregunta nuevamente, a las mismas personas que han contestado de forma afirmativa, que tipo de delitos han sufrido; la mayoría responde el robo de algún objeto, el resto responde; estafa el 4,7 %, amenazas el 12,3%, el 0,2% acoso sexual y el 0,2% acoso psicológico (se han elegido estos por ser tipos delictivos que pueden cometerse de forma online, aunque la encuesta no hace la distinción entre unos y otros). Estas cifras indican, de alguna forma, que la percepción del cibercrimen no tiene la trascendencia ciudadana que podía deducirse en relación al crimen

tradicional (*offline*), sin embargo, existen otros datos, que parecen entrar en contradicción a los aportados por el CIS, nos referimos al estudio ONTSI (2018), ya citado, en el que prácticamente dos tercios de los internautas (65,7%) declaran haberse visto expuestos a alguna situación de fraude (durante los meses comprendidos entre enero y junio de 2018).

Análogamente, también debe analizarse como puede influir la imagen de la justicia en la decisión de la víctima a la hora de interponer denuncia por este tipo de delitos online. De igual forma, el CIS arroja una serie de datos, por ejemplo; respecto a la consideración sobre el funcionamiento actual de la Administración de Justicia en España: el 21,4 % opina que es regular, el 24,1% considera que es malo y el 30,9% opina que es muy malo. Si dicha opinión se solicita a los ciudadanos en comparación con hace unos años, la gente considera; que el funcionamiento es igual en el 54% y peor en el 17,5%. Si se solicita la opinión ciudadana respecto a los medios con los que cuentan los tribunales de Justicia, el 61,0% de los encuestados considera que son más bien insuficientes. A dicha corriente crítica se suman las numerosas voces que desde el seno de los profesionales que integran la Administración de Justicia, han surgido durante los últimos años, y que atribuyen un menor grado de eficacia en su funcionamiento debido a la falta de medios humanos y materiales (VAZQUEZ Y GUTIERREZ, 2017).

Por último, respecto a la complejidad de este tipo de procesos judiciales incoados contra el cibercrimen, viene determinada, principalmente, por las propias características del ciberespacio y del cibercrimen ya citadas en este trabajo lo que provoca, por un lado, que las investigaciones policiales sean complejas, a lo que habría que sumar la escasez de medios y recursos de la Unidades de Policía Judicial[9] , y, por otro lado, un aumento de la dificultad para poder encausar judicialmente a los autores de los cibercrímenes, dando como resultado en muchas ocasiones el archivo de las actuaciones y por tanto que la ley no se logre aplicar en este tipo de delitos. Paralelamente, se considera necesario efectuar un análisis pormenorizado, en relación a la escasez de denuncias por

[9] En la memoria 2019 de la FGE, se indica respecto a la iniciación de oficio de muchos de los procedimientos sobre pornografía infantil que suele tener como punto de partida el hallazgo u obtención de información sobre direcciones IP que su eficacia se ve afectada negativamente por las importantes carencias en medios personales y materiales de los laboratorios de Policía Científica y Criminalística que están determinando preocupantes retrasos en la emisión de informes periciales cuya incidencia, que alcanza a una pluralidad de tipologías delictivas, repercute especialmente en la tramitación de procedimientos por hechos ilícitos de esta naturaleza.

parte de las empresas y su conocida resistencia a denunciar dichas agresiones informáticas[10] con la finalidad de evitar las consecuencias reputacionales que de ello se pudieran derivar.

Podemos concluir, por tanto, en relación a la cifra negra del cibercrimen que el grado de incertidumbre y la reducida percepción de expectativas en la ciudadanía sobre el resultado de este tipo de causas judiciales pueden ser un motivo importante para que la víctima se plantee finalmente no interponer denuncia por este tipo de infracciones penales (a la hora de abordar este fenómeno quizás cobre más sentido que nunca la frase; "la Administración de Justicia no solo debe funcionar bien, sino que además debe parecerlo").

C) Repercusiones sobre su prevención:

La frecuente aparición de noticias relacionadas con el cibercrimen, en toda clase de medios de comunicación, evidencian la importancia que tiene, tanto a nivel particular como a nivel institucional, efectuar una correcta valoración y concienciación específica respecto a los peligros y riesgos de Internet. Sirva como ejemplo; la estafa a la EMT de Valencia, que se realizó entre el 3 y el 20 de septiembre de 2019, por un importe total de 4.040.898,22€ y que evidencia como la falta de concienciación en materia de ciberseguridad, de una directiva de la empresa, resulto clave para la culminación de la estafa. Por ello resulta clave que el usuario de internet sepa, no solo, como detectar las amenazas online, sino también, como adoptar las medidas y precauciones necesarias cuando estas se constaten, tanto para evitar que los riesgos de la Red se materialicen como para evitar su propagación por la misma, bien sea de forma consciente o inconsciente. Al respecto, diversos autores señalan la importancia que tiene la toma de concienciación para la detección de dichas amenazas, así en los casos de *cybergrooming* si la victima sabe distinguir si está siendo manipulada podría neutralizar el impacto de los principios de persuasión de su posible agresor y evitar el desarrollo de un vínculo emocional con el mismo. (SANTISTEBAN, ALMENDROS Y GÁMEZ-GUADIX, 2018).

[10] Desde la FGE se indica la importancia de mejorar la capacidad de actuación penal frente a estas graves conductas que ponen en riesgo la seguridad de los sistemas y, por ende, el normal funcionamiento de las empresas, organismos e instituciones. También indica la necesidad de establecer, en desarrollo del Real Decreto-ley 12/2018 que incorpora a nuestra legislación la Directiva NIS, un sistema ágil y eficaz que facilite la transmisión de información sobre incidentes de ciberseguridad de naturaleza delictiva a los órganos y autoridades responsables de la persecución, enjuiciamiento y sanción de dichas conductas.)

Asimismo, otros factores que influirían negativamente en la prevención del cibercrimen, relacionados con su adecuada percepción, se reflejan en el estudio sobre la seguridad de la información y la e-confianza de los hogares españoles (ONTSI, 2018), concretamente; la existencia de una brecha entre la percepción del internauta, la realidad de sus equipos, y sobre la adopción consciente de conductas de riesgo estaba presente, aproximadamente, en el 43% de internautas; el 49,7% eran conscientes de que cada acción online tenía repercusiones sobre la ciberseguridad y afirmaban que la propagación de amenazas se debía a la poca cautela de los propios usuarios (68,8%); respecto a la realidad de sus equipos el dato más destacable es el de aquellos usuarios que declararon no haber sufrido incidencias de seguridad relacionadas con algún tipo de malware y sin embargo al analizarse sus equipos el 59,6% de los ordenadores y el 18,9% de los dispositivos Android mostraban estar comprometidos por software malicioso.

Por consiguiente, podemos afirmar que si en el espacio físico la percepción adecuada sobre el riesgo a sufrir cualquier delito hace que aumentemos la precaución a la hora de comportarnos de conformidad al contexto en el que nos encontremos, esta aseveración no es válida del mismo modo para los delitos online que para los delitos offline, porque, como acabamos de comprobar la percepción en el mundo virtual se modifica y repercute negativamente sobre la adopción de las posibles medidas de seguridad.

Esta distorsión respecto a la apreciación de la amenaza online también puede deberse a que 9 de cada 10 usuarios de Internet españoles tienen instalado un antivirus, y 8 de cada 10 tiene actualizado el sistema operativo de su equipo, como se recoge en el estudio referido, medidas que son importantes, desde el punto de vista preventivo, pero que no son suficientes, dado que pueden generar una falsa sensación de seguridad que evite que se adopten simultáneamente otras medidas preventivas.

6.3 El Cibercriminal:

En relación al perfil del cibercriminal, es necesario matizar, tal y como dijimos anteriormente respecto al perfil de las cibervíctimas, que tampoco es posible la atribución de características generales a todos los sujetos que delinquen en el ciberespacio, debido a la extensa tipología delictual existente en el mismo. Al respecto, se anticipa la dificultad que conlleva efectuar la perfilación de un tipo de criminal que se oculta detrás de la pantalla de un dispositivo informático y que no se encuentra físicamente en el lugar donde comete su acción criminal, aspectos que en no pocas

ocasiones imposibilita su localización y posterior enjuiciamiento. Por consiguiente, resulta complejo efectuar el profiling de los cibercriminales y el estudio de sus motivaciones personales (hábitos de vida, formación técnica, etc.).

A continuación, se efectúa la necesaria distinción entre la figura del Hacker y la figura del cibercriminal dada la confusión terminológica que puede dar lugar a error al producirse su uso de forma indistinta y sin matices:

6.3.1 Los hackers

Etimológicamente el termino proviene del verbo inglés *"Hack"* que significa alterar, pero su traducción significa pirata informático (diccionario inglés-español Cambridge University Press 2020), no obstante, el termino se ha utilizado de forma amplia y diversa, tanto para referirse a actividades no autorizadas en el entorno digital como para referirse a personalidades famosas como Grace Murray Hopper, conocida como la primer mujer hacker de la historia. Según el DLE *un jáquer (del inglés hacker) o pirata informático* es una persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora.

Conviene especificar, que no existe un consenso científico respecto a la tipología de hackers existente, no obstante, y a pesar del significado peyorativo del término (asociado a la intromisión a la intimidad, el robo de datos personales, patrimoniales, etc.), no todos son "malos", también hay hackers, denominados éticos, que trabajan para proteger los datos y mejorar los sistemas informáticos. Respecto al uso del término es necesario, por tanto, establecer una distinción para tratar de no identificar al hacker con el cibercriminal, como ocurre habitualmente, es decir, no se debe meter a todos los hackers en el mismo saco. La necesidad de establecer una diferenciación terminológica responde, precisamente, a que cuando nos referimos al cibercriminal lo hacemos para definir a cualquier sujeto que utiliza el ciberespacio como parte esencial de su conducta criminal. No obstante, cuando nos referimos al hacker, lo hacemos para definir determinadas conductas online en función de las cuales se establecen diversas clasificaciones o categorizaciones (representadas mediante sombreros de diferentes colores), que no se van a analizar en este trabajo, entre otras razones por su falta de validación empírica. Lo mismo ocurre cuando nos referimos a la denominada "ética del hacker", que también adolece del consenso necesario en cuanto a su significado y cuyo análisis no es objeto de este trabajo, pero que consideramos conveniente mencionar para poder

ilustrar la visión altruista que, tradicionalmente, se ha tenido del hacker en relación a su capacidad de acceso sin barreras a la Red y a la información contenida en la misma. Ahora bien, cabe matizar que desde el año 2005, como consecuencia de los cambios legales operados tras la aprobación de la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005 de la UE, sobre ataques contra sistemas de información, (en España concretamente mediante la LO. 5/2010, de 22 de junio) dichas conductas se han convertido en delictivas y han ido reduciendo, desde el punto de vista legal, la capacidad de acción de los hackers y, por tanto, han afectado negativamente a la imagen de los mismos.

En línea con lo anterior, es también necesario establecer una distinción entre los términos *hacker y crackers* (término acuñado por los propios hackers para definir a los expertos informáticos que acceden a las redes y sistemas fuera del marco legal para obtener un beneficio económico ilícito), no obstante, conviene indicar también que la frontera entre las concepciones morales y legales de los hackers y los crackers pueden ser traspasadas de forma frecuente por los primeros al no encontrar una salida profesional o económica a su actividad.

Actualmente el uso masivo de Internet y el aumento de los conocimientos informáticos de los usuarios ha supuesto la evolución del término hacker, dando como resultado el surgimiento de diversas modalidades de hackers, que engloban desde expertos informáticos hasta los denominados scriptkiddies (término empleado de forma despectiva por otros *hackers), cuyo* perfil corresponde a jóvenes que tienen conocimientos informáticos a nivel de usuario, están adaptados socialmente y cuyos ataques informáticos son al azar mediante programas y *scripts* básicos, causando daños debido al malware utilizado y no tanto a su intención al no disponer de los conocimientos adecuados.

6.3.2 Análisis criminológico del perfil del cibercriminal

Seguidamente, tras efectuar la necesaria distinción terminológica entre los hackers "buenos y malos", nos centraremos en el estudio de los segundos, debido a que su intencionalidad lesiva respecto a los derechos de los demás, bien sea económica o para dañar los sistemas aprovechando sus vulnerabilidades, los situaría, con más énfasis, dentro del concepto amplio atribuido al cibercriminal ya apuntado al inicio de este trabajo. En relación al análisis criminológico del perfil de los cibercriminales conviene efectuar una serie de puntualizaciones respecto a las dificultades que puede presentar su estudio:

- El estudio, cuantitativo y cualitativo, del perfil del cibercriminal presenta serias complicaciones respecto a la definición de sus características específicas debido a la variedad de ciberdelitos

existentes y a las dificultades respecto a su perseguibilidad. Por consiguiente, podemos afirmar, al igual que ocurre con los criminales offline, que existen múltiples perfiles de cibercriminales en función del propósito criminal de los mismos.

- Otro de los problemas que surgen dentro del estudio criminológico de los posibles perfiles de los cibercriminales, tiene que ver con el ámbito espacial en el que se produce el cibercrimen; el ciberespacio, que provoca un cambio, no solo en el tablero de juego, sino también en las reglas del mismo, provocando que el comportamiento de los actores intervinientes se modifique y tenga que adaptarse técnicamente, de forma constante, a la nueva realidad virtual (bien como forma de aprendizaje, por necesidades de índole laboral, por simple curiosidad, etc.)

Es oportuno, por tanto, destacar la importancia de las motivaciones personales al estudiar el *Profiling Criminal* de los ciberdelincuentes. Al respecto WEULEN (2016) señaló, tras investigar las motivaciones personales de los ciberdelincuentes condenados en los Países Bajos durante un periodo de diez años, que en primer lugar se situaba la curiosidad, seguido de la ira, la venganza, la lascivia y por último el lucro. Mediante las encuestas efectuadas, a dichos ciberdelincuentes, pudo determinar la existencia de un perfil cibercriminal, al determinar una serie de factores de riesgo como el uso temprano de las TIC y determinados factores psicológicos como una personalidad narcisista, analítica e introvertida.

En el estudio además se destacan como factores determinantes en las motivaciones personales de los cibercriminales que; tener pareja y al menos un hijo reduce el riesgo de criminalidad en los delitos online(46%) en comparación a los delitos offline (19%); sin embargo, tener trabajo en el sector de las TIC o formación educativa especifica en dicho sector aumenta el riesgo de ciberdelincuencia en comparación a si los mismos se desarrollen en otro sector laboral y educativo, lo que reduciría el riesgo en ambos casos tanto en los delitos online como offline. Finalmente, el estudio destaca que los ciberdelincuentes examinados cometieron los delitos online, principalmente, por curiosidad y como forma de aprendizaje, con un patrón similar de actuación en cuanto al contexto y habilidades.

En la tabla siguiente se exponen, de forma resumida, las conclusiones principales de su estudio:

	Delincuente Offline	Delincuente Online
DATOS DEMOGRAFICOS	• Varón en una proporción muy alta. • Curva de edad/crimen; - Pico de adolescencia tardía/ edad adulta temprana. - Disminución gradual después. • Proporción similar nacionales/extranjeros.	• Varón en una proporcion mayor, aunque está aumentando el número de mujeres. • Curva de edad/crimen: - Indefinida. - Comienzo joven. - Persistente en el tiempo. • Prevalencia raza blanca, asiáticos y europeos del este.
EDUCACIÓN/ NIVEL SOCIOECONÓMICO	• Nivel educación; bajo. • Nivel socioeconómico; bajo	• Nivel de educación; medio/alto. • Nivel socioeconómico medio. • Vive con sus padres/ con otros estudiantes.
AUTO CONTROL	• Bajo autocontrol. • Obtención de beneficios inmediatos. • Costos a largo plazo.	• Alto autocontrol. • Nivel de moralidad mayor. • Autoaprendizaje mayor que el aprendizaje con compañeros.
DISUASIÓN	• Relación coste/beneficios; negativa. • Relación efecto/castigo; negativa. • Relación riesgo/captura; alta.	• Relación coste/beneficios; positiva. • Mayor planificación/ menor riesgo. • Relación riesgo/captura; bajo

Tabla de elaboración propia sobre el estudio del perfil del ciberdelincuente de Marleen Weulen Kranenbarg.

Continuando con las dificultades respecto al perfil criminológico del cibercriminal, cabe hacerse la siguiente pregunta; ¿Por qué apenas existen estudios de perfilación criminal en España en relación al cibercrimen? Una posible respuesta la podemos encontrar en el último informe sobre Cibercriminalidad correspondiente al año 2018, emitido por la Secretaria de Estado de Seguridad perteneciente al Ministerio del Interior, a través de los datos obtenidos por el Sistema Estadístico de Criminalidad (SEC), los cuales muestran una tendencia alcista respecto a los mismos datos de otros años (especialmente en relación con el fraude informático) y, sin embargo, las detenciones y los procesos judiciales permanecen en cifras similares año tras año:

HECHOS CONOCIDOS	2015	2016	2017	2018
ACCESO E INTERCEPTACIÓN ILÍCITA	2.386	2.579	2.505	2.750
AMENAZAS Y COACCIONES	10.112	11.473	11.270	11.960
CONTRA EL HONOR	2.131	1.524	1.537	1.423
CONTRA PROPIEDAD INDUST./INTELEC.	167	121	109	217
DELITOS SEXUALES(*)	1.233	1.188	1.312	1.393
FALSIFICACIÓN INFORMÁTICA	2.361	2.697	2.961	3.095
FRAUDE INFORMÁTICO	40.864	45.894	60.511	88.760
INTERFERENCIA DATOS Y EN SISTEMA	900	1.110	1.102	1.015
Total HECHOS CONOCIDOS	**60.154**	**66.586**	**81.307**	**110.613**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

Tabla sobre la evolución de la cibercriminalidad en España (Fuente de datos: SEC)

En el periodo comprendido entre 2015 a 2018 , según los datos conocidos por las Fuerzas y Cuerpos de Seguridad (excluidos datos de Ertzaintza y Mossos d'Esquadra), se constata el aumento de la ciberdelincuencia, al contabilizarse 110.613 ciberdelitos en 2018 (correspondiendo mayoritariamente a fraudes informáticos-estafas y amenazas-coacciones (el 80.2 % y el 10.8% respectivamente), de los cuales se esclarecieron 24.767 (22,4%) y sólo fueron detenidas y puestas a disposición judicial 5.697 personas (5,15 %).

Con base en los datos sobre cibercriminalidad en España, en los que existe una clara prevalencia de los ciberfraudes y las cibercoacciones, se efectúa seguidamente el análisis criminológico en la que se describen los posibles perfiles de ambos tipos de criminales que actúan en la Red:

Perfil del autor del ciberfraude: hay pocos estudios criminológicos acerca del perfil de este tipo de ciberdelincuentes, alguna de las razones ya se ha apuntado a lo largo de este trabajo, hay pocas detenciones al año debido a la dificultad para su detección y su enjuiciamiento, a pesar de que este tipo de cibercrimen no deja de dar titulares de forma cotidiana. A continuación, se analiza a los autores de fraudes informáticos estudiados en la denominada investigación Yale[11] para extraer las diferencias entre estos, los delincuentes comunes y la población general:

	Delincuente Común	Delincuente Socioeconómico	Población General
SEXO MASCULINO	68,6%	85,5%	48,6%
RAZA BLANCA	34,3%	81,7%	76,8%
MEDIA DE EDAD	30	40	30
EDUCACION SECUNDARIA	45,5%	79,3%	69,0%
EDUCACION UNIVERSITARIA	3,9%	27,1%	19,0%
DESEMPLEADO	56,7%	5,7%	5,9%
EMPLEADO FIJO	12,7%	58,4%	No disponible

Tabla de elaboración propia con los resultados de la denominada "investigación Yale"

[11] Estudio sobre la revisión de sentencias de ocho tipos de delitos socioeconómicos relacionados con el ciberfraude, de los tribunales de los Ángeles, Atlanta, Chicago, Baltimore, Nueva York (Manhattan y Bronx), Dallas y Seattle.

En la tabla se reflejan las diferencias en porcentajes entre los delincuentes comunes, los delincuentes socioeconómicos y la población general. En la investigación los autores, (BENSON y SIMPSON, 2015), tratan de explorar si las personas de estatus social medio y bajo utilizan las técnicas identificadas por el propio Sutherland, en los delitos de cuello blanco, del mismo modo, que las pequeñas y medianas empresas pueden cometer actividades ilegales con técnicas delictivas similares a las empleadas por las grandes empresas y las multinacionales. Al respecto, el resultado de la investigación arroja un resultado con un elevado porcentaje positivo, tal y como se refleja en la tabla, no obstante, cabe matizar que en el estudio se alude a Sutherland en relación a este aspecto y no a otro (dada la diferencia de estatus social entre las personas sometidas a la investigación de las personas de alto nivel social denominadas de "cuello blanco").

Las características que diferencian a los delincuentes socioeconómicos conforme a la investigación Yale son; la mayoria son hombres, provenientes de un entorno social y demográfico distinto al de los delincuentes comunes, diferenciándose también respecto a la edad media, con una mayor probabilidad de que estén casados y tengan vivienda propia, económicamente estables , con un nivel de educación mayor respecto a la población general (y especialmente superior al de los delincuentes comunes) tienen trabajo y se diferencian de los delincuentes de cuello blanco definidos por Sutherland en el estatus social. También se caracterizan en que se tienen a sí mismos en alta consideración, no se autoconceptuan como delincuentes, ni creen del todo que sus actividades sean delictivas.

Perfil del ciberacosador; los datos sobre cibercriminalidad en España indican que tras los ciberfraudes el ciberacoso en la Red se sitúa a continuación como la forma delictiva online más denunciada[12]. A continuación, se analizan los perfiles de los ciberacosadores más significativos con la exhaustividad que permite la extensión de este trabajo:

- *El cyberstalker:* apenas existen estudios de profiling criminológico referentes al acosador online, tampoco existe un consenso a la hora de establecer una comparación entre las características del

[12] Según los datos FGE recogidos en la Memoria de la FGE 2018, el acoso mediante la Red, desde su incorporación como figura típica al Código Penal por LO 1/2015, ha aumentado progresivamente; de los 96 registros del año 2015 fueron elevándose a 131 en 2016 y 200 en 2017 hasta alcanzar en 2018 la cifra de 337.

acoso tradicional y el acoso a través del ciberespacio, ni unanimidad a la hora de establecer una definición de esta actividad.

Cabe destacar al respecto el estudio pionero de BOCIJ Y MCFARLEN (2002), mediante el cual lograron distinguir cuatro tipos de acosadores online, los cuales se reflejan en la tabla siguiente:

	VENGATIVO	COMPUESTO	INTIMO	COLECTIVO
MOTIVACION	Acechar a sus víctimas incluso fuera de línea	Molestar a sus víctimas, sin intención de mantener relación sentimental	Establecer una relación íntima con sus víctimas.	Unión de dos o más personas para perseguir a sus víctimas a través de las TIC
ANTECEDENTES DELICTIVOS/ PSIQUIATRICOS	Antecedentes delictivos no se descarta historial psiquiátrico previo.	No suelen tener antecedentes ni presentan historial psiquiátrico previo.	No constan	No constan
PERICIA USO DE LAS TIC	Nivel elevado	Nivel medio-alto	Rango amplio desde nivel bajo a nivel elevado.	Rango alto a bastante alto.
METODOS DE ACOSO	Amplios; envíos correos masivos, troyanos, robos de identidad etc.	Emisión de amenazas	Mensajes online y salas de chat	Muy variado; correo no deseado, bombardeos, robo de identidad etc.

Clasificación de Bocij y McFarlen sobre los cuatro tipos de cyberstalker (acosadores online).

El estudio analizado tenía entre sus objetivos elaborar no solo una clasificación de los tipos de cyberstalker, sobre la base de la motivación que les mueve a actuar sobre sus víctimas, sino también definir sus características demográficas, obteniéndose los resultados siguientes:

- Respecto al sexo; predomina el masculino (84,6% de los hombres frente a 15,4% de mujeres).
- Respecto a la edad; la edad media se sitúa en 41 años (cuyo rango varía entre los 18 y 67 años).
- Respecto al estado civil del cyberstalker; predominan los solteros (52,3%) frente a los casados (21,7%) o que estén separados o divorciados (17,3%).
- Respecto a los conocimientos informáticos; el 41% de los casos analizados poseía conocimientos medios y un 50% conocimientos altos o muy altos.
- Respecto a la ocupación laboral; de la investigación se desprende que un 50% tenía trabajo frente a un 18,2% que se encontraba en el paro y un 8,3% que estudiaba.

- *El cybergroomer:* con base en los estudios de profiling criminológico de los ciberdepredadores sexuales y efectuando la comparación con el perfil del depredador sexual "tradicional", podemos extraer las conclusiones siguientes entre las características psicológicas de ambos, (MIRÓ, 2012):

- El perfil del agresor en el ciberespacio respecto al del abusador tradicional es significativamente distinto y desde una perspectiva preventiva-especial menos peligroso, al tener un mayor autocontrol y una menor impulsividad.
- Continuando con la comparativa; el cybergroomer es consciente del daño que puede infligir con su conducta mientras que el depredador tradicional no es consciente del daño infligido. Esto quedaría confirmado por la comparación psicológica entre ambos, de forma que; el agresor online respecto al agresor sexual clásico tiene una mayor empatía con las víctimas, menor índice de desviación sexual y menores distorsiones cognitivas.
- Ambos agresores se diferencian, por tanto, en las diferentes necesidades que tratan de cubrir ambos agresores de forma que; el autor del grooming a través de Internet obedece a la necesidad que tiene de escapar, por medio de fantasías sexuales con menores, de la soledad, la baja autoestima o su dificultad para relacionarse con otras personas, tratándose de varones de edad avanzada que en muchas ocasiones no tienen una intención real de llevar a cabo sus fantasías. Mientras que el groomer que actúa en el espacio físico tradicional actúa contra niños debido a la necesidad de ejercer dominio, poder, control o rabia como forma de autogratificación. El objetivo del ciberabusador sexual es mantener relaciones sexuales consentidas con menores de edad de trece a dieciocho años (no es generalmente un pedófilo dado que sus objetivos no son niños menores de trece años).

- El ciberbully: Los datos relacionados con este tipo de cibercrimen son muy variados, no obstante, si comparamos los resultados obtenidos en los mismos llegamos a la conclusión que existen múltiples discrepancias relacionadas con cuestiones de índole cultural, metodológica, conductual o temporal entre otras. Para efectuar un análisis que se aproxime al perfil criminal del ciberbully hay autores que establecen como método de estudio el paralelismo entre el bullying tradicional y el ciberbullying (ORTEGA, CALMAESTRA Y MERCHAN, 2008). De la comparación de ambos tipos de agresores podemos establecer una serie de características, las cuales se relacionan, a continuación, de forma resumida:

- Respecto al sexo hay cierto disenso respecto al porcentaje existente entre los chicos y las chicas ciberagresores, sin embargo, si se compara con el género del agresor en el bullying tradicional se admiten diferencias por el distinto rol sexual; los chicos en el espacio físico efectúan las agresiones de forma directa (física), las chicas de forma indirecta (sutil, emocional).
- Respecto a la edad, si se compara el registro de datos respecto al bullying tradicional el número de casos es similar en ambos casos apareciendo en segundo y tercero de secundaria.
- Otras características coincidentes entre ambos tipos de agresores (online y offline) son: no presentar problemas de autoestima en comparación a sus víctimas; sienten una fuerte necesidad de dominar y someter a otros estudiantes; son impulsivos e iracundos, carecen de empatía, suelen ser desafiantes y agresivos con los adultos incluidos los padres y los profesores; suelen cometer conductas antisociales como el vandalismo; suelen ser usuarios frecuentes de Internet, tener acceso a un ordenador privado y hacer uso de él en dependencias poco vigiladas y atesoran tener conocimientos específicos sobre las TIC.

6.4 Control social del cibercrimen:

Al efectuar el análisis criminológico del control social referido al cibercrimen y al hilo del análisis previo contenido en este trabajo, se considera necesario efectuar un reflexión respecto a la importancia que tradicionalmente se le ha otorgado al control social del delito, protagonismo que ha perdido en gran medida por la sensación de ineficacia que proyecta, principalmente, el control social de carácter penal, circunstancia que le aleja como estímulo preventivo eficaz que pueda servir para cambiar la percepción de impunidad en los usuarios de la Red, especialmente la de aquellos que contribuyen a aumentar año tras año las cifras de la cibercriminalidad.

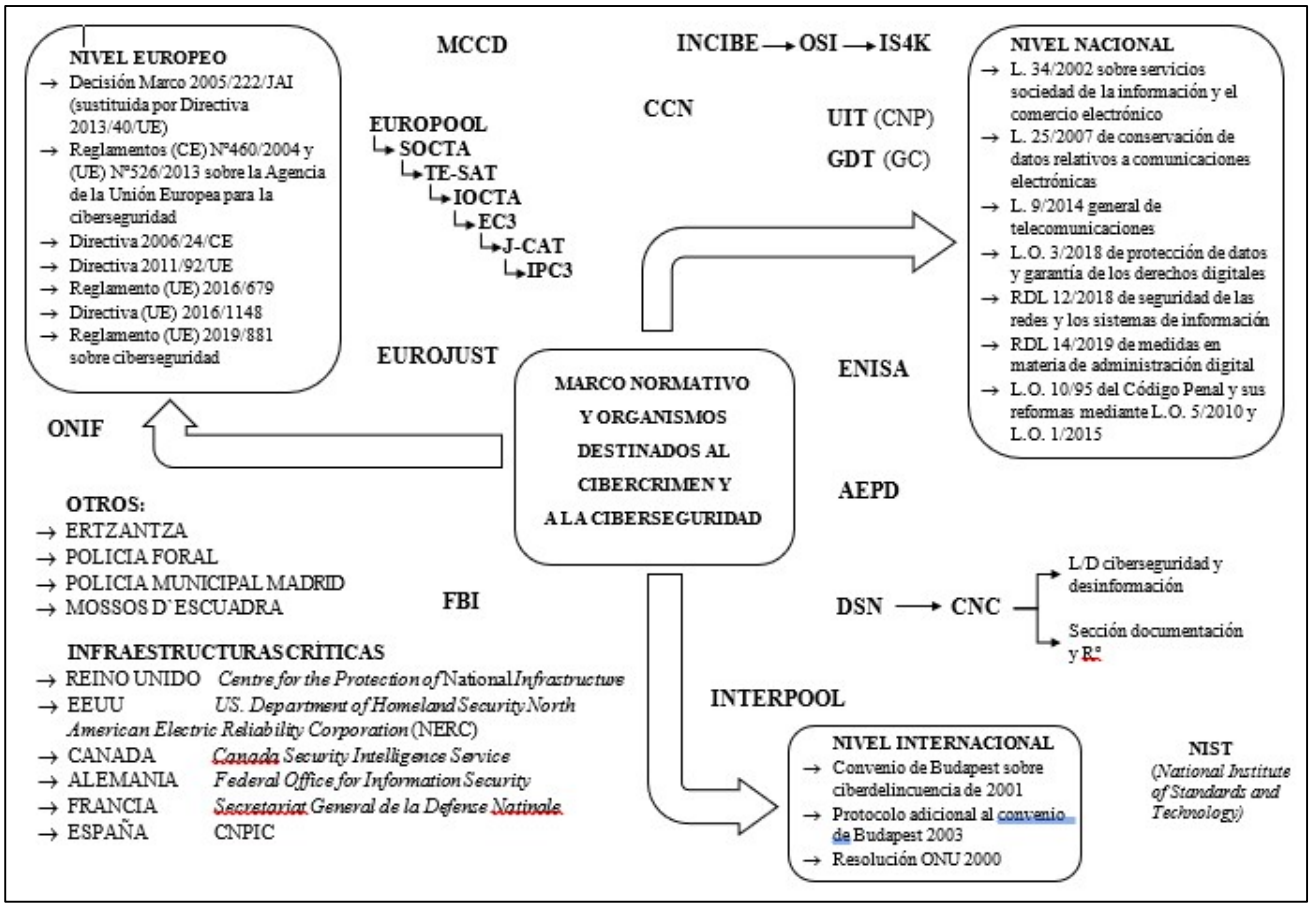
En este apartado se analizarán las posibles causas que producen la minoración de la eficacia del control social formal del cibercrimen, a tal fin, se analizará la problemática que surge en relación a la perseguibilidad judicial de los delitos *online* y como podría enfocarse desde el control social informal la prevención del cibercrimen.

6.4.1 Análisis criminológico del control social del cibercrimen

Las nuevas posibilidades que han surgido con la aparición de las TIC y de internet, ni tan siquiera han sido evaluadas en su totalidad, fundamentalmente por la velocidad a las que han aparecido y siguen apareciendo. El análisis, de este fenómeno "vivo", permite afirmar que ha supuesto un avance enorme a nivel tecnológico, pero también ha abierto un campo enorme a nuevas formas de

criminalidad. Aludiendo a estas últimas ha resultado necesario y obligatorio regular este ámbito debido, fundamentalmente, al carácter transfronterizo de la red, a las dificultades que conlleva perseguir policial y judicialmente a los autores de los delitos cometidos a través del ciberespacio y a la necesidad preventiva que ha surgido a nivel político, económico y social.

En el siguiente cuadro se refleja una muestra resumida del desarrollo legislativo y orgánico que se ha efectuado durante los últimos años para luchar contra el cibercrimen, en el cual se tratan de plasmar los principales organismos destinados a la ciberseguridad y la normativa principal reguladora de la lucha contra el cibercrimen a nivel nacional, europeo e internacional (los cuales se reflejan únicamente a modo de referencia dada la fácil accesibilidad existente para su consulta). Por consiguiente, la finalidad que se persigue con este análisis es doble y trata de evidenciar una realidad un tanto contradictoria; por un lado, que existe un control social formal suficiente y, por otro lado, la percepción de que dicho control social no está calando en la población en general y en los usuarios de internet en particular:



Esquema de elaboración propia que refleja el control social formal que actualmente se ejerce sobre el cibercrimen.

La reflexión criminológica pretendida en este apartado se centra, precisamente, en la necesidad de reflejar que, verdaderamente, si existe control y seguridad por parte de los gobiernos y de los organismos específicos creados para proteger los objetivos más sensibles desde el punto de vista de un ciberataque, como son las infraestructuras críticas, sin embargo, la sensación de seguridad y protección desciende comparativamente entre el internauta institucional y el internauta particular (que no goza de un sistema tan protegido, actualizado y protocolizado).

6.4.2 Problemática del cibercrimen respecto a la actuación de los tribunales penales:

Paralelamente, es necesario recalcar que las dificultades en la lucha contra la delincuencia tradicional siempre han estado presentes desde el punto de vista jurisdiccional y competencial sobre todo cuando esta se produce en un contexto transnacional. La irrupción de la ciberdelincuencia lejos de minimizar el problema lo ha agravado, ello es debido, principalmente, a que el ciberespacio carece de puestos fronterizos, no tiene vallas ni concertinas, ni agentes de la autoridad que puedan vigilarlo, permitiendo a cualquier persona conectada a Internet cometer determinadas conductas delictivas sin necesidad, ni tan siquiera, de que tenga que estar presente su víctima, circunstancia que algunos autores califican de "*sueño para sus usuarios y una pesadilla para los prácticos del derecho*"(GIL LOPEZ, 2015). El principio de seguridad jurídica, por tanto, en este nuevo contexto, parece diluirse en la inmensidad virtual del ciberespacio fundamentada, principalmente, por la ausencia de cualquier tipo de límite espacial, "maniatando", en términos de eficacia preventiva, la acción de la justicia.

Anteriormente se han reflejado en este trabajo las cifras de cibercriminalidad actuales facilitadas por el Ministerio del Interior y hemos podido constatar que el volumen de registros judiciales no se corresponde con las mismas. Entre las razones aducidas desde la FGE para explicar la divergencia en los datos referidos estaría, principalmente, la modificación del artículo 284 LECrim, operada mediante la LO 13/2015, que ha determinado que los atestados por hechos ilícitos en los que no conste autor conocido no sean trasladados a los órganos judiciales o al Ministerio Fiscal, a excepción de los supuestos específicos que se citan expresamente en dicho precepto. Por ello, existe un volumen muy importante de denuncias o diligencias policiales por hechos ilícitos cometidos a través de la red que no llegan al conocimiento de los órganos de la Administración de Justicia y por tanto quedan al margen de las estadísticas judiciales y también de las del Ministerio Fiscal.

Actualmente, la problemática que acarrea la ciberdelincuencia tiene que ver precisamente con la restricción que supone para el derecho tradicional su aplicación, al generarse una serie de incertidumbres jurídicas (GIL LOPEZ, 2015) que se fundamentan en las razones siguientes:

A. *Las peculiaridades del cibercrimen*: que pueden resumirse en cuatro características:

- *La deslocalización*; el uso de las TIC ha transformado las concepciones del tiempo y el espacio, de forma que el ciberdelincuente, como consecuencia del denominado efecto multiplicador de Internet, puede estar alejado del lugar donde comete los hechos y sus efectos producirse en otros países de forma exponencial. Reseñar que los infractores mediante programas informáticos además pueden producir la ruptura del vínculo temporal entre la acción y el resultado para distorsionar el momento de la comisión del ciberdelito.
- *La inmaterialidad*; con las TIC han surgido nuevos elementos inmateriales, como la información, cuyo carácter intangible ha resultado problemático a la hora de aplicar su analogía con los elementos materiales o tangibles protegidos por el derecho tradicional, dando lugar a la necesidad de efectuar sucesivas reformas legales para asegurar su protección.
- *La facilidad comisiva*; la comisión de este tipo de delitos solo exige contar con un terminal conectado a la Red y unos conocimientos técnicos mínimos (reseñar que tal exigencia aumentará en función del nivel de tecnificación que exija el delito en cuestión). El abuso de la Darknet[13] que utilizan los delincuentes para el comercio ilícito en línea de drogas, armas, bienes robados, datos personales y de tarjetas de pago robados, documentos de identidad falsificados y material de abuso infantil, facilita, enormemente, la actividad delictiva en la Red. Este *Internet oculto* se ha convertido en una herramienta clave para impulsar la evolución del cibercrimen y representa un desafío muy complejo para la aplicación de la ley.
- *La atipicidad*; los denominados delitos informáticos regulados en nuestro código penal no aparecen organizados de forma sistemática bajo una misma rubrica, por tal motivo se atribuye a los mismos una falta de tipicidad.

[13] El término Darknet, no se trata de ninguna red, sino de un conjunto de contenidos de carácter ilegal e ilícito ubicados dentro de la Web profunda.

B. <u>El anonimato del autor</u>;

La comisión de este tipo de delitos se fundamenta en gran medida en el carácter anónimo del cibercriminal y la ejecución del delito sin conexión física. Este aspecto dificulta su identificación policial, la cual se efectuará por medio de la dirección *IP* que podrá resultar sencilla o casi imposible en función del nivel de conocimiento del usuario para dejar evidencias digitales o no. Una vez identificada la dirección IP y a través de la correspondiente autorización judicial, se puede acudir al prestador de servicios de acceso para conocer la identidad de la persona a ella vinculada a IP y en su caso incoar un procedimiento contra ella (la gestión del sistema de nombres de dominio la realiza a nivel mundial el ICANN, a nivel nacional la gestión se le encomienda a la entidad pública empresarial Red.es). Ahora bien, respecto a la ocultación de la dirección IP cabe indicar que no hace falta tener los conocimientos de un experto informático, solo tenemos que introducir en cualquier buscador de internet; "como hackear nuestra identificación en la Red" y podemos comprobar el numero ingente de páginas con tutoriales al respecto.

A lo anterior, también hay que sumar la corriente de autores que defienden la intimidad y la protección de las comunicaciones en el ciberespacio por encima de cualquier otro interés institucional, (PEIRANO, 2019), los cuales indican, no solo, la necesidad de combatir la vigilancia online, sino también, como hacerlo, sobre todo en determinados contextos como el periodístico en el que se considera clave la protección de la comunicación respecto a sus fuentes de información, tanto con la finalidad de preservar dicha información, como, para preservar la seguridad de la propia fuente y del propio periodista (sobre todo dependiendo de la latitud del mundo en la que este ejerciendo su labor periodística). El problema que surge, sobre este tipo de información tan detallada acerca de las herramientas más eficaces para evitar el control de los servidores de internet, como, por ejemplo; el acceso a red Tor, crear discos virtuales, la encriptación de e-mails etc. radica en que también puede servir a los cibercriminales para ocultarse, aún más y mejor, dificultando su persecución policial y judicial.

Para tratar de contrarrestar el problema derivado de la averiguación de la evidencia informática se han creado herramientas como Ramsés (Plataforma para facilitar la investigación forense con el objetivo de analizar malware en el entorno financiero, integrada en el proyecto CORDIS de la UE).

C. La problemática que surge respecto a la competencia territorial:

La deslocalización, ya analizada, de las conductas delictivas a través de la Red guarda una relación directa respecto al problema de la competencia territorial para la persecución de los mismos, fundamentalmente porque al cometerse a través de la Red, en muchas ocasiones, resulta de gran dificultad determinar el lugar de comisión sin una localización física concreta.

Con la finalidad de aplicar el principio de territorialidad y poder determinar la jurisdicción competente respecto a la autoría de los mismos se aprobó el Convenio sobre Cibercriminalidad del Consejo de Europa de 2001; pero, ¿qué está ocurriendo en la práctica? que aun existiendo la voluntad internacional para sortear el problema territorial analizado no está siendo suficiente para solucionar los problemas asociados al carácter transfronterizo de la Red (sirva como ejemplo el caso Yahoo[14]).

D. La definición del bien jurídico protegido:

Cabe cuestionarse, respecto a la definición del bien jurídico protegido, si la delincuencia tecnológica contiene nuevos bienes jurídicos o no. Gil (2015) señala que, aunque cambia el medio comisivo para realizar dichas conductas, en comparación a los delitos tradicionales, el bien jurídico protegido es el mismo (por ejemplo; la propiedad o la intimidad), con una excepción, surgida como otro bien jurídico accesorio a los anteriores; la Información.

6.4.3 Prevención del cibercrimen desde el enfoque de las actividades rutinarias:

Una vez analizado porque el control social tiene una ineficacia contrastada respecto a la lucha y la prevención del cibercrimen principalmente a nivel particular y también a nivel público (aunque en menor medida debido a la implementación de medidas de seguridad en sus sistemas informáticos) se tratará de analizar la posible conexión entre el enfoque de las actividades rutinarias o cotidianas y su utilidad para la prevención del cibercrimen.

La prevención del cibercrimen desde el enfoque de las actividades rutinarias cobra sentido pleno al haberse acreditado, de forma empírica, que los usuarios de internet tienen, en última instancia, la capacidad de decisión para elegir mediante sus actos y hábitos si quieren o no ser víctimas de un

[14] En el caso Yahoo, el tribunal de Gran Instancia de París condenó a esta empresa por vender en Francia productos de carácter nazi, cuestión prohibida por la normativa francesa. Estableció el tribunal la necesidad de bloquear el acceso a la web desde Francia y se prohibió la venta de los artículos en cuestión. Yahoo alegó que su sede estaba en estados Unidos y allí esa venta no estaba prohibida, de tal forma que la orden del tribunal era imposible de cumplir en base a las dificultades de determinar con claridad a los usuarios franceses que accedían a los productos de la empresa.

cibercrimen. A este factor de elección personal contribuye, sin duda alguna, el desconocimiento tanto de los adultos como de los más jóvenes, especialmente el de estos últimos, de las medidas de seguridad existentes, los cuales delegan, con una especie de fe ciega, toda su "defensa online" en los programas antivirus y en los *firewalls*. Surge, por tanto, la necesidad de conocer y analizar las conductas que los usuarios de la Red realizan en su constante y "compulsiva" (en muchos casos) interacción social y personal por medio de las TIC y como las mismas se relacionan con la probabilidad de que sean víctimas de un ciberdelito.

Por consiguiente, es necesario incidir en que la prevención de una conducta, sin duda, exige un ejercicio de concienciación previa, requisito que en el caso de los menores de edad se intensifica especialmente. Para lograr que un menor de edad se replantee el uso que hace de las TIC por otro diferente, menos impulsivo, exige un cambio de mentalidad totalmente distinto respecto a la idea generalizada de que "no pasa nada por navegar por la Red" o "apenas hay riesgo cuando utilizo el ordenador o el móvil". ¿Como lograr entonces que los más jóvenes inviertan el orden de sus prioridades, es decir, interaccionar con el mayor número de personas en las redes sociales y con la mayor velocidad posible en pro de una mayor seguridad? La TAC analizada a lo largo de este trabajo apunta las posibles soluciones, las cuales pasan por hacerles ver que las oportunidades de convertirse en cibervictimas dependen en gran medida de su propio comportamiento, por ejemplo; no contactando con desconocidos ni agregándolos a las redes sociales, evitando guardar información personal o tener imágenes personales intimas en el móvil o en el PC, no facilitando datos domiciliarios y/o bancarios a través de Internet, etc. En dicha labor de concienciación el papel de los padres y de la escuela es clave:

- *Respecto al papel de los padres*, por un lado, deben permitir el acceso a la tecnología de sus hijos y, por otro lado, deben saber conjugar los límites necesarios para que puedan hacerlo de la forma más razonable posible. Si atendemos a los datos del INE[15], estadísticas año 2019, casi el 70% de los menores entre 10 y 15 años tiene móvil, el porcentaje más bajo corresponde a los menores de 10 años con un 26,1%, mientras que el porcentaje de menores que tiene móvil a la edad de 15 años se sitúa en el 94.8%, por tanto, podemos afirmar, a la vista de los datos, que esta tarea no

[15] Datos del Instituto Nacional de Estadística referentes a las condiciones de vida, respecto a los principales indicadores de equipamiento y uso de las TIC en los hogares españoles del año 2019, pp.26.

es baladí, porque los padres ni tan siquiera tienen claro la edad a la que tienen que permitir a sus hijos el móvil. El uso de las TIC, principalmente a través del teléfono móvil, mediatiza el comportamiento de los menores de edad, y los condiciona permanentemente, convirtiéndoles en una especie de *"prisioneros online"* debido, principalmente, a los comentarios de las redes sociales (destacándose entre ellos el poder de los *likes* que ya ha sido analizado en este trabajo). En definitiva, los padres necesitan aumentar su conocimiento acerca de cuestiones relativas a; ¿Cuándo debe entrar el móvil en casa?, ¿Hasta dónde hay que dar a los hijos libertad para su uso? o ¿Qué papel tienen los padres en la supervisión de la actividad que realizan los hijos en Internet? Una herramienta de ayuda valiosa al respecto y que puede servir a los padres en esta difícil tarea la encontramos en la página is4K[16] del portal de Incibe.

- *Respecto al papel de los centros escolares*, se considera que pueden y deben ejercer un control informal de este fenómeno con una mayor presencia y eficacia. Continuando con el análisis inicial sobre la repercusión actual y futura de la telefonía móvil en relación a su uso por parte de los menores de edad, podemos comprobar que no existe una coherencia entre la realidad y los contenidos que se imparten en las aulas. Para corroborar esta afirmación, un tanto categórica, debemos analizar los contenidos que se están impartiendo en la ESO, concretamente, en la asignatura de Tecnología; tomando como referencia dos libros de dicha asignatura (ambos elegidos al azar) correspondientes al primer y último curso de la etapa de secundaria (1º de la ESO y 4º de la ESO, que se imparten actualmente), se observa que en el primer curso de esta asignatura no se imparte ningún contenido relacionado con la telefonía móvil, ni sobre seguridad online; en el cuarto curso, respecto a la telefonía móvil tampoco existen contenidos reglados, no obstante, si se imparten contenidos relacionados con la publicación e intercambio de información, y la seguridad informática (donde se explica cómo navegar seguro por internet). Del mismo modo, llama la atención que sobre el *ciberacoso o cyberbullying* en dichos textos no se aborde el tema. Resulta paradójico que, lamentablemente, existan casos de ciberacoso en el último ciclo de educación primaria, cuyos datos enfatizan la necesidad de implementar

[16] is4K (internet segura forkids) Ofrece un catálogo de recursos valiosos tanto para las familias, como los menores y también para los educadores, pudiendo destacarse; La guía de seguridad en redes sociales para familias; el fomento de contenidos positivos online para una infancia digital mejor; la guía de mediación parental; los pactos familiares para el buen uso de dispositivos etc.

programas para mejorar la capacidad crítica de los menores en el uso racional de los diferentes canales de comunicación que ofrecen las TIC con la finalidad de poder prevenir el ciberacoso desde temprana edad (ciclo sexto de primaria) y que, sin embargo, los libros que deberían contemplar estos contenidos, tan importantes para prevenir el cibercrimen en general y el ciberacoso en particular, no los contemplen de la forma que deberían (como por ejemplo; el método KiVa de la Universidad de Turku en Finlandia, apenas conocido e implementado en nuestro país, a pesar de su demostrada eficacia para erradicar el problema del bullying en las aulas).

Cabe matizar que, en la práctica totalidad de centros escolares se imparten charlas sobre estas cuestiones por agentes tutores, psicólogos, trabajadores sociales etc.… y que, en otras asignaturas, como lengua y literatura, se aborda el uso razonable de las redes sociales mediante la lectura de determinados libros, como, por ejemplo; "El libro de los rostros" (ALONSO y PELEGRIN, 2019). No obstante, los datos analizados parecen reflejar que la carga lectiva sobre los peligros de la Red y sobre el uso razonable de las TIC no está siendo suficiente para generar un cambio en la percepción sobre la seguridad *online* de los jóvenes, principalmente, en la etapa escolar en la que coincide la llegada del móvil con los cambios que se generan en sus interacciones personales y sociales.

Por las razones expuestas se considera clave generar en los menores y adolescentes una concienciación distinta respecto a su autoprotección online o, de lo contrario, difícilmente habrá cambios en sus hábitos y rutinas en internet, en definitiva, seguirá afectando negativamente a la prevención del cibercrimen más importante; la de los menores de edad.

7. CONCLUSIONES.

El análisis efectuado en este trabajo se ha basado en el objeto de estudio de la criminología, es decir; el crimen, el delito, el delincuente, la víctima y el control social, pero con un enfoque distinto, marcado por un nuevo ámbito de oportunidad criminal que ha surgido como consecuencia de la interacción personal y social en el ciberespacio, a través de las TIC, el cual ha modificado y sigue modificando el modo tradicional de relacionarnos en sociedad, en cualquiera de las parcelas en las que habitualmente lo hacemos (personales, sociales, económicas, culturales o religiosas).

El estudio criminológico del contexto criminal surgido en el espacio virtual nos indica que se produce un aumento de las posibilidades del agresor motivado de atacar a una víctima debido, no solo, a las peculiaridades propias del ciberespacio y del cibercrimen, sino también, a la disminución de las posibilidades de ser capturado tras realizar dicho ataque. En relación al nuevo contexto delictivo surgido de la interacción online cabe destacar su permanente evolución, provocando que la cantidad de bienes que pueden ser objeto de ciberataques también aumente. Tal es el caso del denominado internet de las cosas que crece a un ritmo vertiginoso y abre la posibilidad a nuevas formas delictivas (incluso el asesinato online).

Se ha sugerido en este trabajo, con la mayor humildad posible, una nueva definición del término cibercrimen y, con base en la misma, una clasificación también nueva de este fenómeno, incluyéndose una nueva categoría referente a los cibercrímenes personales (como la ciberinducción al suicidio y la ciberinducción al daño personal), y cuya finalidad es tratar de distinguir aquellas conductas que atentan contra la vida o la integridad física y moral del resto de conductas que atentan contra otros tipos de bienes, como la intimidad, el patrimonio, la libertad sexual, la información, etc. Cabe señalar que dicha tipología precisaría de un desarrollo empírico adecuado el cual no se ha podido alcanzar en este TFG por cuestiones relativas a las pautas de extensión del mismo, motivo por el cual se ha efectuado una aproximación a los tipos de conductas que se hacen virales por medio de las TIC, concretamente aquellas que conjugan una mayor peligrosidad y popularidad en las redes sociales.

Respecto a las expectativas de crecimiento de la cibercriminalidad, hemos podido comprobar que son coincidentes con las estadísticas oficiales (que aumentan año tras año), sin embargo, esta circunstancia contrasta, de forma alarmante, con el escaso impacto del cibercrimen en los tribunales penales. Todas las investigaciones citadas en este trabajo reflejan un aumento de la criminalidad,

también las cifras policiales sobre el cibercrimen reflejan una clara tendencia alcista, ello es debido a que el ámbito tecnológico ofrece mayores facilidades para la planificación y ejecución criminal y mejores oportunidades de lograr la impunidad debido, entre otras circunstancias, a las múltiples posibilidades disponibles para la anonimización u ocultación del propio rastro, a la volatilidad de las evidencias, al carácter deslocalizado del ciberespacio y al aumento progresivo de internautas que no deja de crecer y, en consecuencia, de forma directamente proporcional, el número de posibles víctimas potenciales.

Esta clara tendencia alcista se explica, además, por la amplia gama de mecanismos de comunicación disponibles (foros, chats, canales Tv, redes sociales, mensajería instantánea, etc.) y por la permanente conexión a la Red de los internautas, que son aprovechadas por los ciberdelincuentes para acosar, intimidar, coaccionar, o defraudar, entre otras conductas ilegales a dichos usuarios de la Red, especialmente a los colectivos de víctimas más vulnerables; los menores de edad.

También se ha incidido, con la exhaustividad que permitía este trabajo, en el análisis de la percepción desvirtuada del cibercrimen que es alimentada por los medios de comunicación y favorecida además por las peculiaridades del ciberespacio y el cibercrimen, a lo que habría que sumar la brecha existente entre la percepción del internauta, la realidad de sus equipos, y sobre la adopción consciente de conductas de riesgo por parte de casi la mitad de los mismos. La conjunción de estos factores acrecienta el problema de la cifra negra del cibercrimen, cuya dimensión real está lejos de ser estimada, por diversas razones que se han tratado de explicar a lo largo de este trabajo, concretamente; la falta de denuncia de la víctima del cibercrimen, la falta de confianza en la administración de justicia, o la publicidad negativa que conllevaría para las empresas el reconocimiento del ciberataque, entre otras.

Se ha efectuado una aproximación a los perfiles de los ciberacosadores y los ciber-defraudadores debido a la preminencia estadística de ambos tipos de delitos online en relación al resto de delitos. Reseñar al respecto la dificultad que conlleva su estudio, dada la multiplicidad de los posibles perfiles de los cibercriminales, que está relacionada con el propósito criminal de los mismos, con la variedad de ciberdelitos existentes y a las dificultades respecto a su perseguibilidad que tienen que ver, principalmente, con el nuevo ámbito espacial en el que se originan provocando un cambio, no solo en el tablero de juego, sino también en las reglas del mismo.

En relación a la cibervíctima se ha tratado de reflejar como su papel en el delito *online* cobra un protagonismo superior al papel de la víctima offline, debido principalmente a los factores siguientes; 1) la víctima, determina los márgenes de riesgo al que va a estar expuesta, por ejemplo; si no utiliza la banca online su patrimonio no podrá ser afectado a través de la Red; 2) la víctima con su forma de interaccionar en el ciberespacio define el ámbito al que puede acceder el agresor motivado; 3) la víctima decide en el uso cotidiano que hace de las TIC la incorporación o no de guardianes capaces para su autoprotección, es decir, sistemas digitales de autoprotección.

Respecto al apartado dedicado al control social del cibercrimen tras su estudio podemos concluir que su desarrollo a nivel legislativo y orgánico no se ha visto corroborado en términos de eficacia preventiva de este fenómeno. Por esta razón, fundamentalmente, se plantea la necesidad de abordar la intervención social y jurídica, de una manera bien distinta, de forma que se logre incentivar al internauta para que desista plantearse la realización de conductas criminales. Esta reflexión surge con una dosis importante de escepticismo debido a la universalización de este tipo de conductas, lo que exige una universalización de la reacción social formal sin fisuras, para evitar que se diluya la misma (lo que exigiría una armonización legal global que actualmente es inviable).

Finalmente se ha abordado la prevención de la cibercriminalidad sobre la base de la importancia que está teniendo la falsa sensación de seguridad de los usuarios de las TIC la cual se origina por una incorrecta valoración sobre los peligros presentes en Internet. Navegamos permanentemente por las redes sociales y demás lugares de comunicación social sin una información concreta sobre los riesgos de su uso. Las estadísticas analizadas en este trabajo respecto al uso de los dispositivos informáticos indican que delegamos nuestra seguridad online a los programas antivirus, a la actualización del equipo y en menor medida al cambio de contraseñas, sin plantearnos que, no solo, es necesario reforzar los mecanismos de protección frente al cibercrimen, sino también, se precisa que los usuarios perciban sus peculiaridades.

La educación de la víctima en seguridad informática, su concienciación para la adopción de software de protección y de rutinas seguras en su actuar cotidiano en el ciberespacio, así como la información real sobre los riesgos en el ciberespacio, serían los primeros pasos a adoptar para la prevención del cibercrimen. Las estrategias de prevención deben enfocarse hacia la educación de los adolescentes en las relaciones inadecuadas con adultos, así como para enseñarles a detectar posibles estrategias de persuasión y manipulación que puedan estar empleando contra ellos. La promoción

de habilidades emocionales en Internet entre los adolescentes podría contribuir a ello (González-Cabrera, Pérez-Sancho y Calvete, 2016).

Con este trabajo se ha pretendido contribuir a mejorar la comprensión del, relativamente nuevo, ámbito de oportunidad criminal generado o favorecido por medio de las TIC, el cual siempre ha estado presente, y que parece adquirir aires renovados con cada avance tecnológico. La evolución de Internet es imparable e innegable, en unos años se completará a nivel mundial, aumentando todavía más nuestra capacidad para interactuar en cualquier tiempo y lugar sin distancias y sin barreras físicas. En dicho contexto resultará clave conocer cuáles son los comportamientos de riesgo en la Red, para poder adoptar hábitos seguros, así como los mecanismos de autoprotección necesarios para minimizar los mismos, siendo conscientes de que la seguridad total seguirá siendo también una quimera no solo en el espacio físico sino también y especialmente en el espacio virtual.

8. BIBLIOGRAFÍA:

ALONSO, A., Y PELEGRÍN, J., *El libro de los rostros*. 7ª ed. Madrid: SM, 2019.

ARBOLEDAS, D., LÓPEZ, T., MUÑOZ, S., OLMO, J., GARCÍA- MONGE, J.A., *Tecnología para 1º de la ESO*. Madrid: SM, 2015.

ARBOLEDAS, D., PEÑA, A., LÓPEZ, T., VALENCIA, R., CHECA, I., GARCÍA- MONGE, J.A., *Tecnología para 4º de la ESO*. Madrid: SM, 2016.

ARNAIZ, P., CEREZO, F., GIMENEZ, A. y MAQUILÓN, J. <<Conductas de ciberadicción y experiencias de cyberbullying entre adolescentes>>. *Revista de investigación en Psicología de la Universidad de Murcia, Anales de Psicología* [en línea]. 2016, pp. 761-769 [consulta: diciembre de 2019] ISSN 1695-2294. Disponible en: https://revistas.um.es/analesps/index

BENSON, M., SIMPSON, S., *Understanding White-Collar Crime*. New York: Routledge. 2015

BOCIJ, P., Y MCFARLANE, L., <<An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers>> >. *First Monday* [en línea]. 2003, vol. 8, núm. 9, pp. 1-10 [consulta: enero de 2020]. Disponible en: https://doi.org/10.5210/fm.v8i9.1076.

BUIL, P., SOLÉ M.J., Y GARCÍA, P., <<La regulación publicitaria de los juegos de azar online en España. Una reflexión sobre la protección del menor Online>> *Adicciones* [en línea]. 2015 · vol. 27 núm. pp. 198-204 [consulta: enero 2020]. Disponible en: http://www.adicciones.es/index.php/adicciones/article/viewFile/706/701

COHEN, L.E. and FELSON, M., <<Cambio social y tendencias en la tasa de criminalidad: un enfoque desde las actividades cotidianas>>. *Revista De Derecho Penal y Criminología* [en línea]. 2018, núm. 20, pp. 359-369 [consulta: marzo de 2020]. ISSN 11329955. Disponible en: https://bv.unir.net:2257/docview/2350468357/fulltextPDF/A730A1058B2A4E3FPQ/1?accountid=142712

Friedberg, I., Skopik F., Settanni G., y Fiedler, R., <<Combating advanced persistent threats: From network event correlation to incident detection>>. *Computers & Security*. [en línea]. 2015. Vol.48, pp. 35-57 [consulta: febrero de 2020]. https://www.sciencedirect.com/. Disponible en: https://doi.org/10.1016/j.cose.2014.09.006

GARCÍA-PABLOS DE MOLINA, A., *Tratado de Criminología*. 4ª ed. Valencia: Tirant lo Blanch, 2009.

GIL LÓPEZ, E., <<La delincuencia en la Red: su regulación en el Código Penal español>>. Madrid. Doopel, 2015.

GIMENEZ PEREZ, A., << Perfiles criminales en el ámbito de la cibercriminalidad social>>. *Revista de Criminalística* [en línea]. 2016, pp. 26-47 [consulta: diciembre de 2019]. ISSN 2346-9307. Disponible en: http://www.skopein.org/ojs/index.php/1/article/view/95/88)

MACHIMBARRENA, J.M. Y GARAIGORDOBIL, M., <<Acoso y ciberacoso en educación primaria>>. *Revista internacional de psicología clínica y de la salud* [en línea]. 2018, vol. 26, núm. 2, pp. 263-280 [consulta: febrero de 2020]. ISSN 1132-9483. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6545150

MALO CERRATO, S., <<Impacto del teléfono móvil en la vida de los adolescentes entre 12 y 16 años>>. *Revista Científica de Comunicación y Educación* [en línea]. 2006, núm. 27, pp. 105-112 [consulta: noviembre de 2019]. ISSN:1134-3478. Disponible en: https://www.redalyc.org/articulo.oa?id=15802716

MARTÍNEZ-FERRER, B. y MORENO RUIZ, D., <<Dependencia de las redes sociales virtuales y violencia escolar en adolescentes>>. *Revista INFAD de Psicología, Universidad Pablo Olavide* [en línea]. 2017. vol. 2. núm.1, pp. 105-114. [consulta: noviembre de 2019] ISSN: 0214-9877. Disponible en: https://doi.org/10.17060/ijodaep.2017.n1.v2.923

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

MONTIEL JUAN I., <<Cibercriminalidad social juvenil: la cifra negra>>. *Revista de Internet, Derecho y Política de la UOC* [en línea]. 2016, pp. 119-131 [consulta: marzo de 2020]. ISSN 1699-8154. Disponible en: https://idp.uoc.edu/

MÜLLER, F. <<The "Werther Effect" management of suicide information by the Spanish print media in the case of Antonio Flores and its impact on the receptors>>. *Cuadernos de Gestión de Información de la Universidad de Murcia*. [en línea].2011. pp 65-71. [Consulta: enero de 2016]. ISSN: 2253-8429. Disponible en: https://digitum.um.es/digitum/bitstream/10201/50898/1/207541-742101-1-PB.pdf

OLVERA RODRIGUEZ, P., <<Web profunda, darknet y Tor>>. *Crimipedia* [en línea]. 2016. Pp. 1-23 [consulta: diciembre de 2019] Disponible en: http://crimina.es/crimipedia/wp-content/uploads/2017/04/Web-profunda-darknet-y-Tor.-OlveraRodriguez_Patricia.pdf

ORTEGA RUIZ, R., CALMAESTRA VILLÉN, J. Y MORA MERCHÁN, J.A., <<Cyberbullying>>. *International Journal of Psychology and Psychological Therapy [*en línea]. 2008. vol. 8, núm. 2, pp. 183-192 [consulta: enero de 2020]. Disponible en: http://hdl.handle.net/11441/58864

PEIRANO, M., *El pequeño libro rojo del activista en la red*. Barcelona: Roca Editorial de Libros. 2019.

ROBLES CARRILLO, M. "El ciberespacio y la ciberseguridad: consideraciones sobre la necesidad de un modelo jurídico". *Publicaciones del Instituto Español de Estudios Estratégicos dependiente del Ministerio de Defensa. Documentos de opinión* [en línea]. 2015, núm. 124, pp. 1-18 [consulta: enero de 2020]. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO124-2015_Ciberespacio-CIberseguridad_Margarita-Robles.pdf

SANTISTEBAN, P., ALMENDROS, C., y GÁMEZ-GUADIX, M., <<Estrategias de persuasión percibidas por adolescentes en situaciones de engaño pederasta por internet (online grooming)>>. *Psicología Conductual* [en línea]. 2018. vol. 26. núm. 2, pp. 243-262. [consulta: enero de 2020]. ISSN 1132-9483. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6545149

VÁZQUEZ CUETO, M. J, y GUTIÉRREZ LÓPEZ, F., << ¿Está justificada la mala imagen de la administración de justicia española? ¿es un problema de inversión?: una comparativa europea mediante el análisis DEA>>. *Revista De Estudios Empresariales. Segunda Época*, [en línea]. 2017. núm. 2, pp. 28-47. [consulta: diciembre de 2019] Disponible en: https://doi.org/10.17561/ree.v0i1.3190

VILLACAMPA ESTIARTE, C. y GOMÉZ ADILLÓN, M.J., <<Nuevas tecnologías y victimización sexual por online grooming>>. *Revista Electrónica de Ciencia Penal y Criminología* [en línea]. 2016, pp. 1-27 [consulta: febrero de 2020]. ISSN 1695-0194. Disponible en: http://criminet.ugr.es/recpc/18/recpc18-02.pdf

VILLACAMPA ESTIARTE, C. y PUJOLS PÉREZ, A., <<El Tratamiento jurídico del stalking desde el prisma de las víctimas y los profesionales implicados: resultados de un análisis cualitativo>>. *Revista de estudios penales y criminológicos, Universidad de Santiago de Compostela*. 2019, vol. 39, pp. 1-57.

VOLPATO, S., << Il fenomeno dello sharenting nel nuovo paradigma dei rapporti genitoriali>>. *Anales de la Facultad de Derecho de la Universidad de la Laguna*. [en línea]. 2016. núm.33. pp. 81-98 [consulta: febrero de 2020]. ISSN 0075-773X. Disponible en: https://www.ull.es/revistas/index.php/derecho/article/view/83

WEULEN KRANENBARG, M., Cyber-offenders versus traditional offenders. An empirical comparison. Director: V. Subramaniam. Vrije Universiteit Amsterdam. Faculteit der Rechtsgeleerdheid. Amsterdam, 2018.

9. FUENTES NORMATIVAS:

Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Boletín Oficial del Estado, 17 de septiembre de 2010, núm. 226, pp.78847 a 78896. Disponible en:

BOE-A-2010-14221

Instrumento de Ratificación del Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, hecho en Estrasburgo el 28 de enero de 2003. Boletín Oficial del Estado, 30 de enero de 2015, núm. 26, pp. 7214 a 7224. Disponible en:

https://www.boe.es/eli/es/ai/2003/01/28/(1)

Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información[17]«DOUE» núm. 69, de 16 de marzo de 2005, pp. 67 a 71, y que ha sido sustituida por la 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 «DOUE» núm. 218, de 14 de agosto de 2013, pp. 8 a 14.

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

https://www.boe.es/doue/2016/119/L00001-00088.pdf

Directiva 2016/1148UE del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (denominada NIS). Diario Oficial de la Unión Europea, de 19 de julio de 2016. Disponible en:

https://www.boe.es/doue/2016/194/L00001-00030.pdf

Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) núm. 526/2013. Diario Oficial de la Unión Europea, de 7 de junio de 2019, núm. 151. Disponible en:

http://data.europa.eu/eli/reg/2019/881/oj

Ley 34/2002, de 11 de julio, sobre Servicios de la Sociedad de la Información y el Comercio Electrónico. Boletín Oficial del Estado, de 12 de julio de 2002, núm. 166, pp. 25388 a 25403. Disponible en:

https://www.boe.es/eli/es/l/2002/07/11/34/con

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a comunicaciones electrónicas e intercambio de información por redes de telecomunicaciones, que supone la incorporación a nuestro derecho de la Directiva 2006/24/CE. Boletín Oficial del Estado, de 19 de octubre de 2007, núm. 251 pp. 42517 a 42523. Disponible en:

https://www.boe.es/buscar/doc.php?id=BOE-A-2007-18243

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. Boletín Oficial del Estado, de BOE», de 10 de mayo de 2014. Núm. 114, pp. 35824 a 35938. Disponible en:

https://www.boe.es/eli/es/l/2014/05/09/9

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, 6 de diciembre de 2018.núm. 294. Disponible en:

https://www.boe.es/eli/es/lo/2018/12/05/3/con

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016. Boletín Oficial del Estado, 8 de septiembre de 2018, núm. 218, pp. 87675 a 87696. Disponible en:

https://www.boe.es/eli/es/rdl/2018/09/07/12

Real Decreto-ley 14/2019 por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Boletín Oficial del Estado, de 5 de noviembre de 2019, núm. 266, pp. 121755 a 121774. Disponible en:

https://www.boe.es/eli/es/rdl/2019/10/31/14/con

Ley Orgánica 10/95 de 23 de noviembre, del Código Penal. Boletín Oficial del Estado, 24 de noviembre de 1995, núm. 281. Disponible en:

https://www.boe.es/eli/es/lo/1995/11/23/10/con

La Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado, 23 de junio de 2010, núm. 152, pp. 54811 a 54883. Disponible en:

https://www.boe.es/eli/es/lo/2010/06/22/5

La Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado, 31 de marzo de 2015, núm. 77, pp. 27061 a 27176. Disponible en:

https://www.boe.es/eli/es/lo/2015/03/30/1

Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Boletín Oficial del Estado, 6 de octubre de 2015, núm. 239, pp. 90192 a 90219. Disponible en:

https://www.boe.es/eli/es/lo/2015/10/05/13

Comunicación de la Comisión de las Comunidades Europeas al Parlamento Europeo, el Consejo y el Comité de las Regiones, de 22 de mayo de 2007. Hacia una política general de lucha contra la ciberdelincuencia. Núm.267 final. Disponible en:

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF

10. OTRAS FUENTES:

Informe de resultados del proyecto saf_e. Cibervictimización y hábitos de uso de las tic e internet de los alumnos de enseñanza no universitaria de castilla y león. CRIMINA, 2018.

Informe Mundial de Drogas: crisis de opioides, abuso de medicamentos y niveles récord de opio y cocaína. UNODOC, 2018.

Informe sobre Ciberamenazas y Tendencias. CCN-CERT IA-13/19, 2019.

11. GLOSARIO:

APT: APT son las siglas del término inglés Advanced Persistent Threat (Amenaza Avanzada Persistente), Se han realizado muchas definiciones de APT pudiendo destacarse la realizada por el National Institute of Standards and Technology (NIST); "amenazas reales sofisticadas (aunque no en todos los casos tienen por qué ser técnicamente complejas) y que afectan a una organización concreta que pertenece a un determinado entorno o sector (industrial, medios de comunicación, etc)".

Ballena azul: Juego en línea, potencialmente peligroso, dañino y autolesivo cuyas reglas han supuesto casos de suicidio entre adolescentes. Su difusión comenzó a través de Internet en el 2016 por medio de la red social rusa Vkontakte.

Bot; Tipo de virus que permite el acceso remoto del sistema informático a través de la Red.

Cybercrime; Delito o actividad ilegal que se realiza utilizando internet.

Ciberespacio: Término que indica el lugar de intercomunicación social transnacional, universal, popularizado y en permanente evolución derivado del uso de las TIC.(Tecnologías de la información y la comunicación).

Cibersuicidio; la Asociación de Investigación, Prevención e Intervención del Suicidio (AIPIS), define cibersuicidio a "la acción de quitarse la vida, motivada por la influencia de páginas web con contenido de ayuda, influencia o motivación para cometer suicidio, salas de chat y foros de internet".

***Darknet*;** Red oscura. Parte "oculta de internet" a la que solo pueden acceder los usuarios que usan un software llamado TOR o "The Onion Router".

Dirección IP; El significado de las siglas IP es Internet Protocol, o protocolo de internet. Este protocolo tiene la función de establecer las comunicaciones entre todos los dispositivos que tratan de relacionarse entre sí en internet. El objetivo de una dirección IP es identificar y localizar de forma inequívoca cada dispositivo en una red interna o externa. Es un número que identifica a una interfaz, que puede ser tanto un ordenador como un smartphone o cualquier otro aparato electrónico que se conecte a internet.

Firewall; Cortafuego. Permite bloquear el acceso no autorizado a un sistema informático.

Facebook; Red social creada en 2004.

Hacking; Cualquier conducta por la cual un sujeto accede a un sistema o equipo informático sin autorización del titular del mismo, de una forma tal que tiene capacidad potencial de utilizarlo o de acceder a cualquier tipo de información que éste en el sistema.

Happy slapping: consiste en la grabación de una agresión física, verbal o sexual y su difusión online mediante las tecnologías digitales (páginas, blogs, chats, redes sociales, etc.). Lo más común es que esta violencia se difunda por alguna red social y, en ocasiones, puede hacerse viral.

Internet; Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Kratom; (Mitragyna speciosa), el Kratom se define como una planta procedente del sudeste asiático que se está popularizando en occidente. Suele utilizarse para aliviar el dolor desde tiempos inmemoriales y que, según sus defensores, es capaz de anular el receptor opioide Kappa del cerebro. Es decir, aunque se consuma una mayor cantidad los efectos siguen siendo los mismos, evitando así la supuesta adicción.

Like; El botón de "me gusta" es una característica del software de comunicación como redes sociales, foros de Internet, blogs y webs de noticias donde los usuarios pueden expresar su opinión, reaccionar o apoyar el contenido.

Malware: *Software* malicioso destinado a dañar, controlar o modificar un sistema informático.

Nativos digitales; Término acuñado para referirse a la generación nacida con la implantación total de Internet.

Online grooming: Acercamiento sexual a menores con el propósito de realizar posteriormente un contacto o abuso sexual.

Online hate speech: Termino para referirse a la difusión de mensajes de odio racial en el ciberespacio.

Pepa Pig; serie infantil de dibujos animados creada por Neville Astley y Mark Baker. Fue estrenada el 31 de mayo de 2004 en el canal británico Channel 5. En España se emite desde 2010 por Clan.

Redes Sociales: Web que permite la relación de personas en el ciberespacio.

Ramsés: Internet Forensic platform for tracking the money flow of financially-motivated malware (Plataforma para facilitar la investigación forense con el objetivo de analizar malware en el entorno financiero).

Scriptkiddies; Jóvenes que, no siendo expertos hackers capaces de acceder a sistemas mediante programaciones propias, realizan sus ataques informáticos, generalmente eligiendo las víctimas al

azar, aprovechando programas y *scripts* básicos y causando daños en muchos casos, más fruto de su impericia o del *malware* utilizado, que de sus propias habilidades.

Sexting: Tipo de online grooming. Consiste en la realización, por parte de menores, de fotografías propias de desnudos completos o de partes desnudas y su envío, generalmente por medio del teléfono móvil, a otros, junto con textos obscenos y con la finalidad de conocer personas o de enviar mensajes de amor o de odio.

Sharenting o oversharing: se produce cuando los padres publican y comparten en las redes sociales, de forma profusa, información e imágenes de sus hijos cuando son menores de edad.

Skipe: Programa que permite la comunicación de texto, audio y vídeo a través de Internet.

Smartphone; teléfono móvil diseñado para permitir a usuario la instalación de aplicaciones y el acceso a Internet.

SMS (Short Message Service): Mensajes cortos de texto.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Software libre: se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software.

Spam: *E-mail* no solicitado que suele enviarse a múltiples direcciones electrónicas bien a través de una dirección electrónica de las ofrecidas por los servicios de correo gratuitos estilo Hotmail, o bien desde un sistema informático infectado, convertido en *botnet* y utilizado por el *spammer* que adquiere las direcciones de correo *hackeando* sistemas informáticos o utilizando *spyware* u otros sistemas de búsqueda de direcciones electrónicas a través de la Red.

Stalking: Acoso continuado a una persona con permanentes solicitudes de contacto que son continuadamente rechazadas por la víctima.

TIC: Tecnologías de la Información y la Comunicación.

Tik Tok: es una red social utilizada principalmente por adolescentes que permite realizar, editar y publicar videos de hasta 60 segundos de duración.

Twitter: Red social que permite a los usuarios enviar y recibir mensajes de hasta 140 caracteres, conocidos como *tweets.*

Web 2.0: Término asociado a aplicaciones web centradas en el usuario, de tal modo, que le permiten compartir información, interaccionar y colaborar con otros internautas creando una comunidad

virtual, a diferencia de la web estática en la que los usuarios se limitan a ser receptores de los contenidos creados para ellos.

Whaling: Modalidad de phis*hing* en la que se ataca a los empleados de alto nivel de grandes empresas o gobiernos.

Whatsapp: Sistema de mensajería instantánea para los teléfonos móviles de última generación.

Wifi: Tecnología de comunicación inalámbrica.

12. ÍNDICE DE TABLAS: