LA RAZÓN HISTÓRICA. Revista hispanoamericana de Historia de las Ideas. ISSN 1989-2659

Número 44, Año 2019, páginas 153-173 www.revistalarazonhistorica.com

Ciberdelincuencia. Aproximación criminológica de los delitos en la red.

Jesús Francisco Espinosa Sánchez.

Universidad de Murcia (España).

Resumen: La aparición de las TIC (Tecnologías de la Información y Comunicación) en nuestra sociedad, ha provocado la creación de una extensa y vasta red de comunicación que interconecta a personas y países entre sí, facilitando la difusión de su cultura y su forma de vida. Además de esto, la tecnología ha contribuido, en grado sumo, a la transformación y modernización de la industria y de las instituciones, alterando, casi por completo, nuestra forma de entender la vida, haciéndonos, en el proceso, dependientes de ella. Sin embargo, aunque la evolución de la sociedad a las nuevas tecnologías ha sido algo positivo, son muchas las incógnitas e incertidumbres que ésta suscita, sobre todo tras la aparición de internet, donde el ciberespacio se ha convertido en el coto de caza perfecto para una nueva forma de criminalidad; la ciberdelincuencia. Este artículo, pretende dar a conocer este tipo de delincuencia, así como enumerar las diferentes medidas que se están llevando a cabo en la actualidad para su lucha, todo ello, con el apoyo de datos empíricos y textos científicos, tomando como base la ciencia criminológica.

Palabras clave: ciberdelito, hacker, sistema informático, criminología, regulación.

Abstract: The emergence of TIC (Information and Communication Technologies) in our society has led to the creation of a vast and vast communication network that interconnects people and countries with each other, facilitating the dissemination of their culture and way of life. In addition to this, technology has contributed to the transformation and modernization of industry and institutions, altering almost completely, our way of understanding life, making us dependent on it in the process. However, although the evolution from society to new technologies has been a positive thing, there are many unknowns and uncertainties that it raises, especially after the

emergence of the internet, where cyberspace has become the perfect hunting ground for a new form of criminality; cybercrime. This article aims to make known this type of crime, as well as to list the different measures that are currently being taken for its fight, all with the support of empirical data and scientific texts, based on criminological science.

Keywords: cybercrime, hacker, computer system, criminology, regulation.

Introducción.

"*Como el mundo está cada vez más interconectado,*

todos comparten la responsabilidad de asegurar

el ciberespacio". Newton Lee

En la actualidad, la aparición de las TIC (Tecnologías de la Información y Comunicación) ha provocado una creciente incertidumbre a la hora de compartir metadatos e información en la red. Debido a esta inquietud (muy común en las sociedades desarrolladas), son muchos los países en los que, en sus ordenamientos jurídicos, regulan los protocolos y políticas de seguridad que se han de llevar a cabo para controlar el flujo de información en internet. Para lograr esta meta, se ha creado todo un entramado jurídico a fin de proteger, tanto los derechos más fundamentales de los que goza el ciudadano, como los intereses del sector público y privado en materia de confidencialidad y seguridad, tanto a nivel estatal como empresarial. Este tema está a la orden del día, puesto que, en los últimos años, se le está reconociendo una gran importancia, tal es esta relevancia, que muchas de las leyes que velan por la seguridad de los internautas han sido cambiadas para que este terreno se vea mejorado y más seguro.

En relación con lo expuesto anteriormente, la amenaza de la ciberdelincuencia está presente en todas las manifestaciones de la vida cotidiana, tanto en el ámbito público como en el privado. Como expondré a lo largo del artículo, son amplias y diversas las naturalezas de los crímenes perpetrados a través de la red, destacando: delitos de índole sexual, económica, política, ciberacoso o "bullying", etc. Además, el avance tecnológico ha supuesto la creación de dispositivos portátiles con una mayor manejabilidad y una mayor red de trasmisión de datos a alta velocidad, lo que aumenta, de manera exponencial, el riesgo de sufrir ataques de origen informático.

En definitiva, la tecnología progresa a la par que avanza la sociedad, razón por la cual, resulta imprescindible la creación de programas y métodos capaces de contrarrestar la creciente oleada de delincuencia que opera a través de la red. Esto lo conseguiremos, como comentábamos anteriormente, a través de programas capaces de penetrar a en los sistemas de seguridad del ordenador, como son el malware, spyware, adware, entre otros.

Para prevenir este tipo de actos ilícitos, se ha constituido el concepto de ciberseguridad, entendido éste, como "el uso seguro y responsable de la tecnología de la información y comunicación (TIC), incluyendo internet, los dispositivos móviles y de comunicación y los instrumentos tecnológicos diseñados para guardar, compartir o recibir información, por ejemplo, los teléfonos móviles, las cámaras digitales, etc."

1. Concepto de ciberdelito.

El concepto de ciberdelito, parte de la denominación anglosajona "computer crime", término acuñado por diversos autores a finales de los años 80. En referencia a la definición de delito informático, De Urbano Castrillo (2011) señala:

> *se trata de un tipo de delito, ya sea tradicional o propio de la sociedad de la información, propiciado por las tecnologías que ésta aporta. El Convenio de Budapest ofrece un concepto basado tanto en la utilización de determinadas técnicas y modos de proceder informáticos …, como en ciertos contenidos cuya vulneración se ve facilitado por el medio Internet. (p.18)*

El autor, una vez ha delimitado el concepto de ciberdelito, diferencia entre dos tipos de delitos informáticos. Por un lado, se encuentran los delitos clásicos, los cuales, se cometen a través de internet (amenazas, ciberterrorismo, delitos contra la libertad sexual…); por otro lado, se encuentran los delitos "strictu sensu" que son aquellos que prevén la intrusión en equipos o la captación de información, fraudes, etc.

Otro concepto de ciberdelito, es el que hace Carlos Sarzana. En su obra Criminalitá e Tecnología, señala que los crímenes informáticos comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

Partiendo de ambos conceptos, podemos definir el ciberdelito como aquellos actos ilícitos que, valiéndose de las ventajas surgidas de la revolución tecnológica, consiguen penetrar en las defensas de los sistemas informáticos, provocando la vulneración de éstos, y dando lugar a una pluralidad de delitos que pueden variar en su esencia delictiva. Hechos que afectan a la intimidad, a los recursos y hasta los negocios de los usuarios, y que, en algunos casos, como en el de las descargas ilegales, se convierten en prácticas toleradas por gran parte de la comunidad (Fernández Riquelme, 2017). Entre sus características, destacan las siguientes:

- Son delitos difíciles de demostrar, debido a la complejidad que entraña la recolección de pruebas.
- Son actos que pueden llevarse a cabo de forma rauda y simple. En algunas ocasiones, estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático, sin que sea necesario que la persona se encuentre presente en el lugar de los hechos.

- Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de las mismos.

Con la aparición del ciberespacio, el hábitat delictivo ha crecido exponencialmente, pues la era de la información multiplica las oportunidades de los delincuentes (Pons, 2017). Debido a ello, se aprobaron, a nivel general, diversos preceptos o compendio de leyes como el "Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos" de 1977, la cual precede al "Convenio sobre el Cibercrimen" que fue aprobado en Budapest hace casi dos décadas atrás. A nivel nacional, el legislador ha optado por regular la ciberdelincuencia en el propio Código Penal, sin considerar la opción de crear una Ley Penal especial. Por ello, dicho Código Penal fue reformado en el año 2010 para introducir nuevos tipos delictivos, así como, reformar algunos de los ya existentes, como son la estafa informática, el "hacking" o daños informáticos.

2. Naturaleza de los delitos informáticos.

Las manifestaciones de este tipo de delincuencia, pueden variar tanto en su naturaleza delictiva, como en los medios utilizados para su ejecución. La facilidad de su comisión, unido a su accesibilidad, hacen de este tipo de delitos un peligroso cóctel para aquellas personas que cometen estos actos bajo el velo del anonimato, lo que les permite reducir drásticamente el riesgo de ser atrapados. Así pues, existen múltiples clasificaciones en torno a los delitos informáticos. Una de estas clasificaciones, es la constituida por la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional Española. Según esta clasificación, la tipología de los ciberdelitos es la siguiente:

- Ataques que se producen contra el derecho a la intimidad. En esta categoría, se encuentran aquellos delitos de revelación de secretos, mediante el apoderamiento y la difusión de datos sensibles registrados en ficheros y soportes informáticos.
- Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor. Se consideran infracciones a la Propiedad Intelectual la copia y distribución, no autorizada, de material informático o audiovisual.
- Falsedades. Falsificación de tarjetas de crédito o débito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad.
- Sabotajes informáticos. Delitos de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos, contenidos en redes o sistemas informáticos. Dentro de esta categoría destacan los siguientes métodos ilícitos:
    1. Malware. El concepto de malware, hace alusión a cualquier tipo de software malicioso que trata de infectar un sistema informático (ordenador) o un dispositivo móvil (smartphone). La finalidad del malware, es sustraer dinero del usuario ilegalmente. Para llevar a cabo esta tarea, el malware puede robar, cifrar o borrar datos,

alterar o secuestrar funciones básicas del ordenador y espiar su actividad en este sin el conocimiento o permiso del usuario.

2. Keylogger. "Keylogger" es el término utilizado para definir a un tipo de amenaza informática cuya función consiste en registrar las pulsaciones del teclado. Este tipo de malware, habitualmente, guarda un log con todo lo que escribimos y lo envía a un servidor controlado por piratas informáticos. A través de este método, los ciberdelincuentes son capaces de analizar el log, pudiendo obtener datos bancarios y contraseñas de distintas webs, entre otros. Una vez obtenida la información, esta es vendida en la Deep Web.
3. Spyware. Es un software capaz de recopilar información de un ordenador, para, seguidamente, trasmitir dicha información a una entidad externa sin el conocimiento o permiso del usuario. Su funcionamiento es igual al de un parásito. El software se instala en el sistema afectado, de forma que se ejecuta cada vez que se inicia el ordenador.
4. Troyanos. Los troyanos son un tipo de malware capaz de camuflarse como software legítimo. Una vez penetrado en el sistema operativo, es capaz de dotar al ciberdelincuente de pleno control sobre el ordenador de la víctima, pudiéndolo espiar, robarle datos confidenciales, eliminarlos, bloquearlos, copiarlos o modificarlos.
5. Virus. Programas que, una vez son ejecutados, infectan diversas partes del ordenador, ya sean procesos u otros programas, trastocando su funcionamiento a través de una pluralidad de formas. En el peor de los casos, los virus pueden terminar dañando gravemente el sistema operativo del ordenador.
6. Adware. El término "Adware", hace referencia a aquellos programas que son fundamentalmente publicidad, y que suelen instalarse en los navegadores de los sistemas operativos. Este tipo de software, es menos nocivo que los anteriores, aunque puede llegar a afectar el rendimiento del procesador con su excesivo spam.
7. Ransonware. El malware de rescate o ransonware, es un tipo de malware que impide a los usuarios acceder a su sistema o sus archivos personales. Una vez el "hacker" consigue bloquear el sistema, pide un rescate a las víctimas a cambio de que puedan acceder nuevamente a sus archivos personales. Uno de los métodos más comunes en la actualidad, es a través de spam malicioso, o malspam, que son mensajes no solicitados que se utilizan para enviar malware por email. Las victimas más habituales de estos actos ilícitos suelen ser empresas o grandes multinacionales, debido al gran capital económico que poseen.

- Fraudes informáticos. Los fraudes informáticos son aquellos delitos que buscan un beneficio económico por medio de la estafa.

- Amenazas. Realizadas por cualquier medio de difusión.
- Calumnias e injurias. Atentados contra el honor consistentes en la divulgación de información falsa a través de los canales establecidos.
- Pornografía Infantil. En esta categoría, se encuentran aquellos delitos relativos a la representación visual, gráfica o textual que, de manera real o simulada, explícita o sugerida, involucren la participación de niños o adolescentes en el desarrollo de actividades de carácter sexual. Dentro de esta categoría delictiva se encuentran:
    i. Grooming: Su conceptualización parte del conjunto de estrategias que una persona, mayor de edad, desarrolla para ganarse la confianza de un menor por medio de Internet, con el fin de obtener concesiones de índole sexual. Hablamos entonces de acoso sexual a menores en la Red, y el término completo sería child grooming. El modus operandi del agresor, se basa en un acercamiento lleno de empatía y/o engaños, pasando al chantaje más cruento a fin de conseguir imágenes comprometedoras de la víctima y, en casos extremos, pretender un encuentro en persona.
    ii. Sexting: El término "Sexting" hace alusión al envío de material audiovisual de contenido sexual y erótico a través de aplicaciones de mensajería instantánea, como WhatsApp, Telegram, etc. Entre sus características destacan:
    Voluntariedad: El material audiovisual es creado y difundido conscientemente por sus protagonistas.
    Carácter sexual: Los contenidos tienen una clara connotación sexual: desnudez o semidesnudez, así como muestra o descripción de actividades sexuales.
    Uso de dispositivos tecnológicos. La difusión y realización de imágenes o videos de contenido sexual admite una generalidad de medios. Entre estos medios destacan: smartphones, ordenador tanto de sobremesa como portátil, tablet, etc.

3. Ciberbullying

El término "ciberbullying" o ciberacoso, hace referencia al uso de redes sociales (Facebook, grupo de WhatsApp, etc.) para acosar a una persona o grupo de personas, mediante ataques personales, divulgación de información confidencial o falsa, entre otros medios. En aras de conseguir una mayor aproximación a la conceptualización de este tipo de delincuencia Calvete, Orué, Estévez, Villardón y Padilla (2010) definen este fenómeno como:

> *la utilización de nuevas formas de agresión basadas en la tecnología: abuso deliberado y frecuente con algún tipo de texto electrónico, imagen o video a través del teléfono móvil, email, chats u otros espacios online como redes sociales, blogs, foros, etc.*

Las conductas antisociales asociadas a este tipo de delincuencia, suelen consistir en: 1) enviar amenazas, insultos, imágenes humillantes, etc.; 2) escribir o enviar enlaces con bromas, rumores o comentarios injuriosos; 3) obtener contraseñas de otras personas, para posteriormente, hacerse pasar por éstas; 4) grabar la humillación de otra persona, difundiendo el material audiovisual a su grupo; 5) grabar la agresión a otra persona y enviar las imágenes o el video del ataque; 6) hacer pública la información sensible o comprometedora de la víctima; 7) excluir deliberadamente a alguien de las redes sociales, chats o foros. Entre las diferencias más significativas existentes entre bullying y ciberbullying, destacan las siguientes:

1. Existe una mayor especialización tecnológica.
2. Este tipo de delincuencia se nutre de formas de agresión más indirectas. El agresor para llevar a cabo la conducta ilícita no necesita estar de forma presencial ante la víctima.
3. A causa de lo anterior, no se percibe la directamente la reacción de la víctima.
4. Al cometerse en el ciberespacio, su difusión y alcance es mayor, por lo tanto, la víctima queda desamparada debido a las dificultades para escapar de esa situación.

4. Ciberdelitos de índole económica.

Llamamos ciberdelitos de carácter económico, a aquellos delitos cuyo fin último es la obtención de una recompensa pecuniaria, a través de diversas herramientas online que varían en función y modo de ejecución. El sector privado y, por ende, las grandes multinacionales, así como las medianas y pequeñas empresas (PYMES), se constituyen como los principales focos de acción de dichas acciones ilícitas, debido, en gran parte, a su poder económico. Por ello, es de vital importancia para la seguridad de sus sistemas, así como la salvaguarda de los datos de sus clientes, la implantación de métodos capaces de identificar, bloquear y neutralizar cualquier amenaza que pueda llegar a afectar a sus sistemas.

Entre las principales amenazas que puedan surgir en las empresas, destacan las siguientes:

1. Accesos no autorizados. Aquellas acciones que buscan el acceso no permitido a ficheros, bases de datos, o a las redes de sistemas ajenos.
2. Interceptación de las comunicaciones. Son aquellas acciones que. por medio de programas maliciosos, logran interceptar mensajes de correo electrónico, conversaciones escritas u orales a través de servicios de mensajería instantánea, remisión o intercambio de documentos, etc.…
3. Manipulaciones de datos o sistemas informáticos.
4. Interferencias dañosas o inutilizadoras de sistemas informáticos. Difusión de malware a través de la red, a fin de sabotear e inutilizar los servidores donde se encuentran alojadas las páginas webs de las entidades privadas

(ciberterrorismo), provocando en el proceso, un grave perjuicio a estas últimas, debido al colapso y posterior paralización de su actividad comercial/empresarial.

5. Copia e intercambio de obras de creación intelectual. Dícese, la reproducción e intercambio de obras de creación intelectual de todo tipo, infringiendo los derechos de autor con fines comerciales, lo que comúnmente se denomina "piratería informática". Las victimas más potenciales de este tipo de acciones ilícitas, suelen ser aquellas empresas que crean contenido audiovisual (productoras de cine) y musical (discográficas).

Con el surgimiento de las nuevas tecnologías, el mercado financiero también ha sufrido un grave impacto. Generalmente, la acción de atacar a los sistemas informáticos de una empresa, va siempre dirigido contra la información que esta maneja; esta información va desde datos de proyectos, claves, usuarios y todo lo que sirva para crear estrategias de mercado. Para combatir dichas amenazas, han ido surgiendo, a lo largo de los años, diversas iniciativas a nivel privado consistentes en ofrecer una serie de servicios y recursos, para procurar una protección integral para las empresas en materia de ciberseguridad. Para llevar a cabo esta labor, las empresas de ciberseguridad, se especializan en la detección y posterior actuación ante el evento. Cabe mencionar también, a aquellas organizaciones privadas que dan como prioridad el conocimiento en la ejecución de la amenaza, la autoría de la acción y como se logró llevarla a cabo.

En la actualidad, se están promoviendo diversas plataformas web gratuitas (de iniciativa privada y contenido público) en materia de prevención y respuesta ante amenazas. Un ejemplo claro de esto, lo encontramos en la plataforma comunitaria OTX (Open Threat Exchange). A través de ella, se permite a los expertos en seguridad investigar de forma colaborativa nuevas amenazas que puedan surgir en la red, comparando los datos de diversas fuentes para, más tarde, integrar esa información en sus respectivos sistemas de seguridad. A día de hoy, dicha plataforma cuenta con más de 80.000 profesionales repartidos en más de 140 países, que participan cada día en alimentar una gran base de datos pública en materia de ciberseguridad.

5. La sociedad y el delito informático.

El progreso tecnológico, ha hecho posible que, cada día, contemos con más y mejores herramientas con las que acceder a contenidos informativos, transmitir datos e imágenes, comunicarnos y relacionarnos con otras personas. Estos avances, se traducen en una mayor interconexión entre diferentes países, facilitando así, un mayor intercambio de información y una mayor difusión entre culturas a escala global. De este modo, internet se constituyó como una herramienta de globalización, derribando las barreras entre los países que conforman el globo terráqueo.

Las numerosas ventajas que ofrecen las TIC, nos ayudan a comprender porque se han convertido en objetos cotidianos, casi imprescindibles, en nuestro día a día. En el año 2015, el Centro de Investigaciones Sociológicas (CIS), ponía de relieve la necesidad en el uso de herramientas tecnológicas (teléfonos móviles, la conexión a Internet, etc.) por parte de la sociedad y, más específicamente, por parte del segmento joven de la población. En la siguiente tabla, se puede observar dicha necesidad:

	Muy necesario	Bastante necesario	Poco necesario	Nada necesario	N.S/N.C
Teléfono móvil	57,5	32,5	9,4	0,5	--
Conexión a Internet	55,7	34,9	6,6	2,8	--
Mensajería instantánea (WhatsApp, …)	43,4	35,8	16,0	4,7	--
Ordenador personal (PC, portátil)	39,6	39,6	15,6	5,2	--
Correo electrónico	33,5	42,9	18,9	4,2	0,5
Redes sociales virtuales	19,8	30,7	38,2	11,3	--
Tablets (iPad, e-book, etc.)	14,6	18,9	37,7	27,4	1,4

FUENTE: Barómetro de marzo de 2015. Estudio nº3057. Centro de Investigaciones Sociológicas.

La globalización, como proceso económico, tecnológico, político, social y cultural, a escala global, ha contribuido, de forma significativa, a la mejora de la calidad de vida de la sociedad actual. El avance tecnológico, ha llevado aparejado un sinfín de beneficios: avances económicos, de comunicación, culturales y ha facilitado el acceso y la distribución de la información a tiempo real. En contraposición, este avance también ha puesto en riesgo los derechos a la intimidad y a la libertad de los individuos, así como a la seguridad de los sistemas informáticos, entre otras desventajas. Asimismo, la proliferación de los delitos informáticos, ha contribuido a que la sociedad del siglo XXI, sea cada vez más escéptica a la utilización de las nuevas tecnologías de la información y comunicación.

La falta de seguridad en el ciberespacio deteriora gravemente la confianza entre la comunidad TIC que está sufriendo una de las revoluciones más importantes en la historia de la humanidad; la seguridad y la prosperidad de cualquier país está conectada a la protección de las redes TIC, a través de las cuales la población puede ejercer sus libertades de expresión, asociación e información (Carlini, 2016). Por ello, es de vital importancia, la incorporación de políticas de seguridad de calado, a fin de mejorar los sistemas de seguridad públicos y privados para garantizar un acceso seguro a sus redes de información.

6. Perfil del ciberdelincuente

El perfil del ciberdelincuente, suele atribuirse al individuo que posee un dominio del medio informático, sin que ello lleve aparejado estar relacionado con una clase social o un segmento de la población en específico. A este respecto, la concreción del perfil del delincuente informático, ha sufrido, a lo largo de los años, una transformación. Tradicionalmente, se consideraban autores de delitos

informáticos al colectivo de jóvenes (de clase media) obsesionados por el medio o personas adultas que, en el ejercicio de su actividad profesional, poseían la destreza y los conocimientos necesarios para cometer dichos actos. Según datos ofrecidos por Digiware, proveedor experto en la generación de estrategias integrales en seguridad de la información de Latinoamérica, aproximadamente el 76% de los ciberdelincuentes son hombres, cuyas edades oscilan entre los 14 años (8%) hasta los 50 (11%), situándose la edad media en 35 años (43%). Así, la visión tradicionalista que atribuía la comisión de los delitos cibernéticos a un sector específico de la sociedad, jóvenes, queda opacada a raíz de los datos anteriormente mencionados. Por tanto, y dejando de lado la variable cuantitativa de la edad, el perfil del ciberdelincuente suele ser el de una persona con un coeficiente intelectual medio, que le permita tener conocimientos informáticos, además de poseer un medio informático con el cual tenga acceso a la red para cometer los actos ilícitos. Según el procedimiento con el cual llevan a cabo el ciberdelito, podemos distinguir:

- Hacker. Individuo que, gracias a sus avanzados conocimientos de informática, es capaz de realizar muchas actividades complejas, a la par de ilícitas, desde un ordenador. Tiene una gran capacidad parar dominar diferentes aspectos relacionados con la informática, destacando: lenguajes de programación, manipulación de hardware y software, telecomunicaciones. Entre sus motivaciones, destacan: el ánimo de lucro, hacktivismo, reconocimiento social, etc…Los hackers a su vez se dividen en:
    1. White Hat Hackers. Son aquellos hackers encargados de la seguridad de los sistemas informáticos. Para llevar a cabo esta labor, estudian y fortalecen los fallos de seguridad que se produzcan en los servidores.
    2. Gray Hat Hackers. Son aquellos hackers que usan sus conocimientos y habilidades para traspasar los niveles de seguridad, para, más tarde, ofrecer sus servicios como administradores de seguridad informática, a fin de corregir dichos fallos.
    3. Black Hat Hackers. Este colectivo constituiría la conceptualización del hacker clásico. Los Black Hat Hackers o sombreros negros, son aquellos individuos cuya actividad, consiste en vulnerar la seguridad de los sistemas, violentar y extraer información de manera ilícita, además de crear una pluralidad de malware para lograr sus fines.
    4. Newbie o Novato. Este sector, lo conforman aquellos individuos que quieren llegar a ser hackers pero que, sin embargo, carecen de los conocimientos técnicos necesarios para convertirse en uno, por lo que, para lograr su objetivo se valen de tutoriales, sitios sobre hacking, software diseñado, etc.
- Cracker. El cracker, es un tipo de hacker cuya actividad consiste en violentar el software original, extendiendo en el proceso, su funcionalidad.

Se relacionan en grupos relativamente pequeños y muy secretos, donde es difícil entrar. El cracker, contribuye a la piratería de software, provocando que programas que son de pago, pasen a ser gratuitos mediante la alteración de sus archivos. Para ello, usan software propio, creado para sus fines. Este software, suele consistir en programas capaces de desbloquear claves de acceso, así como, generadores de contraseñas (KeyGen).

- Phreaker. Tipo de hacker encargado de las telecomunicaciones, móviles, voz sobre IP, etc. Su trabajo, consiste en penetrar en los sistemas telefónicos para obtener privilegios no accesibles de forma legal. Los Phreakers, son capaces de construir equipos artesanales que interceptan llamadas, o que realizan llamadas desde terminales ajenos, sin que los dueños de los mismos se percaten de ello. La motivación de estos hackers, es meramente económica, siendo las compañías telefónicas y las grandes multinacionales las principales víctimas de este tipo de ciberdelincuencia.
- Viruckers. La acción delictiva de este tipo de hackers, consiste en la intrusión en un sistema informático para alojar virus en el mismo, con el objetivo de destruir, alterar y/o inutilizar la información almacenada en él. Existen dos tipos de virus:
    1. Benignos, que molestan, pero no causan daño alguno.
    2. Malignos, que destruyen la información o inutilizan el sistema.

  En cuanto a su modus operandi, este colectivo suele actuar de forma individual y aislada, sin que exista un código moral o ético que marque su comportamiento, de ahí su peligrosidad.

Por consiguiente, para la persecución y detención de este tipo de delincuentes, es de suma importancia, que una ciencia tan necesaria como es la Criminología, sea capaz de renovarse y adaptarse a los cambios surgidos en la sociedad que la era tecnológica ha contribuido a transformar, en pos de una mayor y mejor aproximación a su objeto de estudio, tal y como señalan José Luis de la Cuesta Arzamendi y Ana Isabel Pérez Machío (2010):

> *En efecto, mientras la Criminología clásica y tradicionalista ha venido destacando los aspectos sociales, económicos y culturales como determinantes para la compresión de una específica delincuencia, fundamentada en el fenómeno de la exclusión social, la complejidad del cibercrimen rompe con esta forma de entender y de explicar el fenómeno criminal. (p.101)*

7. Perfil de la cibervíctima.

La ciberdelincuencia, presenta la particularidad de afectar a una generalidad de agentes sociales, desde entidades privadas, hasta instituciones y organismos públicos. Dado que cualquier entidad o individuo interactúa con el ciberespacio, tanto en el terreno económico como en el social o personal, la probabilidad de ser susceptible a ataques cibernéticos, aumenta de forma considerable. A este

respecto, los usuarios privados, se constituyen como las víctimas potenciales que más vulnerables se encuentran ante el cibercrimen, tanto desde una perspectiva cuantitativa, debido a la enorme cantidad de individuos que hacen uso de sus ordenadores privados, como desde una perspectiva cualitativa, a causa del uso del ciberespacio por parte de usuarios particulares, sin seguir las reglas básicas de seguridad informáticas, tales como la instalación de software de protección (antivirus, antimalware, Etc.), como el acceso a páginas webs de dudosa seguridad. Cabe mencionar, por otra parte, al colectivo de personas mayores que, careciendo de unos conocimientos básicos en el uso de las nuevas tecnologías, puedan ser víctimas de delitos informáticos de índole económica.

Las víctimas del cibercrimen, varían en edad y condición social, desde personas mayores de edad, como menores, personas con un gran poder adquisitivo, como personas con menos recursos, económicamente hablando. Si bien las variables de edad y condición social son factores a tener en cuenta, a la hora de crear un perfil victimológico en referencia a los delitos informáticos, será la propia actividad que realicen los usuarios en la red, lo que determinará la aparición de riesgos asociados a esta actividad delictiva. En otras palabras, y como han señalado Pratt, Holfreter y Reisig, lo relevante no son tanto los datos demográficos, como el actuar de la víctima para la configuración del ámbito de riesgo. Por tanto, no se está ante una conducta neutral; en el sentido que no genera consecuencias, sino por el contrario, su comportamiento influye en la estructura, en la dinámica y en la prevención del delito.

8. Situación de los ciberdelitos en España

En nuestro país, a lo largo de los años, se han ido estableciendo, poco a poco, una serie de políticas de seguridad públicas de cara a la protección de las redes informáticas de la Administración General del Estado frente a los ataques, así como, la creación de un marco jurídico de protección a las entidades privadas. Según datos obtenidos del Sistema Estadístico de Criminalidad (SEC), en el periodo comprendido entre 2014 y 2017, hubo un aumento de los delitos informáticos. Dichos datos establecen que, en 2017, ha habido un total de 81.307 delitos, lo que supone un 22,1% más con respecto al año anterior. De esta cantidad, el 74,4% corresponde a fraudes informáticos y el 13,9% a amenazas y coacciones. En el siguiente gráfico, se puede apreciar la tipología delictiva de los delitos informáticos del año 2017:

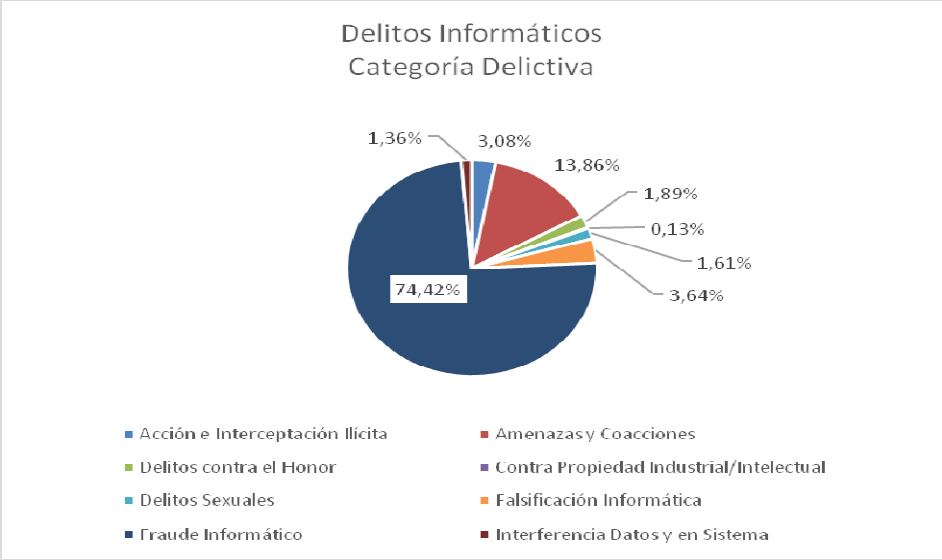

Figura 1. Gráfico propio realizado a partir de datos oficiales.

En 2017, las victimizaciones que han sido registradas por las FCSE (Fuerzas y Cuerpos de la Seguridad del Estado) suman un total de 62.419, es decir, un 14,64% más que en el año 2016. La mayoría de las víctimas de ciberdelincuencia, corresponden al sexo masculino (54,5%). En cuanto a la edad, ésta se sitúa entre los 26 y 40 años, y son objeto de los siguientes delitos: delitos de fraude informático, amenazas y coacciones y acceso e interceptación ilícita. No obstante, si se analiza la distribución global de sucesos conocidos por ámbito y sexo, las mujeres sobrepasan en porcentaje a las víctimas del sexo masculino cuando se trata de delitos relacionados con el acceso e interceptación ilícita, delitos contra el honor, los delitos sexuales y falsificación informática.

A pesar de los datos expuestos en el párrafo anterior, varios informes realizados por organismos públicos revelan que, a pesar de los incidentes de seguridad sufridos, la confianza depositada por los usuarios de Internet continúa recuperándose. Según estos informes, el 43,1% de los usuarios encuestados, confía bastante o mucho en internet, y un 46,4% lo percibe como más seguro cada día, gracias, en parte, a las regulaciones tanto a nivel nacional como europeo en materia de privacidad y protección de datos. Estas reglamentaciones, se clasifican dicotómicamente según su nivel de actuación en dos ámbitos bien diferenciados. Estos dos ámbitos, lo constituyen, por un lado, el ámbito privado y, por otro lado, el ámbito público, los cuales, pasaré a desarrollar a continuación.

9. Ciberseguridad en el ámbito privado.

La irrupción de Internet en nuestras vidas, ha generado una gran incertidumbre y, a la vez, una gran oportunidad para las empresas a la hora de expandirse y dar publicidad a sus productos. Como afirman Nieva Machín y Manuel Gazapo (2016,

p.48) “Internet se ha convertido, sin duda alguna, en un elemento clave para el crecimiento económico”. Sin embargo, esta densa de red de transmisión de información, ha dado lugar al surgimiento de individuos denominados “hackers”, capaces de acceder a información sensible a través de ataques cibernéticos.

Entendemos ataques cibernéticos, como aquellos actos que buscan o bien desestabilizar o colapsar una red, o bien, acceder a un tipo de información sensible que pueda afectar tanto a un interés público (gobiernos, administración pública, …) como privado (pymes, multinacionales, …), a fin de conseguir un beneficio económico o político. Bajo estas premisas, en este apartado, analizaré, tanto las medidas de ciberseguridad que la nueva normativa europea y española obliga a las empresas en el ámbito privado, como las consecuencias que puede acarrear para los intereses de este sector, el acceso exitoso a su red de información.

10. Legislación española en materia de ciberseguridad.

10.1 Regulación europea de protección de datos

El reglamento general de protección de datos, promulgada por la UE, e integrada en el ordenamiento jurídico de nuestro país, entró en vigor el 25 de mayo de 2016 y fue aplicado dos años más tarde. Este compendio de leyes, regula todo lo relativo a la protección de las personas físicas, en referencia al tratamiento de sus datos personales y a la libre circulación de estos datos en la red. Sin embargo, y como es lógico, este reglamento no se aplica a personas fallecidas ni jurídicas, además, tampoco se aplica cuando el tratamiento de esos datos es efectuado por una persona que actúa con fines ajenos a sus actividades comerciales, empresariales o profesionales. El objetivo de este marco regulatorio, radica en otorgar a las empresas, tanto multinacionales, como pymes la flexibilidad, lo que necesitan para hacer uso de las nuevas tecnologías, sin que ello lleve aparejado la vulneración de los derechos más fundamentales de los ciudadanos, como pueden ser los derechos de su esfera personal. Esta regulación, no solo beneficia a las empresas, sino que concede unos determinados derechos que permiten a los ciudadanos ejercer un mayor control sobre sus datos personales. Estos derechos, son los siguientes:

- Derecho a ser informados.
- Derecho de acceder a los datos que les conciernen.
- Derecho a trasladar sus datos personales de un proveedor de servicios a otro.

En consonancia con el párrafo anterior, el tratamiento de los datos personales, que pasan por las diferentes empresas u organizaciones, queda bajo la responsabilidad del delegado de protección de datos. El delegado de protección de datos (DPO), es un perfil de trabajador que tiene la función/responsabilidad de supervisar como se

tratan los datos personales, y de informar y aconsejar a los empleados que tratan los datos sobre sus obligaciones. Este cargo de responsabilidad, puede ser nombrado por la empresa, aunque esta labor puede ser ejercida por alguien externo a ésta. Sin embargo, y a pesar de ser una figura importante de cara a garantizar los derechos de los clientes/consumidores, no todas las organizaciones tendrían que incorporar en su plantilla a este profesional. Este delegado, estará de forma obligatoria en las empresas que reúnan una de las siguientes condiciones:

- Las organizaciones que sean públicas
- Aquellas empresas que, por su actividad empresarial, necesiten manejar grandes cantidades de datos, sin que sea un requisito *per se*, el tamaño de la organización o la cantidad de empleados que ésta tenga.
- Las empresas que operan con datos que son de especial protección (ideología, etnia, orientación sexual, entre otros)
- Entidades que desarrollan el *profilling*. Es decir, aquellos que registren y analicen características psicológicas y de comportamiento de las personas.

El Reglamento general de protección de datos, aplica una legislación estricta para el tratamiento de datos basadas en el consentimiento. El objetivo de estos preceptos, es garantizar que el interesado comprenda lo que está consintiendo. Eso significa, que el consentimiento debe darse de manera libre, de forma concreta, informada y veraz, mediante una solicitud presentada en un lenguaje claro y sencillo. Esta regulación, se promulgó para proteger, en la medida de lo posible, una intromisión, por parte de terceros, a la intimidad de los usuarios que, o bien consumen, o bien contratan los servicios que ofrecen las empresas a través de sus diferentes páginas webs, mediante la implantación de cifrado y sistemas de doble factor de autentificación.

Dentro de este reglamento, se establecen diferentes niveles de cifrado, según la cantidad de metadatos que manejen las diferentes empresas que operan dentro del territorio nacional, así como, aquellas que tengan su sede dentro del continente europeo. En el primer nivel, nos encontramos con los cifrados obligatorios. El establecimiento de este tipo de cifrado, surge de la necesidad de proteger los datos más sensibles o más propensos a ser objeto de ataques en la red. En España, el ejemplo más funcional de esta indicación lo encontramos en la obligatoriedad del cifrado sobre los datos de nivel alto, como, por ejemplo, aquellos datos que afecten a la esfera personal del individuo, tales como la ideología política, las convicciones religiosas o la afiliación sindical.

En el segundo nivel, nos encontramos con el cifrado conveniente. Este tipo de cifrado, se caracteriza por la no necesidad de informar a sus usuarios de una intromisión, provocada por una brecha de seguridad que afecta a sus datos personales, los cuales, son gestionados por la empresa; siempre que éstas últimas

utilicen un sistema de cifrado. En cambio, aquellas empresas que no cifren, están obligadas a informar a los usuarios de los ataques que puedan sufrir, si estos ataques van dirigidos a sus datos personales. En el último nivel de cifrado, nos encontramos con el cifrado voluntario. Este tipo de cifrado, se caracteriza por la no necesidad por parte de las empresas que gestionan y almacenan secretos comerciales, información confidencial o datos disociados, de adoptar medidas de cifrado, mientras que no exista una norma que lo regule. La adopción de medidas de seguridad asociadas a la protección de datos por medio del cifrado, quedaría bajo la voluntariedad de las empresas para, así, aumentar sus niveles de seguridad.

Sin embargo, y a pesar de lo expuesto anteriormente, el reglamento establece la obligación de notificar cualquier brecha de seguridad que se haya producido en sus servidores, por lo que deberán extraer constante sobre los intentos de intrusión y los accesos exitosos no autorizados. La vulneración de esta obligación por parte de las empresas, conllevaría la interposición de sanciones económicas, pudiendo ascender la cuantía de estas sanciones al 4%, como máximo, del volumen de negocio total anual del ejercicio financiero anterior.

10.2 Código de Derecho de Ciberseguridad.

Esta edición, en su actualización más reciente a fecha 30 de abril de 2019, establece una serie de preceptos que fijan las directrices generales del uso seguro del ciberespacio, promoviendo, en sus diferentes artículos, una serie de limitaciones y obligaciones, a fin de regular la libre circulación de metadatos a nivel nacional. Dentro de este código, se encuentra Ley 1/2019 de 20 de febrero, que regula todo lo relativo a la protección de los secretos empresariales, la cual pasaré a desarrollar a continuación.

Esta ley, ubicada en el apartado número 18 dentro de la Normativa sobre Seguridad Nacional, establece una serie de directrices que tienen como objetivo la protección de la información, que abarca, no solo conocimientos técnicos o científicos, sino también datos empresariales, relativos a clientes y proveedores, planes comerciales y estudios o estrategias de mercado. Con la llegada de las nuevas tecnologías, esta información está cada vez más expuesta a prácticas ilícitas que buscan la apropiación indebida de secretos empresariales, como el robo, la copia no autorizada, el espionaje económico o el incumplimiento de requisitos de confidencialidad. La globalización, y por ende, las TICs (Tecnologías de la Información y Comunicación), suponen un gran riesgo a la hora de que se produzcan estas prácticas desleales. Por ello, y para evitar, o al menos paliar de forma eficaz la desincentivación, para emprender actividades asociadas a la innovación, se hace de vital importancia la creación de un marco jurídico legal bien definido, que proteja los intereses del sector privado en materia de confidencialidad y buena praxis profesional.

La ley, se estructura en veinticinco artículos repartidos en cinco capítulos, una disposición transitoria y seis disposiciones. El contenido de los cinco capítulos de los que se compone esta norma es el siguiente:

- El Capítulo I, hace una descripción del objeto de la ley, estableciendo una definición de secreto empresarial conforme a los dictados de la directiva europea.
- El Capítulo II, define, por un lado, las circunstancias en las que la obtención, utilización y revelación de secretos empresariales son considerados lícitos, a ojos de la legalidad vigente. Por otro lado, define aquellas conductas que constituyen una violación del secreto empresarial.
- El Capítulo III, complementa y perfecciona su contenido, abordando la vertiente patrimonial de secreto empresarial.
- El Capítulo IV, se consigna un catálogo abierto de acciones de defensa, que contiene la designación y configuración sustantiva de los más importantes remedios reconocidos al titular del secreto empresarial, para hacer frente a su violación.
- El Capítulo V, por último, regula aquellos aspectos procesales que permiten ofrecer, a los titulares de secretos empresariales, las herramientas efectivas para la tutela judicial de su posición jurídica.

En cuanto a la violación de secretos empresariales, según se especifica en el artículo 3 de esta ley, la apropiación de secretos empresariales, sin consentimiento de su titular, se considera un acto ilícito cuando se lleve a cabo a través del acceso, la obtención de copias no autorizadas u otros archivos/ficheros que contengan el secreto profesional o cualquier otra actuación que, en las circunstancias del hecho, se considere contraria a las prácticas comerciales leales.

Como se puede observar, esta normativa, se crea con el fin inequívoco de la luchar contra aquellos ataques que busquen como fin, el acceso a información o documentación que pueda perjudicar, de manera grave, la confidencialidad de la empresa perjudicada, dotando a éstas, de un régimen jurídico que vele por sus intereses.

10.3 Consecuencias derivadas de las brechas de seguridad.

Las brechas de seguridad que puedan surgir, provocadas por la actividad de uno o varios hackers, pueden derivar en fatales consecuencias, tanto en el ámbito económico como en el terreno comercial de estas organizaciones. Una de las perdidas más notorias por brechas de seguridad sería la económica. La acción de un hacker, puede provocar largas interrupciones en la labor empresarial, generando, en el proceso, la paralización de esta actividad, y perdiendo, por consiguiente, grandes sumas de dinero.

Sin embargo, no todas las consecuencias se limitarían al ámbito económico, sino también a la reputación y el buen hacer de la empresa de cara a sus potenciales clientes, ya que no todos se sienten cómodos a la hora de hacer negocios con una empresa que no da como máxima prioridad la seguridad, perdiendo, en el proceso, la confianza de los mismos y, por tanto, originar un descenso en el número de consumidores que posee dicha organización. También, y como se ha señalado en el primer epígrafe, una brecha de seguridad en los servidores, puede dar lugar a la filtración de los datos personales de sus clientes, tales como el número de las cuentas bancarias o números de la Seguridad Social. Bajo estas circunstancias, el cliente podría interponer una demanda a la empresa por daños y perjuicios.

11. Ciberseguridad en el ámbito público.

La principal prioridad de España en esta materia, es lograr un uso seguro de los sistemas de información y telecomunicación. Para ello, es necesario fortalecer las medidas de prevención, defensa, detección y respuesta a los ciberataques.

Para alcanzar estos objetivos, se debe publicitar un organismo que aglutine y organice a todas las instituciones y agentes encargados de la ciberseguridad, fortaleciéndola en el proceso, y consiguiendo, a su vez, dotar a las administraciones públicas, a la comunidad científica y a los ciudadanos de una mayor confianza en las TICs. Las medidas fundamentales para conseguir los objetivos de ciberseguridad, deben ser análogas a las medidas que han adoptado los países de nuestro entorno. A raíz de esto, el primero de los objetivos principales seria, que los sistemas de información y telecomunicación que utiliza la administración pública tengan el adecuado nivel de ciberseguridad y resiliencia. Para ello, resulta imprescindible potenciar la implantación de un marco nacional, coherente, de políticas y procedimientos que garanticen la protección de la información pública.

Para transformar esto en realidad, es necesario que la administración pública incorpore servicios de seguridad en las mismas. El segundo objetivo principal, sería impulsar la seguridad y fortaleza de los sistemas de información usados por el sector empresarial, en general. Para ello, se debe asegurar la protección del patrimonio tecnológico del país. El tercer objetivo, establece la potenciación de las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente al terrorismo y la delincuencia que encontramos en el ciberespacio. Para lograrlo, es imprescindible que se fortalezca la cooperación judicial y policial internacional, armonizando en el proceso, las legislaciones nacionales. Otro objetivo fundamental, seria sensibilizar a los ciudadanos, profesionales, empresas y administraciones públicas españolas de los riesgos que conlleva operar en el ciberespacio; además de poseer los conocimientos y herramientas necesarias para posibilitar la protección frente a ciberataques.

Las empresas por su parte, deben de ser conscientes de la responsabilidad en la seguridad de sus sistemas, la protección de la información de sus clientes y proveedores, y la confiabilidad de los servicios que prestan. Por consiguiente, es fundamental promover una sólida cultura de ciberseguridad a toda la población española. Como quinto objetivo, se propone alcanzar y mantener los conocimientos, habilidades, experiencias y capacidades tecnológicas, que necesita España para sustentar todos los objetivos de ciberseguridad. Para lograr este objetivo, es necesario fomentar y mantener una actividad de I+D+i en materia de ciberseguridad de manera efectiva. Como último objetivo, se encuentra contribuir a la mejora de la ciberseguridad en el ámbito internacional, para ello, se promoverá y apoyará el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internaciones de Seguridad y Defensa.

Logrando estos objetivos, se alcanzará el objetivo global, que es conseguir que España haga un uso seguro de los sistemas de información y telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta frente a los ciberataques.

La era de la globalización en la que actualmente nos encontramos, ha establecido una situación compleja en nuestra sociedad moderna, de ahí que sea de suma importancia, que las infraestructuras digitales de las instituciones estatales se protejan ante los desafíos que se puedan presentar. Como afirma Aníbal Villalba Fernández, (2015):

> *Esta situación presenta nuevos retos a los que no se sustraen los diferentes actores políticos, principalmente los Estados. Entre estos desafíos se encuentran la protección y recuperación de los sistemas de infraestructuras críticas ante agresiones que utilizan el ciberespacio como entorno y vehículo para interferir en las actividades de los ciudadanos y de las instituciones. (p.8)*

Cada país, posee un nivel diferente cuando hablamos de protección de los activos, los cuales, si fuesen dañados, afectarían de forma directa a la población. Un ejemplo de ello, sería el ataque a suministros de electricidad, agua, combustible, que afectan directamente a la ciudadanía y a la propia seguridad y prosperidad de un país. Debido a lo cual, la prevención, se configura como una tarea decisiva para los profesionales de seguridad del sector público, que deberán revisar y minimizar la exposición a ciertos tipos de amenazas informáticas.

12. Conclusión.

El progreso tecnológico en nuestra sociedad actual, ha contribuido de sobremanera a derribar las fronteras entre países, así como, a la mejora de la calidad de vida de la población. A pesar de ello, son muchas las incertidumbres e incógnitas que su instauración en la vida social suscita, en especial en materia de seguridad. El avance tecnológico, ha supuesto el surgimiento de una nueva forma de criminalidad, denominada ciberdelincuencia, y, con ella, la proliferación de un

sinfín de amenazas que buscan, día a día, la intrusión y posterior vulneración de los sistemas informáticos, ya sean estos públicos o privados. Para combatir dichas amenazas, la Criminología, ha de adaptarse a este nuevo panorama delictivo, dejando de lado teorías tradicionalistas y buscando siempre el análisis objetivo de los hechos a través del método científico.

La labor de esta disciplina, pasa por la prevención, a través del análisis de los factores de protección y de riesgo que entraña la actividad en la red, el estudio de las conductas criminógenas que puedan dar origen a este tipo de delincuencia, así como, la innovación en materia de ciberseguridad, tanto en los medios como en los métodos a utilizar. Como bien señala Eric Schmidt "Es muy difícil identificar la fuente del cibercrimen y detenerla" de ahí, que sea de suma importancia el trabajo conjunto de equipos interdisciplinares para combatir dicha tipología delictiva, con la ciencia criminológica como base y marco asistencial.

Bibliografía.

- Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. IEEE Documento de opinión, 67, 1-16.
- Caro, M. (2010). Alcance y ámbito de la seguridad nacional en el ciberespacio. En Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, 49-82. Cuadernos de estrategia, 147. España: Ministerio de Defensa.
- Centro de Investigaciones Sociológicas (CIS). Estudio nº 3057 "Barómetro de opinión". Marzo, 2015. Disponible en: http://www.cis.es/cis/export/sites/default/-Archivos/Marginales/3040_3059/3057/Es3057mar.pdf
- De la Cuesta Arzamendi, J.L y Pérez Machío, A.I (2010). Ciberdelincuentes y cibervíctimas. En J.L De la Cuesta Arzamendi y N.J De la Mata Barranco. *Derecho penal informático* (pp. 99-120). España: Editorial Civitas.
- De Urbano Castrillo, E. (2011). "Los delitos informáticos tras la reforma del CP de 2010". Revista Aranzadi Doctrinal nº 6, pp. 163-176.
- España, Ministerio del Interior (2017). Estudio sobre la Cibercriminalidad en España. Recuperado de http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+Espa%C3%B1a.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70.
- Estévez, Ana & Villardón, Lourdes & Calvete, Esther & Padilla, Patricia & Orue, Izaskun. (2010). Adolescentes víctimas de cyberbullying: prevalencia, y características. Behavioral Psychology/Psicologia Conductual. 1. 73-89.
- Fernández Riquelme, S. (2017). "El delito como Identidad social. Reflexiones sobre la comunidad y su proceso de integración". En *La Razón Histórica,* nº 35, pp. 1-19.
- Machín & Gazapo, (2016). "La ciberseguridad como factor crítico en la seguridad de la unión europea". Revista UNISCI, 42, 47-68.

- Miró Linares, F. (2012). "El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio", Madrid, Marcial Pons.
- Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO, Revista Latinoamericana de Estudios de Seguridad, 20, 80-93. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2563
- Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. Journal of Research in Crime and Delinquency, 47(3), 267–296.
- Sarzana, C. (1979). Criminalitá e Tecnologia: il caso dei computer, in "Rassegna Penitenziaria e Criminológica". Italia.
- Vallés, L. (2016). La ciberseguridad en el mundo actual. TINO, 50, 585-620.
- Villalba Fernández, A. (2015). "La Ciberseguridad en España 2011-2015 una propuesta de modelo de organización (Licenciatura)". Universidad Nacional de Educación a Distancia.