Breve aproximación a la ciberdelincuencia desde una perspectiva criminológica

Brief approach to cybercrime from a criminological perspective

Pablo D. Punín Tandazo*
Investigador jurídico independiente

Información del artículo
Original – Ruptura, 2021

Citación
Punín, P. (2021). *Breve aproximación a la ciberdelincuencia desde una perspectiva criminológica.* Revista Ruptura de la Asociación Escuela de Derecho PUCE. Edición 2021, p (191-230).

DOI: 10.26807/rr.v3i03.85

Resumen: En el presente artículo se hace una breve aproximación a lo que son la ciberdelincuencia y el ciberdelincuente. También se muestra una clasificación de los ciberdelitos que permite identificar de mejor manera las características de este tipo de criminalidad. Se analizan cuáles son las teorías criminológicas que pueden ser adoptadas para tratar de explicar la ciberdelincuencia y en qué forma se puede presentar el desplazamiento en estos delitos. Por último, se indican algunas de las formas principales de combatir este tipo de criminalidad y la situación de Ecuador en la materia.

La finalidad de este artículo es brindar al lector información necesaria para comprender lo que implica la ciberdelincuencia; y, a partir de ahí,

* Abogado por la Pontificia Universidad Católica del Ecuador en el año 2018. Máster en Criminología y Ejecución Penal por la Universitat Pompeu Fabra en el año 2020. Especialista de Patrocinio Penal en la Contraloría General del Estado. Coordinador y miembro fundador del Observatorio de Criminología, Política Criminal y Ejecución Penal de Ecuador. Docente. Investigador jurídico independiente. Contacto: puninpablo@gmail.com

que pueda profundizar en el estudio de alguno de los temas que de ella se desprenden.

Palabras clave: Ciberdelincuencia, criminología, teorías criminológicas, tecnologías de la información y comunicación, Internet.

Abstract: *This article makes a brief approach to what cybercrime and a cybercriminal are. Also shows a classification of cybercrimes in order to identify in a better way the characteristics of this type of criminality. In the same way, it analyzes which are the criminological theories that can be adopted to explain cybercrime and how displacement can be presented. Finally, some of the main forms to combat this type of criminality are exposed and the situation of Ecuador in this area is analyzed to know if the efforts have been sufficient to reduce the problem.*

The purpose of this article is to provide the reader the necessary information to understand what cybercrime entails and, from there, delve into the study of some issues that stem from it.

Keywords*: Cybercrime, criminology, criminological theories, information and communication technologies, Internet.*

Introducción

El acelerado desarrollo que se ha presentado en las tecnologías de la información y comunicación -en adelante TIC- ha generado la presencia de más usuarios en el ciberespacio y la reducción de la brecha que lo separa del mundo físico. Cada vez son más las conductas y actos ejecutables en el entorno virtual, lo que parece indicar que su objetivo podría ser llegar a convertirse un sitio en el que se pueda realizar todo lo que se puede hacer en la realidad física, sin las limitantes que esta última presenta.

En este sentido, se puede decir que los problemas de la delincuencia no son ajenos a la realidad virtual. La continua expansión del ciberespacio ha derivado en la presencia de conductas consideradas ilícitas. De hecho, mucho de lo que se realiza en este lugar tiene incidencia en el mundo físico,

siendo los ciberdelitos un claro ejemplo. Si se toma en cuenta esto, añadiendo el mayor grado de participación que tendrán los medios tecnológicos dentro de nuestras relaciones interpersonales en un futuro, es lógico comprender que resulte tan necesario el estudio de la ciberdelincuencia.

En el presente artículo se busca hacer una breve aproximación al cibercrimen para quienes estén interesados en conocer más sobre el tema. La idea es otorgar al lector algunos conceptos clave relacionados con este tipo de criminalidad, para posteriormente analizarla desde una perspectiva criminológica que permita comprender de mejor forma las características que la diferencian de la delincuencia tradicional.

Es por esto por lo que en un inicio se analiza el concepto de ciberdelincuencia, para una vez definido, indicar cómo las conductas que se encasillan en ella pueden ser clasificadas. Posteriormente se hace un acercamiento al ciberdelincuente, trayendo a colación algunos estudios de perfilación criminal relacionados con su figura, y se exponen cifras que permiten observar cómo los ciberdelitos tienen una tendencia en aumento.

Desde el campo criminológico se analiza si cabe la aplicación de algunas teorías de la delincuencia en este tipo de criminalidad. Además, se realiza una descomposición del problema referente al desplazamiento en este tipo de delitos. Por último, se describen algunas recomendaciones que se han planteado para combatir al cibercrimen, para luego dar paso a un breve análisis sobre la situación de Ecuador en este campo y conocer si los esfuerzos ejecutados son suficientes para dar un tratamiento efectivo a la problemática.

I. La Ciberdelincuencia

No existe una sola definición sobre ciberdelincuencia aceptada de forma universal; justamente Wall es quién indica que, para lograr definirla, se debe conocer cuál es el impacto que las TIC han tenido en la transformación del mundo (2007). Se señala que este término no es jurídico, sino genérico para describir hechos cometidos contra, o a través, del uso de datos o sistemas informáticos (Yar & Steinmetz, 2019).

Los orígenes de internet se remontan al desarrollo del sistema de alerta temprana e intercepción de bombarderos enemigos desarrollado por el ejército de los EEUU (Yar & Steinmetz, 2019), debido a que se necesitaba coordinación en las estaciones de radar a tiempo real y gran escala. Tras la creación del ARPA[2], se dispuso la creación de una red de computadoras militares, que permita el flujo ininterrumpido de comunicaciones en territorio norteamericano ante un posible ataque nuclear soviético.

En 1996, Lawrence Roberts fue empleado por ARPA y al año siguiente presentó un proyecto para crear lo que se conocería como ARPANET[3] (Paloque - Bergés & Schafer, 2019). El primer nodo de ARPANET fue la computadora central del Centro de Medidas de Red de la Universidad de California, realizando la conexión con el Instituto de Investigación de Standford, enviando el primer mensaje a ese destino. Una vez que se logró comunicar con éxito, se agregaron nuevos nodos que darían origen a la ARPANET inicial (Sain, 2015). El resto es historia.

Se puede decir que la aparición de Internet se erigió como un momento que marcaría el inicio de una forma distinta para acceder a sistemas de información. Hoy en día, resulta muy sencillo encontrar todos los ámbitos del día a día reflejados en la red (Mateos Pascual, 2013). Cyber se utilizó para definir a un nuevo campo emergente que gira en torno a máquinas y sistemas, haciendo referencia en específico a máquinas que pudieran interactuar recíprocamente con sus entornos, llegando incluso a relacionarse con cualquier cosa que implique computadoras y su potencial.

Mientras la sociedad en general daba sus primeros pasos en el ciberespacio, lo hacían también quienes esperan obtener un beneficio ilícito de los nuevos medios que se encontraban a su disposición (Mateos Pascual, 2013). Entonces, esta nueva creación no solamente implicaba avances en lo positivo; sino que, también significó una nueva oportunidad para la delincuencia.

2 Advanced Research Projects Agency (Agencia de Investigación de Proyectos Avanzados).

3 Así se conoció a la red de computadoras para enviar datos militares y generar conexión entre grupos de investigación estadounidenses. Para más desarrollo véase Arpanet (1969–2019) (Paloque - Bergés & Schafer, 2019)

Así, podemos describir al ciberespacio como un dominio artificial que ha sido construido por personas, el cual se diferencia del espacio físico, y pese a que su historia no sea tan larga como la de la humanidad, puede afectar actividades en otros dominios y viceversa. El ciberespacio no es indiferente al mundo físico, sino que también se encuentra vinculado y apoyado de por medios físicos, como computadoras o redes de electricidad. Además, muchos efectos de lo que se haga en el ciberespacio se palparán en el mundo real. Es por esto por lo que se indica que, si se ataca a esta interconexión, pueden existir repercusiones graves sobre las estrategias de seguridad nacionales e internacionales (Pons Gamón, 2017).

Los términos ciberdelincuencia y cibercrimen suelen utilizarse para referirse a situaciones similares. De hecho, el ciberdelito se asocia a aquellas actividades ilegales que se ejecutan mediante el uso de los actuales sistemas de comunicación e información (Fernández - Rodríguez, Miralles Muñoz, & Millana Cuevas, 2019). La ciberdelincuencia se puede definir como cualquier tipo de actividad ilegal en la que se hace uso de internet, una red privada o pública o un sistema informático doméstico; comprende cualquier acto delictivo que usa ordenadores y redes. Además, incluye delitos tradicionales realizados a través de internet (Reyes Neira, 2015).

Los ciberdelincuentes no tienen un perfil de objetivo diseñado, sino que pueden atacar a personas, entidades públicas o privadas y gobiernos. Todo dependerá del objetivo del ataque. Para Miró (2012) ciberdelincuencia es cualquier delito en el que las Tecnologías de la Información y Comunicación juegan un papel determinante en su concreta comisión. Siguiendo esta línea, podríamos decir que los términos ciberdelincuencia y cibercrimen parecen utilizarse de manera indistinta. En este sentido, los vocablos ciberdelito y cibercrimen se pueden considerar sinónimos.

No obstante, no podemos decir que cualquier ataque a un elemento TIC constituye un cibercrimen, esto resultaría en una generalización imprecisa (Miró, 2012). Por ejemplo, partiendo de lo anterior, no podría ser un cibercrimen destrozar a golpes una antena que emite señal de internet; mientras que sí lo sería dañar un puerto de acceso de red mediante la utilización de un virus.

Por lo tanto, para no caer en equívocos, podemos decir que la ciberdelincuencia engloba los delitos cometidos a través de las nuevas tecnologías. Es

un concepto que utilizamos para referirnos al conjunto de conductas que vulneran los derechos de terceros y se producen en un campo tecnológico, misma que provocan un rechazo social y, sobre las que interviene el derecho penal (Fernández Bermejo & Martínez Atienza, 2020).

II. Clasificación de los ciberdelitos

Una vez que hemos comprendido el significado de ciberdelincuencia, es necesario también precisar en qué forma se clasifican los denominados ciberdelitos. Al tratarse de un espacio con características totalmente distintas a la realidad física, es evidente que la ciberdelincuencia tampoco será un fenómeno homogéneo.

Resulta sumamente complicado encasillar a los ciberdelitos en una clasificación única, porque existen varias formas distintas de organizarlos. Se puede, por ejemplo, clasificar debido a las víctimas, así como debido a los objetivos esperados por los ofensores. De igual forma, se podrían clasificar teniendo en cuenta los medios utilizados, por la complejidad de su ejecución, o de acuerdo con el tipo de conductas legalmente prohibidas (Trochez Arias, 2020).

Es por esto por lo que, en este punto, es necesario indicar que he considerado que la clasificación de los ciberdelitos más adecuada para fines didácticos, tomando en cuenta su complejidad, es la establecida por el profesor Fernando Miró. Él hace una diferenciación entre 3 categorías de criminalidad en el ciberespacio, contenidas en dos clasificaciones, atendiendo al propósito criminal con el que se actúa y al contexto de incidencia del ciberespacio al que afectan los delitos.

2.1. Primera clasificación

La primera sistematización atiende la incidencia de las TIC en el comportamiento criminal, de ella se desprenden: 1) Ciberataques puros; 2) Ciberataques réplica; y 3) Ciberataques de contenido.

Dentro de la realidad criminológica se ha comprobado que el ciberespacio puede generar conductas delictivas si la única forma de materializarlas es a través de las TIC. En otros casos, el surgimiento del ciberespacio no ha llevado a la creación de nuevas formas de delincuencia, sino más bien, a la adaptación de conductas criminales realizadas en el entorno físico que ahora tienen lugar en el entorno virtual.

Por último, el ciberespacio ha traído a debate el contenido que se maneja en su interior, si se tiene presente que internet es un medio idóneo para la difusión global; por lo que, existirán conductas en las que lo ilícito verse sobre la difusión, o acceso, a cierta información considerada socialmente peligrosa (Wall, 2005). A continuación, se profundizará en cada una de estas subclasificaciones.

1. Ciberataques puros

Tal como ya se ha indicado con anterioridad, la aparición del ciberespacio y las TIC ha generado el surgimiento de nuevos objetos, bienes y servicios con valor económico y social. En relación con ellos, aparecen también nuevas conductas que tienen lugar solamente en internet (Miró, 2012). Se encontrarán muchos comportamientos ilícitos nuevos que se dirigen contra estos servicios, bienes o terminales que se encuentran en el espacio cibernético. Es justamente a este tipo de conductas ilícitas, que surgen del ciberespacio y solamente pueden llevarse a cabo en él, a las que se conoce como ciberataques puros.

De esta forma, podemos decir que son aquellos que solamente deben -y pueden- ser posibles en el ciberespacio. En ellos las TIC constituyen el único medio comisivo de los ataques, en cuánto son medio y objetivo; y, no es posible cometer estas infracciones si no es en este espacio.

Se establece que la problemática más complicada a la que se enfrentan estos ciberdelitos surge de la total novedad de los comportamientos y la consiguiente falta de estrategias preventivas de carácter criminológico frente a ellas (Miró, 2012). Esto tiene mucho sentido si se comprende que, al ser conductas nuevas, merecen un análisis profundo e integral

para plantear algún tipo de tratamiento preventivo, cuestión que requiere tiempo para comprender la conducta de mejor manera y su evolución.

Un ejemplo claro de ciberataque puro es el Hacking. Esta conducta consiste en el acceso ilícito (sin autorización) a sistemas informáticos ajenos para destruir, modificar o tener acceso a datos de empresas o particulares (Giménez Solano, 2011). Esto quiere decir que la persona que comete esta conducta (hacker) intenta romper las barreras informáticas. Esta conducta también implica siempre un acceso realizado a distancia, ya que, el ofensor busca acceder a los datos sin tener algún tipo de contacto físico con el sistema. El Hacking apareció en el mismo momento en el que surgieron los sistemas informáticos y no como una conducta ilícita, sino como una forma de ayudar a la evolución del sistema (Miró, 2012); sin embargo, hoy en día se asocia con mayor fuerza a la criminalidad porque el solo hecho vulnerar un sistema privado pone en riesgo el valor de la información.

Se entiende, entonces, que el Hacking es una conducta que solamente puede realizarse a través del ciberespacio, comprendiendo a este último como el medio para alcanzar los objetivos que se encuentran también en el (datos e información). Siendo, de esta forma, un ciberataque puro.

2. Ciberataques réplica

Así como existen nuevas conductas que surgieron con el ciberespacio, también hay conductas que ya se realizaban en el espacio físico y se adaptaron para encontrar lugar en la realidad virtual. A las nuevas formas de conducta que no existirían si no lo hiciera el ciberespacio, se deben añadir aquellas que son reflejo de las tradicionalmente ejecutadas en el espacio físico.

Se puede decir que el hecho de adaptar conductas tradicionales al ciberespacio implica que dentro de ellas también estén inmersas algunas conductas criminales tradicionales. Estas son las nuevas formas de realización de infracciones tradicionales que tienen las redes telemáticas. Aquí el ataque no se realiza a un terminal informático, ni tampoco es el contenido el objeto de la ilicitud, sino que la red es el medio a través del

cual se comete una infracción que utilizaba anteriormente otros medios para llevarse a cabo (Miró, 2012).

Son ataques llevados a cabo en el ciberespacio, iguales o similares a crímenes que ya se realizaban en el espacio físico. La adaptación de esta conducta al entorno virtual la hace ver como un tipo de conducta con particular singularidad, de forma en la que pareciese que estuviésemos hablando de una conducta nueva, hasta el punto de que, si bien en el espacio territorial podría apenas tener relevancia dañina, esto podría cambiar en el espacio virtual (Miró, 2012).

Se ha determinado que el problema principal que presentan este tipo de delitos es la potenciación del riesgo para los intereses sociales (Miró, 2012), misma que se desprende del nuevo medio, vasto e inmenso como es el ciberespacio, en el que se ejecuta la infracción.

Un ejemplo de ciberataque réplica es el phishing. Este ciberdelito es un tipo de estafa en la que se hace uso de algunas técnicas de ingeniería social para engañar a una persona con el fin de obtener información o algún beneficio de manera ilícita (López Sánchez, 2019). Usualmente se roban datos de identidad personal o de tarjetas de crédito y cuentas bancarias; utilizando la ingeniería social para hacer uso de la identidad personal de otro, falsificando sitios web, buscando que el usuario confíe en la veracidad del mensaje y proceda a entregar los datos.

3. Ciberataques de contenido

El profesor Miró (2012) establece que este grupo de tipologías de cibercriminalidad es una forma concreta de los que hemos denominado ciberataques réplica, pero con particularidades y problemáticas jurídicas tan especiales, que merece ser tratada por separado. Señala que esta clasificación engloba a todas aquellas conductas en las que el centro de la infracción lo constituye el contenido que se comunica o transmite a través de las redes telemáticas.

Hoy en día podemos decir que internet funciona como un medio de edición y comunicación, por lo que, es normal que se cree una preocupa-

ción sobre los contenidos que se manejan en la red, tomando en cuenta la aparición de conductas en las cuales la ilicitud proviene del contenido distribuido por Internet (Miró, 2012).

Un ejemplo de este tipo de ciberataque es la pornografía infantil que se difunde en el ciberespacio. Este delito comprende toda representación visual y real de un menor desarrollando actividades sexuales explicitas (Morillas Fernández, 2005); por lo que, se entiende que la ilicitud como tal recae sobre el contenido. Estos ciberdelitos plantean dificultades propias relacionadas tanto con la dificultad de prevenir la mera difusión de contenidos en el ciberespacio, como con la compleja cuestión de atribuir responsabilidad a todos los intervinientes en tal proceso[4].

2.2. Segunda clasificación

La segunda sistematización que realiza el profesor Miró es teniendo en cuenta el móvil y contexto criminológico. Esto quiere decir que se toma en cuenta el motivo que lleva al ciberofensor a cometer el delito (Miró, 2012). Esta perspectiva criminológica permite comprender que dentro del ciberespacio existen tres categorías de delitos: aquellos cuyo propósito es la obtención de un beneficio patrimonial, aquellos cuyo objeto es una persona individual dentro de los aspectos de su desarrollo personal y aquellos que tienen un objetivo ideológico o político.

1. Cibercriminalidad económica

Se puede decir que esta es la principal categoría de delitos en el ciberespacio. El cibercrimen económico no es solamente el que afecta al patrimonio de las personas o al sistema económico, sino que, también entran en esta categoría aquellos cuyo objetivo sea conseguir un beneficio económico, aunque afecte a otros bienes jurídicos como la intimidad. El cibercriminal económico utiliza las TIC como medio, atendiendo al propósito de obtención de un beneficio patrimonial. Resulta en el apode-

4 Para mayor desarrollo véase: El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio (Miró, 2012).

ramiento de patrimonio ajeno a través de técnicas informáticas (Luciano & Lo Giudice, 2015).

El ejemplo más claro de este tipo de ciberdelitos puede ser el Scam. Se utiliza este término para referirse a los fraudes que se ejecutan a través de la red, sea por correo electrónico o por una pagina web. Por lo general, los scammers intentan engañar a las personas enviando cadenas por correo electrónico, en las cuales indican que harán una donación benéfica o que obtendrán viajes, vacaciones, dinero, o algo a cambio. Las víctimas ingresan datos bancarios y ahí es en donde los ofensores de este delito ejecutan la estafa (Universidad Veracruzana, 2015). Aquí se evidencia cómo el objetivo principal del ciberdelincuente es obtener un beneficio económico en perjuicio de las víctimas.

2. Cibercriminalidad social

El ciberespacio se ha convertido en un ámbito de comunicación social sumamente importante, en especial por las nuevas generaciones que han nacido en épocas en donde existe la total implantación de las TIC. Las redes sociales e internet se constituyen como un nuevo ámbito de desarrollo personal en el que las personas crean relaciones. Es por esto por lo que se afirma que, todas las esferas personales, al entrar en contacto con los demás, también pueden estar en peligro en el ciberespacio (Miró, 2012). Entonces, podemos decir que este tipo de criminalidad engloba ataques que afectan a las esferas más personales del desarrollo del individuo.

Un ejemplo que se adecúa a la cibercriminalidad social es el acoso por internet o ciberacoso. Esta conducta es la adaptación del acoso tradicional realizado por medio de las tecnologías digitales. Ocurre en redes sociales, plataformas de mensajería, plataformas de juegos y teléfonos. Es un comportamiento repetitivo que busca atemorizar, enfadar o humillar a otras personas (UNICEF, 2021). Estas conductas pueden variar, no existe una sola forma de acosar; por ejemplo, se pueden difundir mentiras o material fotográfico que genere hostigamiento hacia una persona; o, enviar mensajes de amenaza con insultos a través de redes sociales.

Aquí se evidencia que las acciones cometidas por el ofensor causan un detrimento en el ámbito de desarrollo personal de las víctimas, siendo éste el fin último del delito.

3. Cibercriminalidad política

Internet se ha convertido en un instrumento de lucha política e ideológica, puede trasmitir información de forma en la que se convierta en una manera de captación ideológica, puede servir para atacar servicios o instituciones estatales y puede ser un medio para comunicaciones entre individuos separados físicamente, pero unidos por un fin político o ideológico (Miró, 2012). Esto quiere decir que existirán ciberdelitos en los que el motivo de la conducta no sea económico ni social, sino político.

Por lo tanto, no se busca obtener un beneficio económico o afectar el ámbito de desarrollo personal de alguien, sino más bien causar daños a infraestructuras u objetivos sensibles, con el propósito de desestabilizar un Estado, una institución o una organización política.

Hay varias formas de manifestación de ciberdelitos políticos. Por ejemplo, en relación con el ciberterrorismo, se define a esta conducta como la posibilidad de usar las TIC para ejecutar ataques premeditados y políticos contra sistemas de información, así como la difusión de sus fines y logros, añadiendo el riesgo o peligro que sufren los intereses individuales de las personas y el daño a la paz social (Brown & Korff, 2009).

Otro ejemplo puede ser el hacktivismo. Los hacktivistas son activistas políticos que usan las herramientas tecnológicas para protestar en Internet. Además, se conoce que los principales motivos de sus actividades son la lucha por una sociedad alternativa relacionada con la libertad de información, la lucha por la democracia y la lucha por una sociedad abierta (Loreto, 2004). Dentro de este último tipo de conductas podrían encasillarse muchos de los ataques realizados por la organización ANONYMOUS.

Estas dos clasificaciones no son excluyentes una de otra, resultan compatibles y complementarias para comprender de forma más amplia el

tipo de ciberdelito ante el que se encuentra. Se podría encasillar un mismo delito dentro de las dos sistematizaciones, atendiendo las características de la conducta.

Por ejemplo, un caso de Hacking, que como ya vimos, es un ciberdelito puro al solamente poder ser cometido a través de las TIC, también puede ser un ciberdelito económico o político, dependiendo del fin con el que se ejecute. Si se ejecuta con el fin de obtener un beneficio económico estaremos ante un ciberdelito puro/económico; mientras que, si se ejecuta con el fin de liberar información para que su acceso sea gratuito y universal, el ataque será encasillado como un ciberdelito puro/político.

III. El ciberdelincuente

Desde una perspectiva criminológica, es necesario estudiar al delincuente para poder implementar una adecuada política preventiva. Identificar perfiles puede ser una técnica eficaz para introducir políticas de seguridad y posterior identificación de los delincuentes (Cámara Arroyo, 2020).

En este sentido, el estudio de determinados tipos de comportamiento asociados a perfiles socioeconómicos concretos ha arrojado algunas conclusiones importantes en el campo de la prevención delictiva. Sin embargo, existe un acuerdo común en que el perfil del ciberdelincuente es muy heterogéneo en cuanto a sus competencias en el medio informático (Cámara Arroyo, 2020). Esto es comprensible si se tiene presente la alta variación que existe en los ciberdelitos y las características que los particularizan.

Esto se dificulta aún más por la facilidad latente en convertirse en un ofensor de este tipo de criminalidad, tomando en cuenta el nivel de desarrollo tecnológico en el que vivimos actualmente. Es decir, cualquiera podría ser un ciberdelincuente.

Esto no quiere decir que no existan estudios orientados a la perfilación del ciberdelincuente. Para tener una idea, según una investigación realizada en la Universidad de Yale para estudiar las características de los ciberdelincuentes, se ha demostrado que las personas que cometen frau-

des informáticos reúnen las siguientes características: 1) la mayoría son hombres de edad media mayor, 2) casados, 3) económicamente estables porque disponen de un puesto fijo de trabajo, 4) tienen un alto nivel de educación, 5) buena consideración de sí mismos, y 6) no se consideran delincuentes (Garrido, Stangeland, & Redondo, 2006).

Tomando en consideración los estudios de tipo criminológico que se han ocupado de estudiar los perfiles de estos delincuentes, se puede decir que poseen unos conocimientos mínimos del medio informático, sin los cuales no podrían acceder a los distintos sistemas (De la Cuesta & Pérez Machío, 2010).

De acuerdo con Mateos (2013), existe un número elevado de estudios que apuntan a que el perfil típico del ciberdelincuente es una persona de sexo masculino, entre 25 y 35 años de edad, y con ciertos conocimientos tecnológicos e informáticos que le posibilitan usar internet como medio para ejecutar sus actividades, aunque vale acotar que la edad de inicio en la ciberdelincuencia es cada vez menor; por lo que, se deben estudiar los móviles causantes de este hecho (González García & Campoy Torrente, 2018).

En concordancia con lo anterior, se indica que la mitad de las bandas dedicadas al cibercrimen están compuestas usualmente por seis o más personas, de las cuales 76% son hombres cuyas edades oscilan entre los 14 (8%) y los 50 años (11%), con una media de 35 años (43%) (Fernández - Rodríguez, Miralles Muñoz, & Millana Cuevas, 2019). En el informe sobre ciberdelincuencia en España del año 2017, se desprende que la cifra total de detenciones o de personas investigadas por las fuerzas y los cuerpos de seguridad del Estado fue de 4912, de los cuales 77.04% eran hombres (Ministerio del Interior, 2017).

Hay varios factores pueden explicar la brecha de género en la ciberdelincuencia, al respecto Sergio Cámara establece que los principales son los siguientes: 1) El tipo de socialización primaria que enseña a los hombres y a las mujeres una actitud diferente hacia la tecnología; 2) Diferencias en la capacitación; y, 3) Un sesgo de género en el lenguaje informático. Sin embargo, también menciona que, desde los 90, la presencia de mujeres comenzó a aumentar progresivamente y se hizo más relevante (2020).

Si bien los distintos estudios parecen indicar que el ciberdelincuente se perfila como un hombre joven, con ciertos conocimientos sobre informática o las TIC; es necesario volver a indicar que, por la naturaleza misma de estos delitos y el avance de la tecnología, cualquier persona, sin importar sexo, edad, o cualquier otro rasgo distintivo, podría convertirse en un ciberdelincuente.

Un ciberdelincuente es todo aquel que puede ser acusado de ejercer la ciberdelincuencia. De igual forma, se consideran ciberdelincuentes a quienes han logrado adaptar sus comportamientos ilícitos con la tecnología, como puede ser el caso de pederastas, proxenetas, etc. (Fernández - Rodríguez, Miralles Muñoz, & Millana Cuevas, 2019).

En otras palabras, se puede afirmar que, a fin de cuentas, será un ciberdelincuente todo aquel que esté en capacidad de usar las TIC -y efectivamente lo haga- como medio o fin del delito.

IV. La ciberdelincuencia en cifras

Caneppele y Aebi se refieren a la caída de los índices delictivos, en aquellos delitos denominados como "tradicionales" en las sociedades occidentales altamente industrializadas, y la evolución de nuevas formas delictivas, siendo una de ellas el delito cibernético (2017). Entre los argumentos expuestos por los autores se puede evidenciar cómo se intenta relacionar la caída de los delitos tradicionales con la evolución del ciberdelito. De esta forma se crea el debate respecto a si la universalidad de la caída del crimen y las cifras que reflejan menor cantidad de delitos tradicionales, son resultado de nuevas formas de criminalidad; o, un fracaso en la recopilación de datos.

Si bien se llegó a determinar que efectivamente existe una caída del crimen en ciertos delitos, no se puede afirmar de forma sencilla que el aumento del ciberdelito sea el motivo. Efectivamente, existen muchos problemas en la recopilación de datos por parte de la policía, lo que genera un problema en las fuentes estadísticas que reflejan las tasas de criminalidad (Cámara Arroyo, 2020).

Este problema versa sobre la recopilación de datos deriva en una amplia cantidad de cifra negra, siendo esta última la que no permite realizar afirmaciones exactas para determinar causas o motivos de la caída del crimen tradicional ante nuevas formas de delincuencia. No se puede pasar por alto que los delitos cibernéticos han servido para evidenciar la ineficiencia de los métodos policiales de registro de datos. Las nuevas formas delincuenciales son problemas que deben ser abordados de forma correcta y eficiente por lo organismos de control y persecución del crimen.

No se puede dejar a un lado el crecimiento que ha tenido la ciberdelincuencia ante otros tipos de criminalidad con el pasar de los años. Este tipo de delincuencia es muy atrayente para los ofensores debido a las particularidades que la caracterizan. Una de las singularidades que hacen a las nuevas tecnologías atractivas para los ciberdelincuentes, en especial para cometer ciberataques de diferente tipo, es el efecto masivo que podrían conseguir con sus acciones.

Por ejemplo, con el uso de troyanos en miles de ordenadores se pueden realizar ataques de forma simultánea con consecuencias realmente graves. Además, en estos casos resulta sumamente complicado señalar al autor de los ataques, hay mecanismos y técnicas que permiten camuflar y ocultar la dirección de algunos equipos (Roca, 2014).

Estos elementos intrínsecos a este tipo de delitos son los que derivan en que esta criminalidad ocupe un mayor espacio dentro del espectro social. Si a la dificultad de identificar autores (impunidad), se le añade la posibilidad de obtener resultados masivos fácilmente (objetivo del delito), es lógico que los ofensores busquen adaptar sus conductas a este nuevo tipo de criminalidad. El delincuente se encuentra ante menores riesgos y mayores beneficios.

Este decantamiento, que se presume pueden tener los ofensores respecto a este tipo de criminalidad, ya es palpable en algunas cifras. En el año 2015 en España, por ejemplo, fueron registrados 81 307 delitos, de los cuales 74.4% se relacionaron con fraudes informáticos (estafas), mientras que 13. 9 % se vincularon con amenazas y coacciones (2017). El fraude informático es el principal delito cometido en la actualidad en

el contexto español, seguido de las amenazas y coacciones, y la falsificación informática (Pons Gamón, 2017).

Según indica el Ministerio del Interior (2019), en el 2019 se denunciaron 218.302 delitos cometidos en internet, lo que representa un 35,8% más que en el año 2018, en el que fueron 160.729, y prácticamente el doble de los 117.399 registrados en 2017. Además, se señala que los ciberdelitos ya representan el 10% de las infracciones penales conocidas en ese año, mientras que tres años antes solamente eran el 4,6% de toda la delincuencia (López - Fonseca, 2020).

En la misma línea, una evaluación de la INTERPOL relacionada con los efectos del COVID 19 en la ciberdelincuencia, manifiesta la extensión que ha tenido esta criminalidad. Se indica que en un solo cuatrimestre -entre enero y abril de 2020- un socio de INTERPOL del sector privado detectó 907 000 correos basura, 737 incidentes de tipo malware y 48 000 URL maliciosas (2020). Además, según el informe de Riesgo Globales 2020 del Foro Económico Mundial, el riesgo de ciberataques dirigidos a la infraestructura crítica, fraude o robo de datos, están entre los 10 principales riesgos con mayores posibilidades de ocurrir (BID & OEA, 2020).

En Colombia, entre enero y junio de 2020, se registraron 17. 211 denuncias (6.340 más que el primer semestre del 2019); y, también existieron 2. 103 casos de suplantación de sitios web, convirtiéndose en un delito que aumentó en 364% (PORTAFOLIO, 2020).

En Ecuador, de enero hasta mayo del 2021, se denunciaron 606 casos de apropiación fraudulenta por medios electrónicos en la Fiscalía a nivel nacional; mientras que, en el 2020 se registraron 682 casos y en 2019 un total de 828. Según las denuncias presentadas en Fiscalía, en el 2017 se registraron 9421 casos relacionados a delitos informáticos, en 2018 subieron a 9571 y en 2019 a 10 279 (El Universo, 2021).

Por lo tanto, resulta evidente afirmar que la ciberdelincuencia es un tipo de criminalidad que está expandiéndose dentro del espectro social. La tendencia global existente indica un aumento en las tasas de denuncias relacionadas con los ciberdelitos. Es de esperarse que las cifras au-

menten con el pasar del tiempo debido a que las nuevas tecnologías de la información cada vez ocupan más lugares y la brecha con el espacio físico se reduce.

Esta tendencia al aumento también responde, como se mencionó antes, a las facilidades que brinda este tipo de criminalidad a los ofensores. Una criminalidad con bajos riesgos y altos beneficios siempre resultará más atrayente que aquella que conlleva un nivel de dificultad mayor en la ejecución.

Por lo que, si bien no se puede afirmar que la caída del crimen tradicional se debe únicamente al surgimiento de la cibercriminalidad, tampoco podemos negar que sí ha tenido incidencia al respecto.

V. Teorías criminológicas en la ciberdelincuencia

A lo largo de la historia han existido varios estudios dedicados a la comprensión de la delincuencia, con el fin de obtener respuestas que expliquen estas conductas. El estudio de este campo social ha dado como resultado el planteamiento de teorías direccionadas a explicar sus razones de ser.

Resulta necesario indicar en este punto que no existe una concordancia respecto a cuál es la teoría que explica como tal la delincuencia, así como tampoco hay quien diga que la ha encontrado. Lo que sí hay, por otra parte, son teorías que permiten comprender de mejor forma este fenómeno social, tomadas desde perspectivas distintas, aunque no necesariamente excluyentes.

Al ser un nuevo campo o espacio para la materialización de conductas criminales, la cibercriminalidad también merece un tratamiento que pueda explicarla. Es aquí en donde algunas veces se ha cuestionado si, quizás, las teorías relacionadas con la delincuencia tradicional podrían servir, de cierto modo, para explicar la ciberdelincuencia. Es justamente esto lo que trataremos en este punto. A continuación, se explicará cómo

algunas teorías de la delincuencia tradicional podrían también utilizarse para comprender la ciberdelincuencia.

5.1. Teoría de la frustración o tensión

Entre los principales defensores de esta teoría encontramos a Agnew, quién desarrolló a profundidad el concepto de anomia planteado por Durkheim y Merton. Justamente, para este último la conducta delictiva es una reacción esperada a las contradicciones de las estructuras sociales, mismas que ejercen una presión definida sobre sus miembros para que adopten comportamientos disconformes; advirtiendo entonces que, la conducta delictiva, es la reacción normal: un modo de adaptación individual a las contradicciones de la estructura social (Merton, 1968).

Es decir, Merton establece que existe un desajuste entre los fines establecidos culturalmente por la sociedad (un trabajo, una casa, educación de calidad, un auto, etc) y los medios líticos para obtenerlos. Este desajuste puede entenderse como la "anomia". Esta anomia conlleva reacciones para la persona que no puede alcanzar los fines socialmente establecidos, siendo una de ellas la frustración.

Cuando nos frustramos tendemos a buscar una solución a la situación. Dependiendo de cómo se adapte la gente a la situación de anomia, una posible respuesta, y mayoritaria debido a la imposibilidad de acceder a medios lícitos por la estructura social, será la delincuencia (Merton, 1968).

Agnew, por otro lado, define como frustración a las relaciones negativas con otros. Es decir, relaciones en las que la persona no recibe el trato que le gustaría recibir (Tejión Alcalá, 2019). El autor hace la clasificación de las fuentes de la frustración en tres tipos ideales que engloban las situaciones de tensión, siendo estos: 1) Impedir al sujeto alcanzar objetivos valorados positivamente, 2) Retirar estímulos valorados positivamente, o 3) Exponer al sujeto a estímulos valorados como negativos o nocivos.

Al ser un nuevo sitio, el cuál carece de muchas limitaciones existentes en el espacio físico, este podría servir como una vía de escape o supe-

ración de las tenciones a las cuáles se enfrenta la persona, referidas por Agnew. Por lo tanto, el ciberespacio reduce los medios de control social y se erige como un sitio en el que las personas pueden desatar libremente la frustración que viven en la vida real.

De Floor Jansen y Van Lenthe (Cybercrimne Through an Interdisciplinary Lens, 2016) se desprende que la teoría de la frustración es la más usada por los académicos para examinar el acoso cibernético y ciberbullying, partiendo de que el entorno virtual permite a las personas desahogar fácilmente su ira y frustración, siendo muchas veces dirigido contra otras personas o usuarios de la red.

5.2. Teoría del aprendizaje social y la asociación diferencial

El máximo expositor de esta teoría es Sutherland, quien sostiene que los sujetos han llegado a aprender a ser criminales por una serie de técnicas trasmitidas culturalmente, principalmente por el empoderamiento que adquiere el crimen en determinados grupos, donde se consolida dicha actividad y se refuerza para continuar haciéndola (Hikal, 2017).

Esta teoría plantea que el delito es causado por la adquisición de conocimientos relativos a la forma en la que se cometen actividades delictivas y la suma de definiciones favorables a su cometimiento, acompañada de la menor presencia de definiciones desfavorables (Matsueda, 1988).

Esto quiere decir que si una persona se encuentra o convive en un ambiente en el que la percepción del acto delictivo no es negativa, sino positiva, será más propensa a internalizar esta percepción; y, sumando el aprendizaje de técnicas o formas en las que se puede materializar dicho acto, el resultado será una persona con altas probabilidades de cometer un delito.

Dentro del estudio de la teoría del aprendizaje social, se ha mencionado que se trata de una teoría que puede ser aplicada efectivamente en relación con el ciberdelito. Varios estudios han demostrado la existencia de relación de pares delincuentes, definiciones favorables y aprendizaje de técnicas delictivas (Tejión Alcalá, 2019).

Un ejemplo de esto puede ser el hacking. Este ciberdelito puede aprenderse de manera sencilla en internet; además, existen portales dedicados a facilitar información respecto a este tipo de procesos. El grupo de hackers, al relacionarse con sus pares, suma una carga de definiciones favorables al cometimiento de delitos. La combinación de estos dos elementos, a mi opinión, pueden derivar en la materialización de un delito como este.

5.3. Teoría del autocontrol o control social

Las teorías del control sostienen que los individuos se involucran en el delito por la naturaleza humana y las recompensas que puede dar su materialización, sean económicas o emocionales. De esta manera, lo que separa a los delincuentes y a quienes no lo son, es el autocontrol, brindado por cualquier vínculo social (Hirschi, 2003). Es decir, quienes tienen un nivel de autocontrol más bajo, delinquirán más fácilmente. Desde esta teoría se habla de impulsividad y baja capacidad de analizar el coste-beneficio en el tiempo; por lo que, estos elementos pertenecientes al bajo autocontrol conducen al delito.

Hirschi y Gottfredson (1990) establecen que los delincuentes tienen características en común, siendo estas: a) Actitud impulsiva, b) Insensibilidad y c) Poca consideración a futuro. De esta manera, se puede decir que, desde esta teoría, los delincuentes actúan de forma imprevista e impulsiva, sin tomar en consideración cuáles serán los costos de sus actos a futuro.

Colocando esta teoría en aplicación con el cibercrimen, se indica que el surgimiento de las nuevas tecnologías de la comunicación puede contribuir a la destrucción de vínculos sociales tradicionales, si se toma en cuenta la expansión de la globalización y las interconexiones, lo que significa menos capacidad de comunicación real. De esta forma, Internet, al ser un espacio en el que la velocidad de obtención de información o recompensas es mucho mayor que en el mundo físico, podría debilitar la capacidad de autocontrol de las personas (Cámara Arroyo, 2020).

5.4. Teoría de las actividades rutinarias

Según la teoría de las actividades rutinarias hay tres elementos que favorecen la probabilidad de ser víctima de un delito: 1) Delincuente motivado, 2) Victima propicia y, 3) Ausencia de guardianes capaces de evitar el delito (Rodríguez, Oduber, & Mora, 2017).

Nuestras actividades diarias nos posicionan en momentos y espacios en los que somos o más, o menos, propicios a ser víctimas de algún delito. Es por esto por lo que en esta teoría promovida por Cohen y Felson, se indica que la convergencia de los tres elementos mencionados con anterioridad puede generar la oportunidad perfecta para que el ofensor ejecute el acto ilícito (Summers & Rossmo, 2015).

Ya hemos analizado las facilidades que brinda el ciberespacio a los ofensores con relación a la impunidad y los beneficios masivos que puede obtener del ciberdelito; por lo que, es evidente que existirá mayor motivación en los delincuentes en realizar este tipo de delitos antes que delitos tradicionales.

Respecto al segundo y tercer elemento es necesario traer a colación lo mencionado a lo largo de este artículo, el uso de las TIC y los medios informáticos ha llegado a un nivel mundial, cada vez existen más usuarios de internet y el ciberespacio. De esta forma, al tener un crecimiento exponencial, resulta también claro que la cantidad de personas que pueden ser víctimas de un ciberdelito aumente.

Si a esto se le añade la complejidad existente en crear brechas de seguridad efectivas, o medios de vigilancia eficaces ante la prevención de los ciberdelitos, debido a la constante evolución y desarrollo del espacio virtual, el resultado será el surgimiento de más víctimas propicias para la ejecución del ciberdelito ante la ausencia de guardianes capaces de prevenirlo o evitarlo.

5.5. Teoría de las subculturas delictivas

Esta teoría, expuesta por Cohen, se relaciona en cierta medida con la teoría de la anomia de Merton, misma a la que se hizo referencia dentro

de la teoría de la frustración. Debemos recordar que Merton hacía referencia solamente a objetivos de carácter económico o material como causantes de la frustración. Cohen, por otro lado, establece que los jóvenes, sobre todo los que pertenecen a clases sociales bajas, pueden ver otros objetivos como el estatus social de clase media y el reconocimiento social; siendo la falta de oportunidades para conseguir reconocimiento social, o lograr un status, lo que puede llevar a que las personas comentan conductas antisociales (Tejión Alcalá, 2019).

Cohen incluso sugiere que algunos jóvenes conocen desde edades tempranas que no van a alcanzar cierto éxito económico ni un status social determinado y, por lo tanto, no alcanzarán aprobación o reconocimiento social. Es por esto por lo que es posible que estos jóvenes se planteen objetivos y valores distintos a los que han sido impuestos socialmente. Estos objetivos o valores nuevos pueden contribuir a la aparición de una nueva subcultura.

Esta subcultura nueva tendrá valores oponibles a los establecidos por los individuos de la cultura dominante porque son valores que les han sido negados, y porque los miembros de esta nueva subcultura responsabilizan a estos sujetos de su fracaso económico y social (Tejión Alcalá, 2019). Dentro de esta teoría se considera que muchos de los delitos que aparentemente carecen de motivación son dirigidos contra la fuente de su frustración, sea para identificarse con su nueva cultura, o como forma de venganza.

En consideración a la ciberdelincuencia, se puede afirmar que Internet facilita el contacto, dialogo y acercamiento entre personas. Resulta más sencillo encontrar pares a ideas y valores distintos y, así, crear subculturas. Al reconocer que el ciberespacio también puede ser un lugar propicio para el contacto interpersonal y la creación de redes de diálogo, incluso mejor que el mundo físico por la ausencia de barreras, es claro que existirá un mayor intercambio de valores y costumbres que generan el surgimiento de nuevas subculturas con principios propios.

Los grupos hacktivistas internalizan valores e ideas en común, mismas que luego se traducen en principios de acción. Por lo general, los prin-

cipios del hacktivismo, como vimos, van dirigidos al desarrollo de una sociedad con libre información; sin embargo, la cultura dominante tiene claro que, si bien existe el acceso a la información, no toda la información puede estar disponible para cualquiera.

En el ejemplo se evidencia la colisión de valores entre una subcultura y la cultura dominante. Será el nivel de internalización de los valores lo que definirá el accionar de la persona. Es decir, si la persona tiene un nivel de creencia elevado en los valores de la subcultura, o simplemente cree más en los valores de la subcultura que en los de la cultura dominante, en este caso una sociedad con libertad de información no tendrá reparo en ejecutar las acciones que considere necesarias para precautelar los valores en los que cree, pese a que sus actos puedan causar un detrimento, o irse contra los valores establecidos por la cultura dominante.

5.6. Técnicas de neutralización

Las técnicas de neutralización sirven para explicar cómo una persona puede llegar a delinquir mediante la negación del orden social dominante y sus reglas. Surgen como una crítica a la teoría anterior.

Aquí se indica que las dificultades de visualizar al comportamiento delictivo como el fruto de un conjunto de valores y normas desviadas, son de carácter empírico y teórico. Si existe una subcultura delictiva en función de la cual el delincuente considera su comportamiento ilegal como algo correcto moralmente, se debería suponer que el delincuente no debería mostrar sentimientos de culpa; sin embargo, ya existen varios estudios que demuestran que muchos delincuentes si experimentan un sentimiento de culpa o de vergüenza (Sykes & Matza, 2008).

Los defensores de esta teoría indican que esto significa que es sumamente difícil negar completamente la validez de las demandas de conformidad y sustituirlas por un nuevo sistema de normas. Por lo que, consideran que la postura teórica que manifiesta que tanto la delincuencia juvenil, como el comportamiento de obediencia a la ley, se basan en nor-

mas y valores de una subcultura delictiva y la sociedad en su conjunto, genera muchas dudas (Sykes & Matza, 1957).

Estos mismos autores indican que el delincuente no está en una especie de oposición total con la sociedad que cumple la ley, sino que, lo que los lleva efectivamente a cometer delitos que afectan los valores de la sociedad general es la neutralización momentánea del orden establecido, mediante la justificación de los actos ilícitos (Sykes & Matza, 2008). Las técnicas de neutralización consisten en formas en las cuáles las personas justifican su comportamiento delictivo.

Los autores han clasificado las técnicas de neutralización en 5 tipos: 1) Negación de la responsabilidad, 2) Negación del daño, 3) Negación de la víctima, 4) La condena a quien condena y, 5) Apelación a lealtades superiores (Sykes & Matza, 2008).

- La primera hace referencia a que el delincuente no se considera responsable del acto ilícito, se concibe a sí mismo como alguien impulsado por factores externos inevitablemente a cometer el delito, por lo que, la responsabilidad no debe recaer sobre él.

- En la segunda categoría se establece que para el ofensor la maldad de un acto dependerá de si alguien sufrió o no un daño por su conducta, cuestión que está sujeta a interpretación. Es decir, un delincuente puede considerar que un acto de vandalismo es una travesura, que el robo es un préstamo o que las peleas son un simple acuerdo.

- La tercera técnica indica que incluso si el ofensor acepta la responsabilidad de sus actos y admite que causó un daño, el reproche moral se puede neutralizar al considerar el daño no es un mal sino, quizás, algo merecido por quien lo recibe.

- La cuarta neutralización consiste en trasladar el foco de atención de los actos del ofensor al comportamiento de quienes desaprueban su conducta. Aquí el delincuente alega que quienes lo juzgan

son hipócritas al ser personas que también cometen actos desviados de alguna forma.

- Por último, la quinta técnica hace referencia a que el control social puede ser neutralizado mediante el sacrificio de las demandas de la mayoría ante las demandas de grupos más pequeños a los que pertenece el delincuente. Esto significa que el incumplimiento de ciertas reglas puede surgir por el sentimiento de lealtad superior hacia otras normas con las que se identifica el ofensor[5].

Considero que todas las técnicas de neutralización pueden ser utilizadas en el ciberespacio, todo dependerá del enfoque analítico que se le dé a cada caso en concreto. Para ejemplificarlo de forma clara, tomaré solamente una de ellas.

En un caso de ciberacoso, el delincuente sin duda alguna tiene conocimiento de la ilicitud de su conducta, pero esto no quiere decir que va a dejar de hacerlo. Si el ciberacoso se realiza sobre una persona que ha causado algún tipo de daño al ofensor, supongamos un antiguo bravucón de su escuela, un posible argumento del ofensor para justificar su conducta podría ser "este tipo lo merece, durante mucho tiempo abusó de mi", por lo que, estaría negando la calidad de víctima de la persona a quién está acosando, tratando de forzar una lógica que da a entender que merece el daño que le sucede.

VI. Tipos de desplazamiento en la ciberdelincuencia

Para conocer cuáles son los tipos de desplazamiento que pueden presentarse en la cibercriminalidad, considero necesario explicar lo que significa el desplazamiento y los tipos existentes en primer lugar. Este problema criminológico tiene relación con la oportunidad delictiva y la prevención situacional. Al buscar un mecanismo de prevención, dirigido a reducir o eliminar la oportunidad efectiva para que el delincuente realice la ofensa, puede presentarse el desplazamiento.

5 Para mayor desarrollo véase: Técnicas de neutralización: una teoría de la delincuencia (Sykes & Matza, Técnias de neutralización: una teoría de la delincuencia, 2008).

Este último consiste en que puede darse el caso de que, al reducirse las oportunidades delictivas en un lugar o a un tipo de delitos, también la atención de los delincuentes se dirija hacia otros lugares o tipos de delitos (Serrano Maíllo A., 2017), es decir, que adecúan su conducta para poder materializar el delito con distintas condiciones. Justamente, el profesor Alfonso Serrano Maíllo señala que la doctrina contempla las siguientes posibilidades de desplazamiento:

a. Temporal: el delito se pospone para otro momento que se considere menos peligroso.

b. Espacial: el delito que se tenía pensado cometer, se lleva a cabo en otro lugar en que sea más sencillo realizarlo sin ser detectado.

c. Táctico: cometer el mismo delito, pero de forma diferente.

d. De objetivo: se busca un objeto que sea más sencillo de victimizar.

e. De tipo de delito: se comete en un delito distinto del que se tenía pensado en un primer momento.

f. Desplazamiento del ofensor: cuando un nuevo delincuente sustituye al que ha sido detenido o ha desistido de su delito (Teoría criminológica: la explicación del delito en la sociedad contemporánea, 2017)

De este listado corresponde ahora hacer un análisis sobre qué formas de desplazamiento pueden ser observados en la ciberdelincuencia. El primer tipo de desplazamiento que se puede aplicar en la ciberdelincuencia es el de objetivo, mismo que puede darse con amplia facilidad en el entorno virtual. Al elegir un objetivo e intentar acceder a su información, por ejemplo, puede darse que se encuentre protegido a un nivel muy alto, o haya tomado acciones que puedan imposibilitar el cometimiento del delito. El ofensor podrá buscar en la red otros objetivos menos preparados para el ataque con mucha facilidad al existir tantos usuarios.

Por otro lado, un segundo tipo de desplazamiento aplicable al ciberdelito es el táctico. El ofensor puede variar la técnica de materialización

dependiendo de lo que llegue a necesitar en relación con las vulnerabilidades en software y hardware (Jansen & Van Lenthe, 2016), debido a la complejidad que cada une implique.

El desplazamiento temporal también es aplicable a la ciberdelincuencia. Su relevancia es prácticamente nula al entender que el cibercrimen no se enfrenta a barreras espaciales ni temporales (Jansen & Van Lenthe, 2016), dejando a su aplicación casos extraordinarios. Mientras que, el desplazamiento de tipo de delito si se aplica de forma más común en la ciberdelincuencia, permitiendo un cambio entre un delito cibernético a otro, o de un delito cibernético a un delito en el entorno físico.

El desplazamiento espacial también puede aplicarse al ciberdelito, pero debe cambiar sus conceptualizaciones. Como se mencionó anteriormente, el ciberespacio no tiene límites espaciales, por lo que aquí se debería distinguir a los "espacios en línea" (Jansen & Van Lenthe, 2016). A manera de ejemplo, puede entenderse como un espacio en línea a un foro online.

Para finalizar, el desplazamiento del ofensor tiene total cabida en el ciberdelito. Se debe entender que la red facilita el anonimato de las personas (por ende, también de ofensores), por lo que, muchos delitos cibernéticos son realizados por personas distintas, dando continuación a actividades delictivas ya iniciadas por alguien más. Un ejemplo se da con los ataques spam, en los que los patrocinadores pueden cambiar a otros spammers si los que contrataron son atrapados.

De esta manera, se evidencia que los diferentes tipos de desplazamiento pueden llegar a aplicarse en el cibercrimen; algunos con adaptaciones, otros con los mismos elementos del entorno físico, y otros en mucha menor medida, como es el caso del desplazamiento temporal.

VII. ¿Cómo combatir la ciberdelincuencia?

Tal como hemos podido observar a lo largo de este artículo, hay algunos puntos en común en los que convergen quienes se han dedicado a estudiar la ciberdelincuencia. Sobre todo, respecto a lo atrayente que

es este tipo de criminalidad por la facilidad con la que hoy se pueden realizar este tipo de ataques[6], los bajos niveles de riesgo que conlleva y los beneficios cuantiosos que se pueden obtener sin requerir del mismo esfuerzo que se necesita en el espacio físico.

Así mismo, el ciberespacio se ha convertido en el lugar idóneo para obtener datos e información de todo tipo de cualquier persona, organización, institución o Estado. Esto es resultado de la globalización de la información y el avance de las nuevas tecnologías como herramienta para establecer comunicaciones y conexiones libres.

Frente a este contexto, los países se han centrado principalmente por mejorar e implementar medidas de seguridad informáticas como la protección a datos públicos, especialmente por la afectación a sus instituciones estatales[7]. El acelerado crecimiento de las redes criminales y la sofisticación de los ciberataques han llevado a que los Estados soliciten asesoría privada para la implementación de políticas públicas y programas de seguridad (Ochoa Marcillo, 2021).

Según el Índice de Ciberseguridad Global que mide indicadores basados en los niveles de seguridad y protección de datos públicos y privados de varios países del mundo en una escala de 0 a 1. Los países que lideran este ranking son Reino Unido (0.93), Estados Unidos (0.92) y Francia (0.91). En relación con Latinoamérica, Uruguay ocupa la posición 51 con 0.68 puntos, México posición 63 con 0.62, Paraguay posición 66 con 0.60, mientras que Ecuador en la posición 98 con 0.36 puntos (ITU, 2017).

Uno de los conceptos que han surgido para encasillar a varias estrategias direccionadas a combatir la ciberdelincuencia es la gobernanza de

6 Me refiero a la facilidad con la que se puede cometer un ciberdelito que su naturaleza misma no implique el conocimiento de técnicas informáticas de vulneración más complicadas. Por ejemplo: cualquiera de nosotros puede ser un ciber acosador solamente con crearse una red social.

7 Un ejemplo de esto puede ser el reciente ataque que se dio contra la Corporación Nacional de Telecomunicaciones, en el cual existía mucha confusión respecto al tipo de vulneración que sufrió la institución, pero se hablaba de la sustracción de información relacionada con datos personales de los usuarios.

la ciberseguridad. En ella se propone la instauración de una cultura de ciberseguridad que se someta a principios éticos y responsables en el tratamiento de la información y la comunicación, mismos que deben tener alcance en todos los actores sociales e instituciones (Mehan, 2014).

Para alcanzar la gobernanza de la ciberseguridad se necesita de un conjunto de políticas integrales y coherentes que deriven en una mejor forma de organización. Así existirá más probabilidad de anticiparse a futuros riesgos, aunque es necesario advertir que el factor de vulnerabilidad siempre estará presente por la constante evolución y avance de la tecnología (Ochoa Marcillo, 2021).

En la misma línea, Fernando Miró ha dado algunas recomendaciones para reducir los riesgos de ser víctimas de ciberdelitos. Estas indicaciones están dirigidas al ámbito preventivo en su mayoría.

En primer lugar, indica que se deben identificar zonas de riesgo. Esto se logra mediante campañas de información sobre riesgos, avisos en red de infección de spam, sistemas de listas blancas y negras de webs y spam, entre otros. Señala también que se deben separar los objetivos, cuestión que puede conseguirse creando subredes de seguridad o separando la información. En el mismo sentido, también resulta efectivo ocultar los objetivos, cuestión que se puede realizar mediante encriptación, evitar el uso de datos personales en la red, o mejorar los niveles de protección de los canales de pago online (Miró, 2012).

El autor tambien señala que es importante descontaminar constantemente las máquinas con las que trabajamos y en las que almacenamos información, ya que, es más probable la presencia de virus mientras menos desinfección se haga; para esto se necesita también un buen sistema de detección de intrusos como herramientas antispam, antivirus, etc. En relación con lo último, se debe controlar el acceso al sistema, es decir, limitar quienes puede acceder a lo que se busca proteger, cuestión que se puede alcanzar, por ejemplo, mediante el uso de claves y su renovación continua (El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio, 2012).

Entre las acciones que pueden permitir la prevención del cibercrimen, pero al mismo tiempo pueden servir para perseguirlo, encontramos en primer lugar que se debería aumentar el número de guardianes, esto no quiere decir que se aumente la cantidad de personas que están cuidando la información, sino que se implementen guardianes virtuales, por ejemplo: moderadores de foros, sistemas echelon, enfopol, carnivore, etc. En este mismo sentido, también se debería reforzar la vigilancia formal a través de equipos especializados de persecución del cibercrimen o grupos encargados de identificar el ciberdelito y darle seguimiento (Miró, 2012).

Por último, la mayor recomendación es el establecimiento de reglas internacionales, acompañado de canales de cooperación que permitan más celeridad y eficacia en el combate al cibercrimen[8]. Al tratarse de un fenómeno transnacional, que puede ejecutar desde cualquier parte del mundo sin la necesidad de estar presente en el espacio físico en donde se encuentra el objetivo, la ciberdelincuencia se beneficia del trato diferenciado que da la legislación interna de cada país al problema.

Al no existir una forma concreta de combatirlo, o incluso al existir realidades en donde ni siquiera se da un tratamiento a esta criminalidad, las normas pueden convertirse en un límite y, por ende, obstáculo en la lucha contra el ciberdelito. La armonización internacional del derecho en este ámbito libera la posibilidad de unir esfuerzos para que las soluciones que se pretendan ejecutar también sean globales.

VIII. Esfuerzos de Ecuador ante la ciberdelincuencia

Desde el aspecto preventivo, en Ecuador se propuso la Estrategia Nacional de Ciberseguridad, trabajando juntamente con el Banco Interamericano de Desarrollo y la consultora NRD Cyber Security, bajo directrices y coordinación del Ministerio de Telecomunicaciones; sin embargo, no hay más información al respecto.

8 Para más desarrollo véase: Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia (Flores Prada, 2015) & La ciberdelincuencia (Cordero Ruiz, 2021).

El objetivo planteado en esta estrategia es establecer líneas de acción en cuanto a la ciberseguridad en coordinación con sectores públicos, privados, academia y sociedad civil para fortalecer la seguridad y gestionar los riesgos del ciberespacio de forma integral (MINTEL, 2018).

Con esta iniciativa se busca gestionar la infraestructura de la información, analizar el marco legal penal ecuatoriano, la cooperación internacional, la formación y capacitación y la institucionalidad de la ciberseguridad. Entre los principales programas están la seguridad de información y uso responsable de las TIC, economía digital, tecnologías emergentes, fortalecimiento de la inclusión digital y la protección de datos.

Se creó el Centro de Respuesta a Incidentes Informáticos del Ecuador (EcuCERT) con la misión de brindar apoyo para prevenir y resolver incidentes en materia de seguridad informática. El resultado esperado es la masificación del uso seguro de internet, las TIC y los sistemas de telecomunicación. Este centro está direccionado a seguir las posibles amenazas y vulnerabilidades a las redes informáticas del Ecuador (ARCOTEL, 2021).

Con la vigencia del Código Orgánico Integral Penal en el año 2014, se introdujeron nuevos tipos penales relacionados con la ciberdelincuencia. En esta normativa se reflejan 15 artículos referentes al delito informático, por ejemplo: art. 103: pornografía con utilización de niños, niñas y adolescentes; y, art. 190: apropiación fraudulenta por medios electrónicos.

Con relación a ciberataques puros, el COIP contempla 5 tipos penales: revelación ilegal de base de datos, interceptación ilegal de datos, transferencia electrónica de activo patrimonial, ataque a la integridad de sistemas informáticos y acceso no consentido a un sistema informático[9].

En el mismo sentido, el 26 de mayo de 2021 se publicó la Ley Orgánica de Protección de Datos Personales con el fin de que esta normativa permita una mejor protección en este campo. La ley contempla un régimen

9 Véase los artículos 229, 230, 231, 232 y 234 del Código Orgánico Integral Penal respectivamente. La redacción de estos tipos penales previene la única posibilidad de que se materialicen en el ciberespacio.

sancionatorio para algunas conductas que puedan llegar a afectar el tratamiento de datos personales (Naranjo & Subía, 2021). Habrá que ver si la tipificación de este tipo de conductas influye sobre los ofensores en relación con la prevención, ante lo cual la literatura pone resistencia con bases empíricas. Sobre todo, si se toma en cuenta la transnacionalidad de estos delitos y las altas probabilidades de impunidad (Kemp, 2021).

En este punto resulta adecuado mencionar que Ecuador se ubicó en el puesto 8 del ranking global 2018 de pishing y tiene un nivel bajo en ciberseguridad (0,367 puntaje IGC) (Ochoa Marcillo, 2021). Las capacitaciones sobre ciberseguridad se han llevado a cabo mayormente por el sector privado, cuándo esto debería ser una iniciativa estatal para facilitar la ciberprotección en todos los niveles.

Los efectos de las estrategias y planes estructurados no son visibles debido a que no existe información respeto a su ejecución. Sin embargo, e puede decir que el trabajo de las agencias encargadas de atender las emergencias relacionadas con ciberseguridad no ha sido efectivo si tomamos en cuenta que los ciberdelitos tienen más espacio en nuestra realidad cada año[10].

La misma lógica anterior puede ser aplicada para los efectos que se han derivado de la tipificación de nuevas conductas relacionadas con el ciberespacio. Es decir, la creación de nuevos delitos en el código penal tampoco ha surtido efectos que reduzcan la presencia de esta criminalidad; sino que, la tendencia ha ido al aumento.

Para finalizar, es importante indicar que Ecuador no forma parte del convenio de Budapest sobre Ciberdelincuencia, ni de ningún otro instrumento internacional relacionado con la materia. La importancia de la armonización del derecho a nivel internacional en este ámbito y el establecimiento de relaciones de cooperación resultan fundamentales para lograr crear estrategias eficaces que, de alguna forma, permitan combatir la ciberdelincuencia. Por lo tanto, es urgente aumentar los esfuerzos y establecer vínculos de cooperación.

10 Esto puede observarse en el apartado “La ciberdelincuencia en cifras”.

IX. Conclusiones

Es evidente el desarrollo de la tecnología y todo lo que ella representa dentro de nuestra realidad. Las nuevas formas de comunicarse, intercambiar ideas, palabras, fotografías, o todo tipo de información a través de las redes, emergen cada día. Como bien se señaló, la brecha entre el ciberespacio y el entorno físico cada vez es menor. Hoy en día se puede hacer prácticamente todo lo que es realizable en el mundo físico.

Este avance no conlleva solamente beneficios, sino que, muchos de los problemas del mundo "exterior" también han encontrado un lugar en el ciberespacio. La ciberdelincuencia es una nueva forma de criminalidad que se vincula directamente con Internet y las TIC, a tal punto que su expansión va de la mano. Pese a que existan distintas concepciones del fenómeno, en todas ellas es fundamental el papel de la red y los medios tecnológicos.

Existen varias formas de clasificar los ciberdelitos, muchas de ellas dependen de características propias de las conductas, así como existen otras que atienden a factores distintivos externos a ellos. Las distintas clasificaciones existentes pueden complementarse para brindar una percepción más adecuada de cada ciberdelito.

Al ser un tipo de criminalidad distinta de la tradicional, puede simplemente asumirse que las teorías criminológicas que abordan la delincuencia en el mundo físico no se podrían aplicar en ella. Sin embargo, hemos podido observar cómo algunas de las teorías más discutidas también pueden adecuarse a la ciberdelincuencia. Esto no quiere decir que ellas sean suficientes para explicar este tipo de criminalidad, sino que, pueden servir para tener una mejor comprensión de estas conductas y continuar en la elaboración de nuevas teorías más completas.

Así mismo, podría parecer que la ciberdelincuencia como tal es una forma de desplazamiento delictivo, cuestión que no me atrevo a descartar tomando en cuenta que los ciberataques réplica pueden ser un ejemplo de esto. Sin embargo, no toda la delincuencia tradicional se ve reflejada en el ciberespacio, por lo que, tampoco es preciso afirmar que este tipo de criminalidad en general sea una forma de desplazamiento. Todo dependerá

del enfoque y el delito. Algo que sí pudimos observar es que este problema criminológico puede presentarse también dentro de los ciberdelitos.

El problema de la ciberdelincuencia radica principalmente en que la naturaleza misma del ciberespacio, basada en libre intercambio de información y el surgimiento de nuevas conexiones, genera las condiciones adecuadas para que el delincuente encuentre aquí un sitio en el que pueda ejecutar actos delictivos de manera más sencilla y con menos control. Esto genera que la cibercriminalidad sea cada vez más atrayente para los ofensores, cuestión que se evidencia con las cifras expuestas indicativas de una mayor presencia de ciberdelitos en el espectro social con el paso del tiempo.

Es por esta misma razón que los esfuerzos para combatirla tambien deben avanzar. Un fenómeno con alcance mundial requiere de unión y cooperación, por lo que, resulta prioritaria y urgente la armonización del marco legal que le da tratamiento. Es necesario que todos los actores sociales, a nivel micro y macro, trabajen continuamente por la protección en el ciberespacio.

Referencias bibliográficas

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

Holt, T., Bossler, A., & Seigfried-Spellar, K. (2017). Cybercrime and Digital Forensics an Introduction. Nueva York.

Cohen, E. (1955). Teoría de las subculturas delictivas.

Serrano Maíllo, A. (2017). Teoría criminológica.

Jansen, F., & Van Lenthe, J. (2016). Cybercrimne Through an Interdisciplinary Lens. Londres.

Fernández - Rodríguez, J. C., Miralles Muñoz, F., & Millana Cuevas, L. (2019). Perfil psicológico en el ciberdeilncuente. *Revista Iberoamericana de las Ciencias Sociales y Humanísticas*.

Cámara Arroyo, S. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social*, 470-512.

Sain, G. (2015). Historia de Internet. *Revista pensamientp penal*.

Mateos Pascual, I. (septiembre de 2013). Ciberdelincuencia. Desarrollo y persecución tecnológica. *Ciberdelincuencia. Desarrollo y persecución tecnológica*. Madrid, España: Universidad Politécnica de Madrid.

Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Revista Latinoamericana de Estudios de Seguridad*, 80-93.

Fernández Bermejo, D., & Martínez Atienza, G. (2020). *Ciberdelitos*. Ediciones Experiencia.

Trochez Arias, I. (2020). *Universidad Santiago de Cali*. Obtenido de https://repository.usc.edu.co/bitstream/handle/20.500.12421/4251/REVISI%c3%93N%20DE%20LA%20CLASIFICACI%c3%93N.pdf?sequence=3&isAllowed=y

Wall, D. (2008). *Hunting shooting and Pishing: New Cybercrime Challenges for Cybercanadians in the 21st Century*. British Library.

Wall, D. (2005). *What are Cybercrimes?* California: Sage Publications.

Giménez Solano, V. (2011). Hacking y ciberdelito. *Hacking y ciberdelito*. Valencia, España: Universitat Politécnica de Valencia.

López Sánchez, J. (enero de 2019). Métodos y técnicas de detección temprana de casos de phishing. *Métodos y técnicas de detección temprana de casos de phishing*. Barcelona, España: Universitat Oberta de Catalunya.

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

Luciano, G., & Lo Giudice, M. E. (octubre de 2015). *UADE*. Obtenido de https://repositorio.uade.edu.ar/xmlui/bitstream/handle/123456789/4243/A14S20%20Material%20Did%c3%a1ctico%202.pdf?sequence=4&isAllowed=y

Universidad Veracruzana, U. (18 de mayo de 2015). *Universidad Veracruzana*. Obtenido de https://www.uv.mx/infosegura/general/noti_scam-3/

UNICEF, U. (octubre de 2021). *UNICEF*. Obtenido de https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

Brown, I., & Korff, D. (2009). Terrorism and the Proportionality of Internet Surveillance. *European Journal of Criminology*, 119-134.

Loreto, V. (2004). ¿Movimientos sociales en la red? Los hacktivistas. *El Cotidiano*, 0.

INTERPOL. (2020). Obtenido de INTERPOL: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

BID, B., & OEA, O. (2020). *Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y El Caribe*. OEA.

El Universo, E. (25 de mayo de 2021). *El Universo*. Obtenido de El Universo: https://www.eluniverso.com/noticias/seguridad/mas-de-600-denuncias-por-delitos-ciberneticos-se-han-registrado-en-ecuador-en-lo-que-va-del-2021-nota/

PORTAFOLIO. (15 de septiembre de 2020). *PORTAFOLIO*. Obtenido de PORTAFOLIO: https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642

López - Fonseca, Ó. (07 de junio de 2020). *El País*. Obtenido de https://elpais.com/espana/2020-06-07/los-ciberdelitos-son-ya-el-10-de-las-infracciones-penales-conocidas.html

Sykes, G., & Matza, D. (2008). Técnias de neutralización: una teoría de la delincuencia. *Delito y sociedad*, 163-171.

Tejión Alcalá, M. (2019). Las teorías de la frustración en la sociedad contemporánea. Un análisis multinacional de los efectos de la frustración y la ira en conductas antisociales. *Las teorías de la frustración en la sociedad contemporánea. Un análisis multinacional de los efectos de la frustración y la ira en conductas antisociales*. Madrid, España: UNED.

Hikal, W. (2017). La teoría de la asociación diferencial para la explicación de la criminalidad y la articulación de una política criminal. *Derecho y cambio social*.

Flores Prada, I. (2015). Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia. *Revista Electrónica de Ciencia Penal y Criminología*.

Cordero Ruiz, N. F. (2021). La ciberdelincuencia. *La ciberdelincuencia*. Alcalá, España: Universidad de Alcalá.

Wall, D. (2007). *Cybercrime: the transformation of Crime in the Information Age.* Cambridge Polity.

Yar, M., & Steinmetz, K. (2019). *Cybercrime and society* (Tercera ed.). SAGE.

Paloque - Bergés, C., & Schafer, V. (2019). Arpanet (1969-2019). *Internet Histories*, 1-14.

Reyes Neira, J. M. (29 de septiembre de 2015). Ciberdeilncuencia: una realidad virtual contada a medias. *Ciberdeilncuencia: una realidad virtual contada a medias*. Bogotá, Colombia: Universidad Piloto de Colombia.

Garrido, V., Stangeland, P., & Redondo, S. (2006). *Principios de criminología.* Valencia: Tirant lo Blanch.

De la Cuesta, J. L., & Pérez Machío, A. (2010). Ciberdelincuentes y cibervictimas. En J. L. De la Cuesta, & N. De la Mata, *Derecho penal informático* (págs. 99-120). Madrid: Civitas.

González García, A., & Campoy Torrente, P. (2018). Ciberacoso y cyberbullying: diferenciación en función de los precipitadores situacionales. *Revista Española de Investigación Criminológica*.

Ministerio del Interior, E. (2017). *Estudios sobre la cibercriminalidad en España.* Madrid: Ministerio del Interior.

Caneppele, S., & Aebi, M. (2017). Crime drop or police recording flop? on the relationship of decrease of offline crime and the increase of online and hybrid crimes. *Journal of Policy and Practice*.

Roca, J. L. (28 de marzo de 2014). Cibercrimen y ciberterrorismo: ¿exageración mediática o realidad? *Trabajo de Fin de Grado*. Madrid, España: Universidad Politécnica de Madrid.

Ministerio del Interior, E. (2019). *Estudio sobre la cibercriminalidad en España*. Madrid: Ministerio del Interior.

Merton, R. (1968). *Teoría y Estructuras Sociales*. Columbia: Columbia University.

Matsueda, R. L. (1988). The current state of differential association theory. *Crime & delinquency*, 277-306.

Hirschi, T. (2003). Una teoría del control de la delincuencia. *Capítulo Criminológico*, 5-31.

Gottfredson, M., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Rodríguez, J., Oduber, J., & Mora, E. (2017). Actividades rutinarias y cibervictimización en venezuela. *Revista Latinoamericana de Estudios de Seguridad*, 63-79.

Summers, L., & Rossmo, K. (2015). Aplicaciones prácticas de la teoría de las actividades rutinarias a la investigación criminal. *Crimen, oportunidad y vida diaria: libro homenaje al profesor Dr. Marcus Felson*, 171-186.

Sykes, G., & Matza, D. (1957). Técnicas de neutralización: una teoría de la delincuencia. *American Sociological Review*, 664-670.

Serrano Maíllo, A. (2017). *Teoría criminológica: la explicación del delito en la sociedad contemporánea*. Dykinson.

ITU, I. T. (2017). *Global Cybersecurity Index*. International Telecommunications Union.

Ochoa Marcillo, A. (2021). Trabajo de fin de máster. *Desafios globales del cibercrimen*. Quito, Ecuador: Universidad Andina Simón Bolívar.

Mehan, J. (2014). *CyberWar, CyberTerror, CyberCrime and CyberActivism*. Ely, UK: It Governance Publishing.

MINTEL, M. d. (2018). *Plan Sociedad Información*. Obtenido de Estrategia Nacional de Ciberseguridad: https://plansociedadinformacion.mintel.gob.ec/pr1/p1-proy1/

ARCOTEL, A. d. (2021). *Ecucert*. Obtenido de Centro de respuesta a incidentes informáticos del Ecuador: https://www.ecucert.gob.ec/centro-de-respuesta-a-incidentes-informaticos-del-ecuador/

Kemp, S. (22 de septiembre de 2021). Ciberdelincuencia. (R. Bolaños, Entrevistador)

Naranjo, J., & Subía, M. (30 de mayo de 2021). *Naranjo, Martínez & Subía*. Obtenido de https://nmslaw.com.ec/ley-organica-proteccion-datos-personales/