CIBERCRIMINOLOGÍA

LA CRIMINOLOGÍA DE LA NUEVA ERA.

Jesús Florentino García V.

Jefe del Departamento de Criminología de la extinta Policía Federal México. Docente de la Licenciatura en Criminología y Coordinador de la Maestría en Victimología, del Colegio de Estudios de Posgrados de la Ciudad de México.

Abstract

El presente artículo pretende comprender como la evolución de las tecnologías, las comunicaciones y la información, han llevado a la humanidad a tener un estilo de vida diferente, principalmente en el espacio digital, en el que se encontrará expuesto a circunstancia que lo pueden llevar a su victimización, por ello la Criminología como ciencia encargada del estudio de las causas del comportamiento desviado, aplicara sus conocimientos dentro del ciberespacio, a lo que se denominara Cibercriminología, la cual a través de una metodología analítica y científica buscara las causas del cibercrimen, y con apoyo de la Cibervictimología, tratar de conocer las factores que pudieron influenciar a la victimización del cibernauta.

Hoy en día el número de cibervíctimas y cibercriminales dentro del ciberespacio a incrementado de manera considerable, lo que han relacionado principalmente a cuestiones informáticas, tecnológicas y de ciberseguridad, sin tomar en consideración los aspectos personales que pueden influenciar (económico, psicológico, educativo, social, entre otros), lo que ha permitido establecer una clasificación de cibercrímenes, los cibercriminales y las cibervictimas, desde los aspectos sociales.

Palabras Clave: Cibercrimen, Cibervictimización, Cibercriminología, Civervictimología, Clasificación Cibervictimológica, Tipo de Cibercriminales.

CIBERCRIMINOLOGÍA

LA CRIMINOLOGÍA DE LA NUEVA ERA.

En los últimos años la sociedad ha evolucionado y cambiado su forma de vida, gracias a las Tecnologías de Información y Comunicación (TIC), así como a los avances de esta nueva era digital, tanto en redes sociales y plataformas de comunicación, permitiendo cambios radicales en la comunicación, desarrollo social, económico, político, científico, entre otros; facilitando las actividades, que por mucho tiempo fueron del espacio físico, y hoy se desarrollan a través del espacio digital, pero así mismo se ha presentado un aumento del comportamiento delictivo contra los cibernautas.

Una de las problemáticas que ha permitido este aumento, se debe al pausado avance de las legislaciones que permitan la debida investigación y persecución jurídica, sin embargo, Gracias al Convenio de Budapest en el año 2001, se establecieron los primeros antecedentes sobre delitos contra los sistemas y/o medios informáticos, en los que se consideran como primera instancia aquellos delitos cometidos contra la integridad, la confidencialidad y los datos de la información, velando por los derechos humanos de carácter fundamental; pero como en los aspectos penales y jurídicos que se han desarrollado a través de la historia, estos se enfocan en la conducta y el agresor, y que a pesar de que se trata de velar por los derechos humanos, las victimas pasan a un segundo término.

Otros de los aspectos que han permitido el aumento de estos delitos se deben a la falta de conocimientos en materia de Seguridad de la Información, pues la falta de cultura digital facilita estos delitos, principalmente en los aspectos vulnerabilidad, riesgos y amenazas que se puedan tener o generar; lo que ha puesto en juego las habilidades y destreza del Cibercriminal, a fin de establecer procesos de victimización más eficientes.

Es necesario señalar que dentro de los delitos cometidos en la red pública de internet, se habla de términos como vulnerabilidad, amenazas y riesgos, estos enfocados a aspectos electrónicos y/o digitales, más no personales; lo que lleva a las áreas de investigación, a tratar de comprender las circunstancias o factores que influyeron para la comisión del crimen, desde los aspectos sociales, más allá de los aspectos digitales, informáticos y tecnológico.

Día con día los delitos a investigar se ven más relacionados con las tecnologías y/o medios digitales más actuales, lo que ha llevado a que diversas materias y disciplinas, principalmente de carácter forense, a intervenir en las indagatorias, una de ellas la Criminología convencional, aplicada al espacio físico, la cual se ha visto en la necesidad de exportar sus conocimientos al espacio digital, por lo que hoy se ha denominado ***CIBERCRIMINOLOGÍA***.

En el año 2007, Jaishankar Karuppannan define por primera vez a la Cibercriminologia como la encargada del estudio de las causas de los delitos que se desarrollan en el ciberespacio, y el impacto generado en el espacio físico, a través del estudio del comportamiento criminal y victimización dentro del espacio digital, a partir de la criminología y las teorías aplicables; lo que lo lleva a posicionarse como el padre de la Cibercriminología. (Arroyo, 2020)

Por otra parte, el Dr. Kyung-shick Choi y el Teniente Coronel Marlon Mike Toro-Álvarez, ambos Cibercriminólogos y expertos en Ciberseguridad, escriben el primer libro en español titulado "*Cibercriminología: guía para la investigación del cibercrimen y mejores prácticas en seguridad digital*", dentro del cual

establecen que la Cibercriminología se encargara del estudio de los diversos escenarios, factores y/o causas que permiten la materialización del cibercrimen.

Con lo que hoy sabemos de Criminología, la evolución agigantada de las TIC y las repercusiones que se han presentado dentro de las sociedad, podremos decir que la Cibercriminología se encargara de *conocer, identificar y comprender el comportamiento antisocial como criminal dentro del mundo digital y el uso de medios tecnológicos para el desarrollo de conductas antisociales como delictivas*; al igual que la Criminología en el espacio físico, pero está en el espacio digital; pues a través de los años se ha tratado de identificar o comprender la naturaleza del origen del comportamiento desviado, llevando al surgimiento de diversas teorías para la explicación del mismo.

Dentro de las teorías criminológicas existen diversas teorías utilizadas para comprender el comportamiento desviado en el espacio físico, como la teoría de la tensión, las actividades cotidianas, de aprendizaje social y vínculos sociales, sin embargo hoy el uso y manejo de tecnologías de la información, la comunicación y el internet, han permitido el desarrollo de nuevas teorías o posturas, la primera de ellas la Teoría de la Transición Espacial de Jaishankar del 2008 (Arroyo, 2020), en la cual se establece que los comportamiento criminales que en algún momento se llevaron en el espacio físico, transitara al espacio digital influenciados diversos factores que abarcaran el ciberespacio, entre los que destacan el anonimato, la falta de su regulación y disuasión, sin dejar de considerar las características del delincuente.

Por otra parte, se trata de conocer las características y vulnerabilidades de las víctimas dentro del ciberespacio las cuales serán *Cibervíctimas*, siendo aquella encargada de determinar el proceso de victimización, para el espacio digital, *Cibervictimización* (García, Pérez, González, & Pérez, 2016), la cual consiste en el padecimiento de agresiones realizadas a través del internet o algún medio tecnológico, esto por parte de la Victimología, la cual, dentro del mundo digital, se ha denominara como ***CIBERVICTIMOLOGÍA***.

La Cibervictimología es un termino poco definido o conceptualizado dado al desconocimiento de sus alcances. Zamora (2016) la establece como la encargada del estudio de las formas de victimización en el espacio virtual y los efectos que produce en la vida de las víctimas.

Por otra parte, es señalada como parte de la Cibercriminología que se ocupara del estudio de las víctimas de los ciberdelitos, que sufren ataques cometidos a través de la tecnología. (Rubio & Selma, 2020)

La victimización dentro del ciberespacio se puede ver influenciada por diversas causas y factores, tanto personales, sociales e incluso materiales, por lo que hoy en día podemos definir a la Cibervictimología, como la rama de la Victimología que se *encarga del estudio de la víctima dentro del espacio digital, a fin de comprender y conocer los elementos personales, digitales y tecnológicos que influyeron o la llevaron a la cibervictimización*; y que al igual que la Victimología, partirá de la valoración de los hechos y las circunstancias del crimen, a fin de determinar los niveles de riesgo y de vulnerabilidad que presenta una víctima, lo que permitirá establecer el proceso de victimización.

La victimización del espacio físico, no tiene un camino específico, a diferencia de la cibervictimización, pues este más que un

proceso se pudiera considerar un ciclo, ya que existe una planificación, organización, selección de objetivos, ejecución e innovación; lo que eleva los niveles de riesgo dentro del ciberespacio. El conocer dicho proceso y/o ciclo permitirá su clasificación cibervictimológica, esto con base a las múltiples clasificaciones que existen, pero ahora dentro del ciberespacio.

Sin embargo, dentro de la red pública de internet existen circunstancias infinitas que pueden llevar a la victimización de los cibernautas, pero las circunstancias victimológicas serán delimitadas, por los aspectos tecnológicos, digitales y personales de las cibervíctimas, lo que permite clasificarlas al menos seis tipos:

CLASIFICACIÓN CIBERVICTIMOLOGICA

Cibervíctimas altamente vulnerables: dentro de esta clasificación se encontraran a todas aquellas personas que no cuentan con conocimientos mínimos y/o básicos en el manejo y/o uso de las tecnologías de la comunión, la información y el internet; encontrando principalmente, Niños, Niñas, Adultos Mayores (Tercera Edad), o personas con niveles de estudios básicos.

-**Cibervíctimas de simplicidad**: estas víctimas tienden a ser todas aquellas personas que no verifican la información a la que acceden, quedándose con lo de primero que han apreciado, buscado o encontrado; o aquellas que no validan la veracidad y fiabilidad de las páginas o sitios de acceso, dándoles su voto de aprobación y confianza, lo que permite la cibervictimización.

-**Cibervíctima por necesidad** (afectiva y económica): dentro de esta clasificación podremos encontrar dos tipos de víctimas: las primeras de ellas, atraviesan por situaciones sentimentales y/o emocionales de abandono, ya sea familiar o de pareja, lo que genera una situación de vulnerabilidad donde pueden ser fácilmente enganchadas (principalmente en redes sociales), las cuales por su situación emocional son manipulables fácilmente, para el desarrollo de actos determinados.

Por otra parte, se encuentras las personas que atraviesan situaciones económicas desfavorables, no cuentan con trabajo o sus ingresos son totalmente nulos o insuficientes, lo que las lleva a acceder a determinados actos y circunstancias con la esperanza de satisfacer su necesidad económica, lo que permite su victimización dentro del ciberespacio.

Estas dos cibervictimizaciones pueden ser exportadas al espacio físico posteriormente.

-**Cibervíctimas por participación**: estas serán todas aquellas que le facilitan al cibercriminal los elementos necesarios para su proceso de cibervictimización, a pesar de contar con los conocimientos en el uso y manejo del internet, las tecnologías de la comunión y la información.

-**Cibervíctimas comunitarias**: son todas aquellas personas que pertenecen o forman parte de un grupo, institución y/o sociedad, las cuales se verán afectadas en sus intereses colectivos, a partir de la victimización de la colectividad a la que pertenece.

-**Cibervíctimas de ficción**: estás son todos aquellos cibernautas que se señalan o se creen cibervíctimas de un delito, esto relacionado principalmente con el desconocimiento o confusión de la logística y normatividad de páginas, sitios y/o personas

de los que se dicen víctimas, sin existir en realidad la comisión de un delito.

Una vez conocidas las características de la víctima que permita su clasificación Cibervictimología, se podrán desarrollar las actuaciones Cibercriminológicas en la investigación de delitos relacionados con medios electrónicos o digitales.

A partir de la identificación del tipo de cibervíctima, será necesario identificar el tipo de *Cibercrimen* que se desarrolló; para esto se toma en cuenta las áreas de oportunidad de victimización, la esfera que se ha visto afectada, así como las posibles causas y consecuencias generadas en la victima.

La identificación de dichos aspectos nos permitirá conocer la naturaleza del cibercrimen, a partir del análisis del contexto, los factores de riesgo de forma individual como colectiva, lo que encamina a la Cibercriminología a categorizar el ámbito del delito cibernético en al menos tres esferas.

La primera de ellas de naturaleza ***Social,*** esto derivado que el ser humano hoy se desenvuelve dentro de las redes sociales, en la que se exponen creencias, estilo de vida, estatus económico, entre otros; afectando de forma individualizada, y siendo estos aspectos los que se convierten en su vulnerabilidad, y el área de oportunidad de los cibercriminales, pues a partir del estudio y análisis de la información se podrá desarrollar de forma exitosa la victimización.

Así mismo, encontramos a los delitos de naturaleza ***Económica****,* en la cual se ven afectados los intereses patrimoniales, esto derivado de las negligencias y/o necesidades de las víctimas, independientemente del proceso de cibervictimización ya sea directo o indirecto, es decir, se haya colaborado o no con el cibercriminal.

Y por último encontramos a los delitos cibernéticos de ambiente ***Político****,* los cuales tiene como fin afectar al estado, creando una desestabilidad social, crisis económicas, de seguridad nacional, entre otros.

No obstante, al identificar la naturaleza nos permitirá conocer el tipo de cibercrimen que se ha desarrollado, de acuerdo a los comportamientos antisociales o delictivos identificados, aunados a los fines y objetivos, lo que nos permite conocer al menos las formas del cibercrimen.

El ***Ciberespinoaje*** (Stalkear[1]) es una de las conductas que hoy más se desarrolla dentro del ciberespacio, pues se asecha a los objetivos o a las víctimas de forma constante, esto a través de diversos medias o estrategias, sin que la víctima se pueda percatar, lo que permite a los cibercriminales obtener mayor información de la que se pudiera obtener en el espacio físico, y ser usada a su favor.

Otro de los cibercrimenes que más se desarrollan son aquellos ***Contra la seguridad de la Información***, ya que hoy por la falta de seguridad (digital), en sitios web, páginas, redes sociales, entre otros, se vuelven las áreas de oportunidad perfecta de los cibercriminales, convirtiéndose en la ocasión perfecta para la cibervictimización; el cual podrá tener una naturaleza, social, política o económica.

Los ***Ciberataques – Ataques de intrusión o dirigidos****,* presenta una mayor amenaza o

[1] Búsqueda de información sobre una o varias personas sin el consentimiento de estas, o se den cuenta

riesgo, ya que este tipo de cibercrimenes son de más carácter político o empresarial, lo que puede orillar al surgimiento de conflictos políticos que pueden desencadenar ciberguerras o incluso guerras en el espacio físico.

Estos tipos de delitos permiten a la Cibercriminología clasificar a los *Ciberdelincuentes* o *Cibercriminales,* tal como lo hace el Dr. Cámara Arroyo: Toolkit/newbies, Ciberpunks, Internals, Cordes, Cyberterrorits, esto de acuerdo al nivel de uso y manejo de las Tecnologías de Información y Comunicación; por lo que la Cibercriminología los clasificara como:

Fuente: Red pública de internet.

TIPO DE CIBERCRIMINALES

- **Novatos** (Toolkit/newbies): serán todas aquellas personas que, con conocimientos simples y básicos de las TIC, operan a través de softwares de dominio público y redes del tipo social, para el desarrollo de actos criminales.
- **Vándalos** (Ciberpunks): estos son los cibercriminales con conocimientos en sistemas, con el objetivo de alterar sitios web, distribuir virus a través de spam, así como desarrollar actos de vandalismo dentro del ciberespacio.
- **Vengativo económico, político y/o social** (Internals): este tipo de agresores formaron o forman parte de estructuras organizacionales del sector público o privado o relaciones interpersonales, contra las que presentan resentimiento, llevándolo a cometer actos de venganza, ya sea a través del daño de sistemas de seguridad o divulgación de la vulnerabilidad de la organización, secretos políticos o personales.
- **Ocioso** (Cordes): Conocidos como codificadores, encargados del desarrollo de sistemas maliciosos (malware) sin un objetivo en específico.
- **Extremista** (Cyberterrorits): agresores con el más alto nivel en conocimientos en el manejo y uso de TIC, con la finalidad de realizar ciberespinoajes o ciberataques en contra del Estado.

Todos estos Cibercriminales cuentan con un factor a su favor, el anonimato, lo que permite que el desarrollo de sus actividades sea difícil de rastrear y conocer, mas no imposible; sin embargo, esto permite que los índices de *Cibercriminalidad* seas mayores que en el espacio físico.

Para este caso la cibercriminalidad se limitará a todas aquellas conductas desviadas o delictivas ocurridas en el ciberespacio, sin importar que posteriormente puedan emigrar al espacio físico, por ello, no pierde su categoría de cibercrimen, pues este se originó dentro o a través de la red pública de internet.

El conocimiento del tipo de cibervíctima, la naturaleza y tipo del cibercrimen, así como el Cibercriminal e información de la investigación criminal permite a la Cibercriminología el desarrollo del *Ciberperfil criminal*, con el cual se aportarán elementos para las áreas de investigación e inteligencia, a reducir el número

de sospechosos, identificar otros cibercrimenes que se puedan relacionar a la misma persona, o incluso la identificación directa del probable responsable.

Aunque el tema de la Cibercriminología pareciera un tema de investigación y análisis de actual para México, no es así, ya que desde el año 2015 se comenzó con la aplicación de estudios Cibercriminológicos por parte de la Extinta Policía Federal (México) en colaboración de la Procuraduría General de la República (PGR) y Fiscalías Generales de Justicia, en la investigación de delitos de alto impacto como: Secuestro, Trata de Personas, Delincuencia Organizada, Narcotráfico, Tráfico de Armas, Fraudes, Extorsiones, entre otros; con los cuales se logró la identificación de zona de operaciones, modus operandi, probables responsables y sus detenciones.

Por otra parte en el año 2018 a través de RedCiber, se realiza el I Simposio de Cibercriminologia y Ciberseguridad, en Colombia, el cual conto con diversas personalidades especialistas en el tema, tales fueron los casos del Dr. Kyung-shick Choi y el Dr. Emanuel Ortiz, fundador de la Asociación Internacional de Informática Forense, en las que se abordaron temas de comportamiento cibercriminal y cibercriminalidad de gran trascendencia.

"La criminalidad se hace presente en todos lados, pero más en aquellos que cree que nadie la puede tocar ni ver"

A la fecha dichos estudios han tomado fuerza ante la persecución del delito, por lo que las solicitudes de colaboración institucional se han elevado de forma considerable ante la nueva institución de Seguridad Pública Federal de México; ya que esta institución se considera la única en su especie a nivel nacional, que desarrolla este tipo de estudios e investigaciones.

No obstante, los resultados han sido satisfactorios, ya que han sido llevados como elementos probatorios ante los sistemas del Poder Judicial Federal como Local, obteniendo como resultado sentencias del tipo condenatorias con penas privativas de la libertad, por la comisión de crimines y cibercrimenes.

Referencias

Arroyo, S. C. (2020). Derecho y Cambio Social. Recuperado en: file:///D:/Users/Administrador/Downloads/Dialnet-LaCibercriminologiaYElPerfilDelCiberdelincuente-7524987%20(3).pdf.

García, D. Á., Pérez, J. C., González, A. D., & Pérez, C. R. (2016). Risk factors associated with cybervictimization in adolescence. International Journal of Clinical and Health Psychology.

Rubio, M. B., & Selma, A. A. (2020). Una década de reformas penales: Análisis de diez años de cambios en el Código Penal (2010-2020). Bosch.

Zamora, R. A. (2016). Las opiniones personales en las redes sociales generan el ciberacoso, en el. Ecuador: UNIVERSIDAD CENTRAL DEL ECUADOR.