Perfiles del ciberdelito: un campo de estudio inexplorado

Cybercrime profiling: an unexplored field of study

Silvia Sánchez Barahona[1]
silviasanbara@hotmail.com
Código ORCID 0000-0003-2634-8171

https://doi.org/10.5377/derecho.v1i30.12223

Fecha de recibido: junio de 2021 / Fecha de aprobación: agosto de 2021

Resumen

El análisis de la incidencia y expansión del ciberdelito requiere de un enfoque complementario y especializado que viene dado por la Criminología. La perfilación en el ámbito del ciberdelito nos permite recopilar y analizar información sobre rasgos de comportamiento que han sido moldeados por la evolución tecnológica, la hiperconectividad, el anonimato en el manejo profesional o empírico de programas creados y/o utilizados para la comisión de delitos en el ciberespacio, y la utilización del delito informático como medio dirigido contra personas individuales e infraestructuras políticas y económicas.

Los cambios sociales generados por las nuevas tecnologías afectan nuestro bienestar económico, social y político. Ante cada innovación tecnológica crece en paralelo la conducta antisocial que la utiliza para su beneficio y en detrimento de terceros. El presente trabajo pretende destacar la importancia que merece la Criminología como parte integrante de la especialización y permanente capacitación de los operadores de Justicia penal con el objetivo de implementar políticas de persecución penal que contrarresten la acelerada expansión de los delitos informáticos.

Partiendo de la identificación de las motivaciones en la comisión de los delitos informáticos pueden elaborarse estudios interesantes sobre la incidencia de este fenómeno criminógeno en nuestra región latinoamericana, tomando como punto de referencia los estudios y análisis de expertos europeos y norteamericanos.

La prevención y lucha contra la expansión del ciberdelito es una de las prioridades en la coordinación y cooperación de las diferentes instituciones policiales de la región (véase Ameripol o Interpol) en sintonía con las líneas de actuación dictadas por el Convenio de Budapest y en el marco de cooperación internacional contra el crimen organizado.

Palabras Clave

ciberdelito / perfiles / criminología / legislación penal

Abstract

A qualified analysis on the effects and expansion of cybercrimes requires a specialized approach from a Criminologist´s point of view. The profiling of cybercrime incidents allows us to collect relevant information about some behavioral facts that have been molded by the constant evolution of technology. Some issues have triggered the outreach of a cybercrime environment like hyper-connectivity trends, an anonymous professional profile in the use of up-to-date technology or the self-acquired skills to use software programs in a cybercrime anonymous space, or the use of cybercrime as a resource to target down against individual victims and political and economic infrastructures.

Social changes generated by technology innovations have a direct effect on our economic, social, and political well-being. For each technological innovation there is a parallel world where an antisocial behavior merges and uses technology for its own benefit and to infringe damage to individuals and/or any political or economic network.

One of the main objectives of this article is to outline the importance of Criminology studies as part of the specialized training for all Justice workers in Central America´s judicial system in order to draw and enforce assertive crime policies in the region that counterbalance the rapid expansion of cybercrime.

Through the identification of cybercrime motivations, we can elaborate interesting field studies about this criminological phenomenon in our Latin American region. Both prevention and efforts against the expanding of cybercrimes are the main priorities in the coordination and cooperation strategies of various police institutions in our region (see Ameripol or Interpol), as a reminder of the Budapest Convention cyber security guidelines and other international liaisons approved and established in the Central American region to work against all types of organized crime, including cybercrimes.

Key words

Cybercrime / profiling / criminology / crime legislation

[1] Abogada penalista, Título de Experto en Teoría General del Delito (Universidad Autónoma de Madrid, España), Título de Experto en Análisis de Inteligencia para la Seguridad, Universidad Autónoma de Madrid, España), Diploma de Alta Especialización en Derecho Penal Económico, Escuela de Práctica Jurídica de la Universidad Complutense de Madrid, España).

Tabla de contenido

1. Un compromiso hacia la especialización y la coordinación interregional

La ciberdelincuencia es una amenaza silenciosa de rápida expansión y generadora de daños de gran impacto. Esta realidad exige la armonización de normas jurídicas entre los países de la región Iberoamericana, lo mismo que la actualización y capacitación constante en la materia, incluyendo aspectos importantes para la detección temprana de las redes organizadas de cibercrimen o individuos actuando en solitario.

En cualquiera de los casos, el análisis de la incidencia delictiva permite identificar las motivaciones detrás del ciberdelito, sean estas políticas, económicas, sexuales.

La armonización de la normativa penal en materia del ciberdelito y la coordinación interregional de las instituciones de orden público en Centroamérica es, hoy en día, una necesidad primaria que permitiría compartir bases de datos para una efectiva persecución, investigación y sanción de la ciberdelincuencia.

Existen actualmente algunas iniciativas de monitorización y recolección de datos sobre la ciberdelincuencia en países de la región Centroamericana que merece la pena destacar, como el Observatorio Guatemalteco de Delitos Informáticos (OGDI) o la Sección de Delitos Informáticos del Organismo de Investigación Judicial de Costa Rica (OIJ), pero también merece una mención especial el trabajo que realiza el Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC), que abarca una temática muy interesante a partir de la divulgación del conocimiento en materia de la prevención para promover la protección de datos.

No obstante, el sistema de justicia penal de nuestros países necesita el conocimiento especializado que permita a sus operadores comprender los aspectos conductuales especiales del ciberdelito para luego proceder a implantar procesos judiciales dinámicos y ajustados a la nueva realidad tecnológica en que vivimos. La nueva realidad jurídica para combatir el delito informático requiere no solamente de la especialización penal a partir de las escuelas de Derecho, sino que necesita la complementariedad de la Criminología para conducir políticas de persecución penal contra el ciberdelito desde el enfoque conductual de la víctima y del victimario a través de la perfilación, y el análisis geográfico de incidencia delictiva del delito informático.

2. La ciencia criminológica como puente hacia una nueva política criminal contra el cibercrimen

La adopción interna de las directrices que marcan los convenios internacionales y acuerdos de cooperación interregionales es apenas el marco conceptual para que los países de la región centroamericana armonicen la legislación penal que regula el ciberdelito. Pero también es necesario que el sistema de justicia penal armonice también su funcionamiento desde la base formativa de sus integrantes y es ahí donde destaca el aporte de conocimientos que nos brinda la Criminología como ciencia complementaria al estudio del Derecho Penal.

La transformación de las relaciones sociales y comerciales con el uso y abuso de las nuevas tecnologías ha propiciado la expansión de los delitos informáticos que, a su vez, se han transformado en acciones cada vez más complejas y diversas, requiriendo para ello la continua adecuación y modificación de la norma penal para sancionar estas conductas. Las nuevas tecnologías nos acercan en materia de cooperación y comunicación de datos para la prevención y lucha contra el crimen organizado transnacional, pero la realidad es que la innovación tecnológica también transforma la conducta de las personas, ya sea por la alta competitividad en el mundo laboral o en las relaciones sociales e interpersonales, ya sea porque se aumenta la dependencia con el medio tecnológico o por otras muchas razones ajenas y diferenciadoras de la delincuencia común. Lo cierto es que, en el mundo del ciberdelito, las acciones no pueden estudiarse desde la misma perspectiva del delito común y las formas de participación son mucho más complejas que las formas convencionales de inducción, coautoría y complicidad que conocemos.

Estas acciones complejas exigen que el proceso formativo del operador de justicia sea altamente especializado y requiere asimismo de un proceso de homogeneización legislativa en materia penal para evitar lo que podría denominarse **"paraísos de impunidad virtual"** en los países de la región donde existe poca o nula capacidad de investigación, prevención y sanción de los delitos informáticos.

El aumento exponencial de los ciberdelitos y la variedad de acciones delictivas es uno de los desafíos a los que se enfrenta el sistema de justicia penal a la hora de definir políticas de persecución y sanción. No está de más advertir que actualmente el cibercrimen es el negocio ilegal más lucrativo[2], sofisticado, creativo y difícil de detectar al que se enfrentan los investigadores. La multiplicidad de acciones delictivas por medios tecnológicos contrasta con la dificultad de encasillar al delincuente informático bajo un solo perfil, especialmente porque las acciones obedecen a una amplia variedad de motivaciones y a quien hoy en día llamamos *hacker* no siempre es un delincuente.

En opinión de la catedrática Antonia Linde[3] (2020), especialista en ciberdelito y profesora de Criminología de la Universidad Oberta de Cataluña (España), el ciberdelincuente no

[2]Ampliar en: https://www.iniseg.es/blog/ciberseguridad/la-mente-de-un-ciberdelincuente/

[3] Opinión emitida en la nota periodística de INISET (2020).

siempre pertenece a un "grupo homogéneo" y puede actuar influenciado por factores muy diversos y complejos a la vez (autocontrol, estilo de vida, relaciones sociales, situación laboral), multiplicando también sus motivaciones (curiosidad, reto, venganza, lucro, etc.).

Estos conceptos resultan más fáciles de asimilar desde un punto de vista criminológico ya que abordaríamos el problema de forma más acertada a partir del análisis de puntos coincidentes en la conducta del ciberdelincuente. Unos de los aspectos importantes a tomar en cuenta al momento de extraer y analizar el perfil del ciberdelincuente es que el delito informático puede ser el **objeto** o el **medio** de la acción delictiva (XIX Cumbre Judicial Iberoamericana, 2018). De acuerdo con esta clasificación, al primer grupo pertenecerían delitos como la Destrucción de registros informáticos, el Uso de Programas Destructivos, el Acceso y uso no autorizado de información o el delito Registros Prohibidos (Código Penal de la República de Nicaragua, Ley 641/2008). En cambio, en el segundo grupo integraríamos la comisión de actividades delictivas derivadas del uso de la tecnología y que se ejecutan como medio para la perpetración de delitos más graves o en concurso con éstos, como pueden ser las acciones delictivas relacionadas al fraude de pago, uso criminal de datos, ataque a infraestructuras críticas, distribución de pornografía y/o abuso sexual infantil (XIX Cumbre Judicial Iberoamericana, 2018).

En cualquiera de los casos, acciones delictivas como medio o como objetivo del ciberdelito requieren una constante revisión de la base de datos policial a nivel nacional y regional para analizar la información estadística de incidencias y coincidencia de perfiles.

En el caso de Nicaragua, están previstas algunas modalidades de delito informático como **medio** de la acción delictiva en figuras típicas como la Explotación sexual, pornografía y acto sexual con adolescentes mediante pago, el delito de Intrusión y, en el caso de los delitos contra a la libertad empresarial como el delito de Apoderamiento de secreto de empresa (Código Penal de la República de Nicaragua, Ley 641). Sin embargo, la legislación penal en materia de ciberdelincuencia tuvo una actualización tardía, si tomamos en cuenta la fecha de entrada en vigor de la Ley 641 o Código Penal en el año 2009, al contrario del resto de países de Centroamérica que han puesto en marcha estrategias contra el cibercrimen insertando nuevos tipos penales a la legislación penal interna e implementando estrategias nacionales de seguridad, como es el caso de El Salvador con la promulgación de la Ley Especial contra los Delitos Informáticos y Conexos[4] de 2016 o Panamá con la Estrategia Nacional de Seguridad Cibernética de Panamá del 2013[5].

Ahora bien, la elaboración de la política criminal interna y la modificación de la norma penal sustantiva está íntimamente relacionada con el estudio previo de los datos de incidencia del ciberdelito. La lectura de estos datos estadísticos va más allá de la visualización de los gráficos por sexo, área geográfica o líneas de tiempo. De hecho, los

[4] Ampliar: https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2010-2019/2016/02/B6B74.PDF

[5] Ampliar: https://www.ipandetec.org/wp-content/uploads/2018/08/IPANDETEC-Budapest-final-DD.pdf

Revista de Derecho
No. 30, II Semestre 2021.
ISSN 1993-4505 / eISSN 2409-1685

informes anuales o periódicos que únicamente se limitan a compilar datos estadísticos en gráficos y variables, carecen de contenido analítico que permita su interpretación.

En el caso específico de Nicaragua, la aprobación en octubre del 2020 de la Ley Especial de Ciberdelitos (Ley 1042/20) es el reflejo de la falta de análisis sobre la incidencia delictiva del cibercrimen a nivel local, un dato comprobable en los informes estadísticos policiales que datan del 2009, ya que éstos carecen de información estadística sobre el comportamiento de la incidencia delictiva de cualquiera de las modalidades de delitos informáticos previstos ya en el Código Penal del 2009.

El análisis de la información estadística se conecta con las dos modalidades delictivas expuestas arriba y que permiten elaborar una definición específica para cada supuesto si el delito informático ha sido el objetivo o el medio para la comisión de otros delitos. En adición a lo anterior, un estudio criminológico permitirá extraer los rasgos característicos relacionados al perfil del ciberdelincuente. Para ello es necesario contar con una base de datos detallada y actualizada que no descarte la información compilada por los investigadores y que ayude a identificar las motivaciones del delincuente en la comisión de delitos ciber-dependientes (Kranenbarg Weulen, 2018), sea que éstos se utilicen como medio para la comisión de otros tipos penales en concurso o sean independientes en sí mismos.

Un estudio reciente elaborado por la criminóloga holandesa Marleen Kranenbarg Weulen (*Cyber-offenders versus traditional offenders. An empirical comparison*. 2018) aborda esta temática explicando que las acciones delictivas que requieren un alto conocimiento tecnológico conforman el grupo de delitos informáticos que son en sí mismos el ***objetivo*** del crimen, por ejemplo, las estafas informáticas a través de métodos de manipulación de datos e información como el *hacking*, *pharming*[6], *phishing*, el uso de *malware o* el robo de credenciales para modificar páginas web *(web defacement)*[7], en los que el elemento tecnológico es la clave necesaria para la perpetración de estos delitos. No obstante, aunque el lenguaje de estas formas de comisión nos pueda parecer complejo y confuso, al indagar un poco más en la ingeniería del ciberdelito nos daremos cuenta de que no todos los ciberdelincuentes pueden presumir de altos conocimientos tecnológicos y que a veces sólo basta con ser un poco autodidacta para el simple robo de credenciales de una página de internet.

Es por ello por lo que algunos investigadores han hecho un intento por compilar algunos de los rasgos característicos de los infractores mediante el uso de la ***taxonomía del hacker*** (Rogers, 2001), que permite identificar los perfiles hipotéticos del infractor según sea su nivel de conocimiento informático y su motivación (venganza, lucro, curiosidad, notoriedad, ego). Estos trabajos empíricos han proporcionado algunas de las características comunes en este grupo de infractores que están relacionadas con la adquisición de habilidades informatizadas y el auto aprendizaje o la superación de

[6] https://www.iniseg.es/blog/ciberseguridad/hablemos-de-ciberseguridad-ii-pharming/

[7] www.incibe.es

barreras informatizadas que les condicionan su posicionamiento en el mundo del ciberdelito.

3. La importancia del estudio motivacional del ciberdelito

Como hemos dicho antes, el análisis de las características conductuales del ciberdelincuente debe formar parte de la formación y especialización de las unidades de análisis investigativo a nivel local en el sistema de justicia de cada país de la región y exige la conformación de una base de datos que debe ser compartida en las capacitaciones y foros regionales internacionales del cibercrimen para que la región latinoamericana gestione con mayor eficacia sus políticas de persecución penal.

El estudio y análisis de las motivaciones que influyen en el ciberdelincuente no hace distinción en cuanto a si el delito informático ha sido el **medio** (sustracción de secreto de empresa) o el **objetivo** (destrucción de un registro informático relacionado con el secreto empresarial). Según las investigaciones llevadas a cabo por Kranenbarg Weulen (2018) han expuesto es que en ambos casos podemos extraer motivaciones **intrínsecas** o **extrínsecas** que guían las acciones delictivas de los infractores.

Las motivaciones **intrínsecas** surgen como las más relevantes puesto que la mera actividad ilícita se convierte en la verdadera recompensa para el infractor, es el beneficio principal de su acción. El infractor se nutre de la curiosidad, del autoaprendizaje, del reto para romper barreras informáticas, lo hace por aburrimiento o porque está de moda. En cambio, las motivaciones **extrínsecas** tienen que ver con los resultados de sus acciones: al infractor le motiva actuar por venganza, movido por la ira o por hacer *bullying* contra la víctima, por causar impresión en otras personas o para enviar un mensaje determinado al objetivo, porque actúa motivado por el lucro personal o porque sus acciones son actos políticos dirigidos, y en ocasiones la guía es una posición de poder que únicamente puede lograrse en forma virtual (Kranenbarg Weulen, 2018).

En cualquiera de los casos, habrá que tener presente que la identificación y recopilación de información sobre la posible motivación del infractor deberá hacerse en retrospectiva por el especialista y requerirá de un trabajo minucioso y detallado que se apoye en el conocimiento y técnicas de análisis criminológico.

Esto implica saber distinguir las motivaciones de aquellos infractores individuales que han utilizado el medio tecnológico para cometer acciones delictivas relacionadas con la explotación sexual comercial; y por otro lado, habrá que establecer las motivaciones de quienes han incurrido en las mismas actividades como parte del crimen organizado; o la identificación de las motivaciones de quien individualmente ha sustraído un secreto de empresa a través de un programa informático intrusivo y lo que ha motivado al sujeto que ha incurrido en una acción similar para difundir dicho secreto empresarial. Este es el tipo de análisis criminológico que requiere el estudio motivacional del infractor y que alimenta el sistema penal para generar políticas de persecución efectivas.

Todo estudio motivacional de la conducta de un infractor debe hacer referencia a la edad promedio del sujeto y este aspecto criminológico también es esencial en el análisis de las motivaciones del ciberdelincuente. Algunos de los indicadores de las motivaciones en la comisión del delito informático están relacionadas con la edad promedio y sexo del infractor. De hecho, algunas investigaciones realizadas por Kranenbarg Weulen, Holt, & Van Gelder (2019) relacionadas con las motivaciones del delito común y del ciberdelito han expuesto que el medio virtual en el que se desarrolla el delito informático es un medio aparentemente *inofensivo* en el que predomina (inicia) la interacción de los jóvenes infractores a edades tempranas (-18 años) y a través de la cual conectan con una segunda realidad por medio de la proyección alternativa de su personalidad. Quienes han crecido con la evolución tecnológica son, en muchos casos, nativos digitales. Su lenguaje, comportamiento y relaciones interpersonales están adaptadas y habituadas al medio tecnológico.

Esta comodidad en el mundo virtual coincide con la fase de iniciación y exploración de experiencias en las que el joven adquiere o refuerza habilidades informáticas especiales, para quien la recompensa es evitar ser descubierto y la prioridad es el juego permanente del anonimato. Para algunos expertos, esta desinhibición *online* se caracteriza por i) la neutralización (en internet no existen límites); ii) el anonimato (actuar bajo otra realidad); y iii) la seguridad (minimización del riesgo a ser castigado).

Los jóvenes saben que el internet les permite mantener el anonimato y la invisibilidad, no dejan huellas de sus actividades, se mueven en un entorno sin fronteras físicas ni barreras y que facilita la comunicación e interacción multinacional donde pueden continuar el auto aprendizaje por medio de tutoriales de otros delincuentes en el ciberespacio. Esto último nos exige tener presente que el ciberdelito se ha convertido en una actividad empresarial altamente lucrativa en su vertiente individual u organizada y además se ha convertido en un entorno de mercado con sus propias regulaciones.

Paralelo a los mercados físicos, en la realidad virtual de internet, el mercado del cibercrimen opera en un contexto de anonimato donde existen sectores de mercado mejores y peores, constituido por una amplia gama de delincuentes con distintos objetivos. En el mundo del ciberdelito también los infractores se han impuesto regulaciones para poder acceder al nicho de mercado en el que desarrollan sus actividades ilícitas, creando barreras para posicionarse en un *ranking* reputacional virtual.

En este contexto, para cualquier sistema penal el *ranking* reputacional de los infractores adquiere relevancia al momento de compilar información y realizar el análisis de sus motivaciones puesto que los niveles de conocimiento adquiridos a lo largo de cierto período de tiempo pueden denotar el nivel de sofisticación, planificación y tipo de motivación del infractor. Las modificaciones en el *ranking* reputacional de un infractor y la relación de éste con el entorno pueden servir de indicativo en la planificación de acciones delictivas futuras. Por ejemplo, un infractor en su fase de iniciación puede ascender en el *ranking* y pertenecer a un grupo de élite, ya sea a través del autoaprendizaje motivado por el activismo político, y posicionarse en este grupo élite con el objetivo de aglutinar seguidores y planificar un ataque simultáneo e intrusión en

la base de datos de un gobierno. O bien, dado el posicionamiento del infractor, puede darse una modificación en las acciones delictivas y actuar en solitario (sin ningún ánimo de lucro) motivado únicamente por el desafío que representa romper las barreras de un programa determinado e incurrir en el vandalismo informático.

4. La especialización en nuestros sistemas penales es prioridad

Si bien se ha hablado que extraer un perfil criminológico definido para los delitos informáticos no es tarea fácil, existen suficientes datos sociológicos con los que podemos puntualizar algunos rasgos diferenciadores de los delitos comunes. Creo que lo primordial es no perder de vista que la especialización es la clave para actualizar y homogeneizar los sistemas penales de nuestra región latinoamericana.

Por ello debe hacerse énfasis en el enfoque conductual del delito informático, no solamente en los informes estadísticos sobre la incidencia delictiva por tipos de delito en un país o región, sino que debemos analizar los indicadores, su evolución, su expansión, la motivación, fluctuaciones demográficas, etc. La mejor herramienta para ello es precisamente la Criminología, que involucra aspectos psicológicos y sociológicos para comprender este fenómeno.

Si nuestros especialistas necesitan comprender las acciones ejecutadas por un llanero solitario que actúa por sí sólo y luego es contratado por una red organizada (*crime as a service*[8]); o comprender la motivación de quien sustrae una base de datos con información privilegiada de un banco nacional o de quien realiza un *hacktivismo* político en solitario, nos debemos auxiliar de la metodología específica que nos proporciona la Criminología.

La tendencia del ciberdelito debe ser analizada partiendo del origen, del surgimiento de los *browsers*, los *crackers* y los *hackers,* para hacer más comprensible la información actual con la que contamos para definir estrategias de investigación, prevención y sanción.

En este marco de ideas insisto que es necesario integrar la Criminología en la currícula universitaria y/o formativa de los operadores de justicia penal de cada país de la región. Por mencionar un ejemplo actual, en el año 2014 Nicaragua suscribió en Madrid, España, el *Convenio Iberoamericano de Cooperación para la Investigación, Aseguramiento y obtención de pruebas en materia de Ciberdelincuencia*, pero fue hasta el mes de febrero del año 2020 que fue ratificado y publicado, con lo que se demuestra que, a lo largo de seis años, ninguna de las instituciones integrantes del sistema de justicia penal nicaragüense (Policía Nacional, Poder Judicial, Fiscalía, Procuraduría General de la República) ha implementado estrategias para la capacitación periódica y permanente de su personal en materia de ciberdelincuencia. En el caso de la Policía Nacional de Nicaragua, la Dirección de Investigaciones Económicas (DIE) creó una Unidad de Ciberdelitos para la investigación especializada de estos grupos delictivos, pero a la fecha se desconocen los datos estadísticos relacionados con la incidencia delictiva del ciberdelito en el país según la

[8] N. de A. Traducido del inglés *crimen como un servicio*.

tipificación del Código Penal de 2009. Esto lo vemos reflejado en los informes estadísticos anuales que publica la institución policial nicaragüense y en los que no existe ningún dato referencial sobre la incidencia de delitos informáticos en las modalidades ya descritas (Anuario Estadístico Policía Nacional de la República de Nicaragua, 2017). Esta observación es parte de lo expuesto anteriormente en cuanto a la obsolescencia formativa del sistema de justicia penal nicaragüense y las carencias formativas especializadas de su personal, tanto operativo (policial) como Fiscales y funcionarios del Poder Judicial.

La participación de nuestros países en las propuestas de cooperación internacional en la lucha contra la ciberdelincuencia no solamente afianza relaciones internacionales, sino que exige resultados. Cada línea de actuación que implementa nuestro sistema de justicia penal en relación con políticas de persecución penal contra el cibercrimen debe planificarse como una verdadera estrategia de seguridad nacional donde se invierten recursos en conocimiento porque el ciberdelito avanza a pasos de gigante y los infractores se multiplican y especializan a gran velocidad.

En este camino hacia la especialización la cooperación interregional es clave y debemos aunar esfuerzos para que nuestra región refuerce el marco jurídico existente y defina políticas criminales eficaces y sólidas.

Referencias bibliográficas

Anuario Estadístico Policial (2017). Policía Nacional de la República de Nicaragua. Managua: Nicaragua.

Banco Interamericano de Desarrollo & Organización de los Estados Americanos. (2020). Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe.

Cumbre Judicial Iberoamericana & E-Justicia. (2018). Compendio Normativo sobre Ciberdelincuencia (XIX Edición).

Convenio sobre la Ciberdelincuencia. (2001). Budapest. Recuperado de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Comisión Europea. (2013). Estrategia de Ciberseguridad de la Unión Europea. Bruselas.

Estrategia Nacional de Ciberseguridad. (2019). España.

Estudio sobre la Cibercriminalidad en España. (2018). Ministerio de Interior, Secretaría de Estado de Seguridad.

INISET. (2020). *La mente de un ciberdelincuente: sin límites al respeto.* Recuperado de https://www.iniseg.es/blog/ciberseguridad/la-mente-de-un-ciberdelincuente/

Kranenbarg Weulen, M. (2018). *Cyber-offenders versus traditional offenders. An empirical comparison.*

Kranenbarg Weulen, M. *Offending and Victimization in the Digital Age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap.* Artículo publicado en revista *Deviant Behavior*. https://www.tandfonline.com

Ley No. 641. Código Penal de la República de Nicaragua, publicada en *La Gaceta Diario oficial* No. 232, del 03 de diciembre del 2007. Nicaragua.

Ley No. 896. Ley Contra la Trata de Personas, publicada en *La Gaceta Diario Oficial* No. 38, del 25 de febrero de 2015. Nicaragua.

Rogers, M. (2001). *A New Hacker Taxonomy*. Tesis Doctoral, Universidad de Manitoba (Canadá).

Temperini, M.G.I. (2014). *Delitos Informáticos en Latinoamérica. Un estudio de derecho comparado,* 14 Simposio Argentino de Informática y Derecho.

Velasco, E. & Sanchís, C. (2019). *El delito informático*. Ed. Tirant Lo Blanch.