NATURALEZA DE LOS DELITOS INFORMÁTICOS Y ALGUNOS ORDENAMIENTOS JURÍDICOS

NATURE OF COMPUTER CRIMES AND SOME LEGAL SYSTEMS

Presentado por:

EDINSON MICOLTA PERLAZA - CÓDIGO: 12.798.921

Presentado a:

GEORGINA DE LEON VARGAS

DIPLOMADO: DERECHO PENAL Y DE LAS NUEVAS TECNOLOGÍAS.

ENSAYO COMO NOTA DE DIPLOMADO

UNIVERSIDAD SANTIAGO DE CALI, FACULTAD Y PROGRAMA DE DERECHO

SANTIAGO DE CALI, VALLE DEL CAUCA

OCTUBRE, 2022

RESUMEN.

En este trabajo se investigó respecto a la regulación jurídica y el tratamiento legal que se le ha otorgado a nivel nacional e internacional a la ciberdelincuencia, teniendo como punto de partida el avance social desde lo tecnológico que ha ido en conjunto con el desarrollo de los medios de comunicación en los últimos años; es en este contexto de desarrollo que el derecho debe de adaptarse y moldearse a las necesidades sociales del momento histórico, toda vez que se deben de garantizar los fines esenciales del Estado en todo momento y en toda conducta humana aunque eso signifique que sea a través de medios digitales y abstractos como lo son el internet y las redes sociales, pues esto da seguridad en la ciudadanía aparte de garantizar el principio y objetivo de la seguridad jurídica, para que estos servicios y bienes tecnológicos sean de confianza para los ciudadanos, teniendo en cuenta que existen diversos aparatos o herramientas que permiten acceder a los medios de comunicación, pero sin importar eso se debe de buscar la manera de proteger los bienes jurídicos tutelados en el código penal en vista de el mal uso que le dan algunas personas a la tecnología, en cuyos casos se configuran ciberdelitos o actividades ilícitas y criminales digitales, es por esto que en el mundo los Estados se han preocupado por legislar e incorporar al ordenamiento jurídico esta clase de criminalidad, así mismo el derecho internacional se ha preocupad por progresar y evolucionar en la doctrina y en la legislación sobre la materia, siendo una obligación por estudiar las conductas que configuran tipos penales. En este sentido es que el presente ensayo busca profundizar en el conocimiento de los delitos cibernéticos, de su significado, sus clases y los cambios sociales que se han gestado en Colombia. Además de tener un enfoque local sobre las consideraciones jurídicas de los delitos informáticos, también se revisará la materia en otros países y como esas legislaciones han tratado el tema, teniendo un marco internacional de derechos informáticos.

PALABRAS CLAVES.

Delitos informáticos, derecho comparado, herramientas informáticas, conductas digitales ilegales, derecho internacional.

INTRODUCCIÓN.

Si se realiza un análisis de la sociedad contemporánea y su desarrollo en los últimos años, se puede observar que la curiosidad por la tecnología ha llevado al hombre a tener avances científicos y nuevas formas de interacción y comunicación, como por ejemplo el haber posibilitado la comunicación desde los celulares, todo desde el alcance de las manos de cualquier persona, siendo una situación muy diferente del pasado en donde las personas o no podían comunicarse o tenían forma de hacerlo pero eran muy rudimentarias; además el gran logro tecnológico es la posibilidad de interactuar desde cualquier parte del mundo, es decir, actualmente se está viviendo en una era de las ciencias aplicada e informáticas, y a partir de este contexto es que se cuestiona por la eficiencia del derecho cuando se presenta un mal uso o un abuso de estos medios, de cómo puede llegar a afectar a la sociedad al ser una gran influencia en todas las esferas de la vida del ser humano, y que sobre todo se presentan conductas que no están tipificadas por la Ley penal ya sea porque no se han podido preveer debido a la novedad de la materia o porque no se le ha prestado la especial tención que se merece.

Ahora último los países se han preocupado por regular la materia cibernética y las conductas en torno a la vida tecnológica, por ello se han preocupado por suscribir tratados internacionales sobre la delincuencia informática, tal como lo es la la Convención sobre el delito cibernético y el convenio de Budapest, a través de los cuales se desarrolló una armonización del derecho, y del trabajo de varios Estados, para que sumados los esfuerzos se puedan formular medidas preventivas y punitivas cuando se configuran delitos, ya en específico, en Colombia se expidió la Ley 1273 de 2009 y la Ley 679 de 2001 que tratan el tema de la confidencialidad y la privacidad e integridad de los datos digitales.

Los efectos de la ciberdelincuencia para Colombia, en cuanto al uso de redes e internet han sido notorios y progresivos, dejando en evidencia los peligros para las personas que en la mayoría de ocasiones no son conscientes sobre la vulnerabilidad en la que se encuentra su información personal y la susceptibilidad frente a cualquier otro usuario malintencionado que desee desplegar acciones negativas, por eso es pertinente cuestionarse ¿Qué respuesta ha dado Colombia frente al uso de la tecnología y los

medios de comunicación informáticos al momento de la comisión de conductas delictivas? se es consciente que ha existido una evolución y perfeccionamiento, sin embargo, se sabe con anticipación que probablemente existen aún vacíos normativos y que el Estado no ha desarrollado las políticas públicas necesarias para afrontar esta nueva forma de delincuencia.

Siendo coherentes con todo lo mencionado hasta el momento, cabe aclarar que se hará uso de una metodología cualitativa y descriptiva, con un método hermenéutico y un enfoque deductivo haciendo uso de artículos científicos encontrados en las revistas jurídicas de Scielo, Dialnet, Scopus, y Redalyc, y extrayendo la información más pertinente para construir el ensayo, toda vez que el objetivo general es describir naturaleza de los delitos informáticos y algunos ordenamientos jurídicos, lo cual se logrará a través de tres objetivos específicos: primero, estudiar la Historia de la tecnología y sus implicaciones en la sociedad; segundo, explicar las clase de delitos cibernéticos, informáticos o electrónicos existen; tercero, estudiar desde el derecho comparado como afrontan los delitos informáticos otros ordenamientos jurídicos.

1. HISTORIA DE LA TECNOLOGÍA Y SUS IMPLICACIONES EN LA SOCIEDAD.

A lo largo de la historia de la humanidad ha sido notorio la necesidad de la comunicación a través de cualquier medio, desde pictogramas, dibujos, señales de humo, cartas, telegramas, correo postal, celulares, computadoras, etc., toda vez que el hombre es un ser social por naturaleza, y siempre ha necesitado transmitir sus pensamientos, deseos y metas en la construcción de la civilización; con el tiempo las formas de transmitir información desde sitios muy lejanos comenzó a modernizarse hasta tal punto que con el internet se pueden realizar actividades antes nunca imaginadas. La época del internet ha brindado a nivel global tener al alcance cualquier servicio o bien que necesite, como por ejemplo, lo comercial, económico, lo cultural y la información o conocimiento que desee ya sea de entretenimiento o algo científico (Valdés,1996).

El internet surgió a mediados del siglo pasado, siendo una herramienta revolucionaria y llegando a posicionarse en la cúspide de los medios de comunicación,

haciendo que las personas dejaran a un lado otros medios de comunicación arcaicos como el telegrama, el fax, o el teléfono fijo. Para los años ochenta la industria de las telecomunicaciones tuvo un mayor auge y se amplió aún más el acceso al internet comenzando a crearse canales de acceso como el Wifi donde se podía acceder al internet desde un computador de mesa o a uno portátil, y con el tiempo el Wifi también llegó a los celulares los cuales ya no solo eran usados para llamadas telefónicas, sino que comenzaron a evolucionar incorporando otras funciones (Valdés, 1996).

Para la década de los dos mil fue muy notable la globalización de la tecnología en casi todas las sociedades contemporáneas, y llegaron los celulares inteligentes que abrieron las puertas a las redes sociales. Las redes sociales se posicionan como una nueva forma de interacción personal entre todas las personas del mundo, el único requisito para poder acceder era tener un dispositivo móvil o un computador para poder estar conectados y en contacto, pues se manejaba una mensajería instantánea y plataformas digitales que ofrecían información precisa en tiempo real (Mayer. & Oliver, 2020)

Al día de hoy, la sociedad moderna continúa en constante evolución y experimentación con la tecnología desde las comunicaciones y desde lo científico, lo que ha irradiado todas las esferas de la vida de las personas de manera directa o indirecta. El acceso a información variada a través de la red y web de internet a nivel internacional ha provocado que incluso se creen nuevas formas de trabajo, en vista que una persona puede desempeñar su trabajo desde cualquier lugar del mundo; estas nuevas formas de vida han definidos a esta generación como la generación de la era digital y que hace uso de la conocida nube, en donde los datos personales migran fácilmente en ese mundo abstracto e infinito de información, lo cual es un reto para los dueños de los negocios que proveen internet, porque deben de ofrecer a sus usuarios y clientes una infraestructura digital adecuada y segura para que en sus prácticas se sientas seguros y confiados, disminuyendo las posibles amenazas informáticas (Ojeda, Rincón, Arias & Daza, 2010).

A medida que transcurrió el tiempo las amenazas informáticas salieron a flote, siendo el internet una herramienta para los delincuentes en donde sus conductas quedaban impunes debido a la falta de regulación jurídica, pues la falta de legislación

era una ventaja con fundamento en el principio de legalidad, y así fue como surgieron los comportamiento indebidos conocidos como delitos informáticos, que se han convertido en un nuevo campo del derecho donde debe de estudiarse los comportamientos humanos en la era digital combinando las disciplinas técnicas y jurídicas y de auditoría informática porque no es solo a través de dispositivos simples como los móviles que se cometen delitos sino que ahora los delincuentes también usan grandes bases de datos e información clasificada, como lo es en el sistema bancario, financiero o crediticio. Es decir que se encuentran en riesgo los derechos de las personas jurídicas y de las personas naturales en igual medida en su honra , dignidad y vida (Rico,2013).

Al día de hoy se presentan diversos delitos de gran trascendencia y riesgo para las sociedades como lo son el terrorismo digital, las tratas de personas, la pornografía, la prostitución infantil, hasta el narcotráfico, etc., es por esto que los países se vieron en la obligación y en la necesidad de reglamentar los medios digitales y las redes sociales, así por ejemplo, ahora se manejan registros de datos digitales lo cual deja un rastro en los servidores de todos los clientes o usuarios que tienen acceso al internet, de todas formas ha de considerarse lo contraproducente que son estas medidas, pues mientras se garantizan con ellas una seguridad y estabilidad de navegación, al mismo tiempo se está vulnerando la privacidad de las personas y su libertad, lo cual es una situación controversial y es por ello que se ha de tratar de ponderar derechos (Acurio Del Pino,2016).

Para dar una definición sobre delito informático (electrónico o cibernético) se tiene que tener en cuenta la interdisciplinariedad y las diversas facetas que desempeña el delito, así por ejemplo, la doctrina ha debitado arduamente desde el ordenamiento interno e internacional, es en este sentido que no existe una definición puntual, absoluta y universal, y sobre todo porque cada país tiene sus propias leyes y sus propias medidas para enfrentar la realidad de los delitos informáticos que en ocasiones son muy diferentes o particulares. Pero a grandes rasgos se pueden ver las características de los delitos informáticos y por ende se pueden definir como conductas criminalizadas por las leyes penales desde las antijuricidad, la tipicidad y la culpabilidad, y que al momento de su configuración se debe de hacer uso de herramientas tecnológicas, informáticas o electrónicas, ya sea como un método, como un fin o como un medio para lograr la

realización del tipo penal y necesariamente esa conducta debe estar regulado por el legislador y tipificado siguiendo el principio de legalidad (Arocena,2012).

Se puede observar que los delitos informáticos tienen ciertos elementos indispensables para que se configuren, por ejemplo, es importante entender tres elementos o características trascendentales que permiten enmarcar una conducta como un delito informático: primero debe hacerse uso de medios informáticos; segundo el objeto sobre el que recae esa conducta debe ser un bien o servicio digital perteneciente del ciberespacio; y tercero el ordenamiento jurídico debe de prever la conducta. De aquí que se pueda considerar que aquellos delincuentes que son ágiles para evitar la justicia podrían fácilmente evadir penas y sanciones al cometer delitos en países donde saben que no existe regulación jurídica, es decir, se presentan delitos a nivel internacional y posiblemente de forma anónima, siendo difícil de perseguir o de poner límites (Valdés,1996)

2. DELITOS CIBERNÉTICOS, INFORMÁTICOS O ELECTRÓNICOS.

Dentro de la tipología de delitos informáticos existen innumerables clases, de todas maneras acá se mencionan las más generalizadas. La manera de infringir en la web se ha ido sofisticando y evolucionando hasta el punto en que el fenómeno ha vuelto volátil y el internet un medio de fácil acceso para la comisión de delitos. Con el tiempo la complejidad desde lo técnico del delito ha hecho que la doctrina plantee y prevé ciertas conductas. Hoy en dia se identifican múltiples conductas en las que cada una tiene una finalidad precisa, pues no es lo mismo un hackeo a una empresa privada, a un gobierno, una extorsión, un robo de datos o un robo de cuentas bancarias, etc., sin embargo a continuación se resaltan los delitos más llamativos para la comunidad internacional y para el ordenamiento interno de Colombia:

En primer lugar exister un terrorismo ciberneutico o un cirberlavado, cuando es de conocimiento público y a traves de algun de medio de comunicación un menaje que genera terror en la comunidad, el ejemplo clasico es el 11-S, el evento de las torres generales en Estados unidos el 11 de septiembre del año 2000, para el cual un investigador del caso llamado Barry Collin le asigno el nombre que ya venia usando

desde los años ochenta. Las diversas formas tradicionales de generar terror se trasladaron al mundo digital haciendo que la red se convierta en un espacio inseguro donde pueden darse ataques premeditados hacia cierta información, sistemas, gobiernos, organizaciones políticas, etc. (Ruiz,2018)

Como segundo delito informático se puede mencionar el ciberbullying, es una moderna forma de abusar o hacer grooming, definiéndose como patrones de comportamientos agresivos dirigidos hacia una persona, muy común en los estudiantes o jóvenes dentro de una vida escolar, se caracteriza por ser continuo en el tiempo y repetitivo ocasionando graves problemas sexuales, morales y psicológicos a la víctima presentándose toda clase de acciones que atentan contra el equilibrio mental y la salud, puede darse a través de palabras, amenazas, injurias, calumnias que atenten contra el buen nombre con falsas acusaciones, o con la exposición de información privada y reservada, con la suplantación de nombre como la creación de perfiles falsos, o la promoción de discriminación por cuestiones varias como religión, orientación sexual, idioma, origen, raza, ideaología política esto se da sobre todo a través de las redes sociales como facebook, instagram y twitter o cualquier plataforma de amplia difusión que sirven de herramientas para menoscabar la integridad y dignidad de la víctima por parte de una persona o grupo de personal (Ruiz,2018).

Como tercer delito, está la estafa digital, que se adecua cuando una persona o varias personas a través del engaño logra que la víctima le realice consignaciones o transferencias bancarias de manera voluntaria inicialmente. Este es uno de los delitos más comunes en donde se presenta manipulación para lograr obtener dinero, o alteración de alguna información o acceso a datos cibernéticos, en especial los datos sobre la identidad de la víctima, con una especial carácteristicas y es que siempre se presenta un menoscabo en el patrimonio del afectado, es una nueva modalidad de estafar, por lo tanto se vulnera el mismo bien jurídico tutelado solo que cambia es la forma o las herramientas utilizadas por el delincuente, al día de hoy algunas formas conocidas de cometer este delito son el phishing y el hacking (Ojeda, Rincon, Arias & Daza, 2010).

El hacking es toda aquella conducta que se inmiscuye de manera ilegal en los datos o información privada y reservada sobre el manejo financiero de una persona sin llegar a tener el consentimiento del titular de dicha información, son muy destacados los ataques por obtención de información a través de virus, y también aquellos ataques a grandes multinacionales y empresas. Mientras que el phishing es una forma de estafa a través de las cuales los delincuentes logran hacer que la misma víctima proporcione la información personal y financiera para realizar la ciberestafa de forma que extraiga el patrimonio sin ninguna dificultad o restricción (Mayer, & Oliver, 2020).

Como cuarto delito cibernético se encuentra la pornografia infantil, que si bien se sabe que todo delito contra los menores ha existido desde hace mucho tiempo en países como Dinamarca y Holanda, sin embargo, en este delito lo característico es que se comercializa contenido ilegal de un menor a través de medios virtuales o digitales como lo son películas, videos, revistas, en vivos, libros, imágenes; este delito tiene raíces muy profundas que empiezan desde las personas que producen el contenido, también aquellas que lo distribuyen, aquellas que lo comercializan, y aquellos que lo consumen, toda esa cadena de personas hacer parte del ciberdelito y configuran una conducta punible (Mayor, 2018).

3. DERECHO COMPARADO: DESARROLLO JURÍDICO DE OTROS PAÍSES PARA AFRONTAR DELITOS INFORMÁTICOS.

En primer lugar se tiene a México, que a nivel interno hizo un reforma al código Penal Federal, con la reforma número 75 desde su expedición desde 1999. A través de esta reforma se incorporaron unos artículos, desde el artículo 211.1 hasta el artículo 211.7, donde incorporan delitos informáticos, tales como la revelación y apropiación de información reservada y secreta y sobre todo privada a través de herramientas informáticas accediendo a sistemas o programas digitales, pese a esto el Estado mexicano no ha creado procedimientos claros sobre cómo enfrentar el delito informático, lo que se le suma a este país es que trate de evolucionar en su legislación sobre el derecho informático y acogiéndose a los estándares internacionales y a la ratificación que hicieron al Estatuto de Roma en 2005; obviamente falta más motivación por parte

del legislador para considerar la importancia de la materia y desplegar y materializar los compromisos que adquirió al firmar el Estatuto de Roma y el convenio de Budapest, es decir que no se ha presentado una eficacia en la incorporación de instrumentos internacionales a su territorio nacional, por eso es que México es uno de los países con mayor índice de ciberdelitos en donde diferentes grupos delictivos tiene la oportunidad de cometer conductas ilegales y quedar en la impunidad (Mayer,2017).

En segundo lugar, Estados Unidos desde 1994 profirió el Acta Federal de Abuso Computacional cuya finalidad fue definir que es un virus en lo concerniente a lo informático. Después de los acontecimientos del 11 de septiembre del año 2000 y del terrorismo presentado se expidió la Ley Patriótica, sinedo un referente a nivel mundial para regular la materia del ciberdelito, a partir de ese momento el Estado le dió la facultad a entidades estatales de tener acceso a información confidencial tanto de las personas naturales como de las juridicas para evitar grabes delitos es por ello que el FBI, la CIA, y la NSA no tienen en cuenta el derecho de la privacidad de las personas toda vez que buscan el bienestar general y la seguridad y amparo de todo el país frente a cualquier delito, ciberdelito y sobre todo frente al terrorismo, es por ello que esta Ley tuvo muchos detractores y opostores por considerar que no respetaba la libertad y promovia el abuso de las institcuiones estatales (Hernandez,2009).

En tercer lugar, la Unión Europea desarrolló un sistema que garantiza la protección de todos los países pertenecientes a ella a través de unos procedimientos y legislación internacional sobre el bienestar y calidad de los productos y servicios cibernéticos para que las personas puedan acceder con confianza a la web. Es decir, que la unión europea desarrolló unos procedimientos para sancionar e imponer penas pero al mismo tiempo también respeta lo que cada país quiera regular y desarrollar legislativamente (Estrada,2010).

En cuarto lugar está Colombia que ha sabido desarrollar los delitos informáticos durantes los últimos años,incluyendo en el sistema jurídico modalidades de delitos cibernéticos, que se cometen usando dispositivos digitales, es así cómo se expidió en 1989 el Decreto 1360, por el cual se buscó conseguir un soporte técnico y lógico con software en el Registro Nacional de Derecho de Autor, para cuando se cometieron delitos

informáticos relacionados a los derechos de autor, llegando a defender la propiedad intelectual y la creación de sistemas informáticos. Por lo que se constituyó como una de las normas clave para sancionar los delitos contra derechos de autor, previo a la reforma al código penal colombiano del año 2000 (Dominguez & Vazquez, 2022)

Por otra parte, para el año 2001 se implementó un estatuto para prevenir y contrarrestar la explotación, pornograficas y turismo sexual con menos de edad a través de la ley 679, dentro de dicha normativa no fueron tenidos en cuenta aquellas situaciones en las cuales, para la comisión de las conductas dichas, se utilizan medios informáticos. Para finales del año 2009 con la modificación del Código Penal se adiciono la ley estatutaria 1273 por medio la cual se creó un nuevo bien jurídico tutelado que fue denominado “protección de los datos y la información” creando nuevos tipos penales, donde el sujeto activo se valiera de medios tecnologicos e informaticos para atentar contra la integridad, disponibilidad y confidencialidad de la información, imponiendo sanciones pena privativa de la libertad y en algunos casos penas pecuniarias (Contreras, 2003)

El derecho a la intimidad establecido en el articulado quince de la Carta Magna con la creación de la ley 1273 del año 2009 con esto el esfuerzo del legislador por la regulación de los delitos informáticos, constituyen un avance importante para la adaptación del marco jurídico colombiano a las necesidades tecnológicas que están siempre en constante cambio, con el fin de proteger y salvaguardar la información de los diferentes ataques y delitos contra la misma, en cuanto a las técnicas como fines utilizados por la delincuencia para cometer o llegar a algún propósito (Colas, 2016)

En la Comunidad Económica Europea (CEE), encontramos a Colombia en el mismo nivel que los países pertenecientes a dicha comunidad, donde ampliaron a un nivel internacional los acuerdos jurídicos que se relacionan con el amparo de la información y los demás recursos informáticos, por medio del convenio “cibercriminalidad” suscrito en Budapest, Hungría en el 2001, vigente desde julio del año 2004. Tal ley sigue siendo muy general y se requiere de una amplia interpretación por parte de los abogados y jueces para aplicarla frente a nuevos delitos. Es una necesidad de que en Colombia existen primordialmente políticas criminales encaminado a prevenir,

sancionar y amparar estas acciones, políticas que después se traduzcan en leyes y normas que tipifiquen la variedad de conductas que al pasar los días aparecen y crecen en las redes sociales en el país (Chen, 2010)

CONCLUSIONES.

En Colombia con la expedición de ley 1273 de 2009 y la Ley 679 de 2001 se empezó a regular la materia en delitos informáticos, teniendo en cuenta que los antecedentes históricos tienen en consideración la inserción del internet a la vida de la civilización y sociedad moderna, el avance científico y el wifi al igual que la evolución de los dispositivos y herramientas digitales han obligado a los Estados a regular jurídicamente los delitos tecnológicos, los cuales deben de cumplir con ciertas características para que se puedan configurar, las cuales son que los delitos se comentan con una herramienta tecnológica, que las consecuencias negativas o la conducta esté dirigida también a un bien y servicio digital, además de tener que estar establecida en la Ley penal, toda vez que estudiar esta materia sirve para evitar inseguridades y amenazas a los usuarios al momento de navegar digitalmente por necesidades de entretenimiento o de trabajo, pues la era digital en la que el hombre actualmente vive, le permite laborar a distancia y remotamente desde cualquier parte del mundo. En cuanto a la definición de delito informático es difícil lograr limitarla porque cada ordenamiento jurídico regula la materia a su manera, sin embargo, puede ser definido como una conducta criminalizada por el derecho penal que cumple con las tres características para que pueda adecuarse, es decir, que esto va a depender del entorno y país en el que se ejecute.

Cómo segunda conclusión respecto al segundo sub acápite, se puede decir que existe diversos ciberdelitos y con una naturaleza propia para cada caso, teniendo en común que se hace utilización de medios digitales, tecnológicos o informáticos para la comisión del ciberdelito; la víctimas en la mayoría de casos son personas que se volvieron vulnerables frente a la falta de seguridad de la web y a las posibilidades que brindan los medios de comunicación y el internet a los delincuentes y abusadores. Entre los delitos más destacados entre la doctrina se encuentran cuatro que se explicaron en el desarrollo del ensayo de manera general, los cuales son: El terrorismo ciberneutico o

un cirberlavado, el ciberbullying, la estafa digital, la pornografia infantil. Cada uno vulnera un bien jurídico tutelado dentro del ordenamiento jurídico de cada país.

Como tercer y última conclusión se puede indicar que a nivel internacional cada país ha tratado de manejar los delitos informáticos a su manera para hacer frente a los flagelos propios de la era digital, por ello han tenido que de una forma u otra en gran medida o poca legislar e incorporar en la Ley penal esas conductas delictivas. Para el caso colombiano se ha expedido una serie de leyes que reforman el código penal para tenerse en cuenta los delitos informáticos, tales como el Decreto 1360 del año 1989 y la ley 1273 del año 2009, así es como se han creado nuevos tipos penales que ayudan a las autoridades a tomar cartas en el asunto, sin embargo, siguen existiendo ciertos vacíos jurídicos y se necesita mayor regulación en la materia para que dejen de ser normas tan abstractas y generales y no dejar que los ciberdelincuentes comentan conductas dañosas para la sociedad y que queden en impunidad.

REFERENCIAS BIBLIOGRÁFICAS.

Acurio Del Pino, S. (2016). Delitos informáticos: generalidades. recuperado de: http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599

Arocena, Gustavo A.. (2012). La regulación de los delitos informáticos en el Código Penal argentino: Introducción a la Ley Nacional núm. 26.388. Boletín mexicano de derecho comparado, 45(135), 945-988. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002&lng=es&tlng=es.

Chen Mok, Susan. (2010). Privacidad y protección de datos: un análisis de legislación comparada. Diálogos Revista Electrónica de Historia, 11(1), 111-152. Recuperado de: http://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1409-469X2010000100004&lng=en&tlng=es.

Colás Turégano, Asunción. (2016). El delito de intrusismo informático tras la reforma del CP español de 2015. Iuris Tantum Revista Boliviana de Derecho, (21), 210-228. Recuperado de: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572016000100010&lng=es&tlng=es.

Domínguez Arteaga, Rosa Amelia, & Vázquez, Rodrigo Vera. (2022). Análisis espacial del ciberfraude al comercio electrónico: consideraciones en agenda política Tamaulipeca. Podium, (41), 21-40. Recuperado de: https://doi.org/10.31095/podium.2022.41.2

Estrada, A. C. (2010). La informática forense y los delitos informáticos. Revista Pensamiento Americano, 4, 81-88. Recuperado de: https://d1wqtxts1xzle7.cloudfront.net/47365075/Pensamiento_Americano_n.6_2010-with-cover-page-v2.pdf?Expires=1665989191&Signature=ad3sTqYlhfMuQR32DF1V7GapeGIIVGdbPDar~Rb66aEblmsO-vyAtr7bDMUQb-FBJIBtK~nJRyNiuJbSKqv5lsRf5ReWLysbSNbDNiXF4recGP3jKIcRlulc-89ilVImvfcXBKLrn9bGIdO1CA8GMiupNlztGVKv4oUqRTTaso2ZDnhAeNaokV-IMIDmiYFUvSYK31yfV2H-dOR5clX4He1y99lT1ESSmjRslJurhupMJ~25j8XodFz3id-v8nwxyYhF6WdwN2mOonYAkYJWTAacccE3wTZB9fBhTSuDbElizvYu3pfDPexU47GASjp2-Sr8oThxtdqyRqcjHPTSCQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=71

Mayer Lux, Laura. (2017). El Bien Jurídico Protegido En Los Delitos Informáticos. Revista chilena de derecho, 44(1), 261-285. Recuperado de. https://dx.doi.org/10.4067/S0718-34372017000100011

Mayer Lux, Laura, & Oliver Calderón, Guillermo. (2020). El delito de fraude informático: concepto y delimitación. Revista chilena de derecho y tecnología, 9(1), 151-184. Recuperado de: https://dx.doi.org/10.5354/0719-2584.2020.53447

Ojeda-Pérez, Jorge Eliécer, Rincón-Rodríguez, Fernando, Arias-Flórez, Miguel Eugenio, & Daza-Martínez, Libardo Alberto. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11(28), 41-66. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=en&tlng=es.

Rico Carrillo, Mariliana. (2013). Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos. Revista IUS, 7(31), 207-222. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100011&lng=es&tlng=es.

Ruiz-Morales, Manuel Luis. (2018). El uso de drones en España: el ámbito espacial de la ley penal. Derecho PUCP, (81), 137-162. Recuerdo de: https://dx.doi.org/10.18800/derechopucp.201802.005

Valdés, J. A. T. (1996). Los delitos informáticos: situación en México. Informática y derecho: Revista iberoamericana de derecho informático, (9), 461-474. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/248768.pdf