Ciberterrorismo vertiente criminal de las más peligrosas, una aproximación al contexto guatemalteco

Cyberterrorism, the most dangerous criminal aspect, an approach to the Guatemalan context

Silvia Judith Corado Asencio
Maestría en Derecho Penal
Centro Universitario de Oriente
Universidad de San Carlos de Guatemala
judith.corado@gmail.com
https://orcid.org/0009-0009-3297-5519

Recibido: 15/01/2024
Aceptado: 16/04/2024
Publicado: 15/05/2024

Referencia del artículo

Leonardo Torres, D. A. (2024). Ciberterrorismo vertiente criminal de las más peligrosas, una aproximación al contexto guatemalteco. *Revista Diversidad Científica,* 4(1), 227-235.
DOI: https://doi.org/10.36314/diversidad.v4i1.118

Resumen

PROBLEMA: determinar la necesidad que exista un tipo penal que establezca los márgenes sobre los cuales los órganos jurisdiccionales pueden encuadrar determinadas acciones y omisiones realizadas con medios tecnológicos. **MÉTODOS:** científico, analítico y sintético y revisión literaria para fundamentar investigación. **RESULTADOS:** al analizar la información obtenida resulta necesario indicar que aunque existe a nivel internacional avances sobre el tema, en Guatemala son pocos respecto al tema de prevención de ataques cibernéticos a nivel de Estado. Ser un país vulnerable, las posibilidades de ataque son altas y los niveles de seguridad pocos; si las instituciones estatales o entidades privadas de alto nivel, tuviesen un ataque ciberterrorista, no existirá como procesar al responsable, conocer el grado de participación y qué pena imponer. **CONCLUSIÓN:** en un mundo que gracias al internet ha dado pasos agigantados, permite que un porcentaje alto de personas tengan acceso a un dispositivo móvil y puede ser utilizado positiva o negativamente y ocasionar graves daños a nivel institución; por ello crear un tipo penal en la legislación guatemalteca es necesario como medida de prevención y seguridad a nivel informático. El ciberterrorismo ha iniciado en otros países y es cuestión de tiempo para que su expansión y consecuencias negativas lleguen al país. A nivel público y privado el Ciberterrorismo es una amenaza, que para estudio

análisis se deben considerar muchos términos en materia de derecho, estableciendo así un “delito” idóneo e identificar de manera razonada el bien jurídico tutelado.

Palabras clave: ciberterrorismo, vertiente criminal, terrorismo, guatemalteco

Abstract

PROBLEM: determine the need for a criminal offense that establishes the margins within which jurisdictional bodies can frame certain actions and omissions carried out with technological means. **METHODS:** scientific, analytical and synthetic and literary review to support research. **RESULTS:** When analyzing the information obtained, it is necessary to indicate that although there is progress on the subject internationally, in Guatemala there is little regarding the issue of prevention of cyber attacks at the State level. Being a vulnerable country, the possibilities of attack are high and security levels are low; If state institutions or high-level private entities had a cyberterrorist attack, there would be no way to prosecute the person responsible, know the degree of participation and what penalty to impose. **CONCLUSION:** in a world that, thanks to the Internet, has made leaps and bounds, it allows a high percentage of people to have access to a mobile device and it can be used positively or negatively and cause serious damage at the institutional level; Therefore, creating a criminal offense in Guatemalan legislation is necessary as a prevention and security measure at the computer level. Cyberterrorism has begun in other countries and it is a matter of time before its expansion and negative consequences reach the country. At a public and private level, Cyberterrorism is a threat that, for study and analysis, many terms in law must be considered, thus establishing a suitable “crime” and identifying in a reasoned manner the protected legal asset.

Keywords: cyberterrorism, criminal aspect, terrorism, Guatemalan

Introducción

En Guatemala existe un sinfín de temas en legislación que analizar; dentro del presente trabajo el problema planteado es ¿Existe una teoría del tipo penal en Guatemala aplicable al ciberterrorismo a efecto de garantizar en cada caso el respeto del derecho al debido proceso? Ante esa problemática, se plantea la siguiente hipótesis: “No, no existe una teoría específica del tipo penal de ciberterrorismo en Guatemala lo cual genera incertidumbre jurídica y a la vez posibles lesiones al derecho al debido proceso, como de ahí que este tipo penal en particular debe establecer la tipificación porque son distintos al resto de delitos que se cometen en el ámbito nacional”. Es necesario que exista un tipo penal que establezca los márgenes sobre los cuales los órganos jurisdiccionales pueden encuadrar determinadas acciones u omisiones realizadas a través del uso de medios tecnológicos para causar temor, miedo y pánico dentro del Estado de Guatemala. Que conociendo el tipo penal se genere el trámite idóneo para este tipo de delitos que requieren una investigación profesional y tecnológica.

Con la creación de internet, la web y las nuevas tecnologías de comunicación han provocado en el mundo entero una revolución, que se ha extendido a las actividades más simples hasta las más complejas del diario vivir, tal es el auge del internet y las nuevas tecnologías que ya no se pueden contener o eliminar. El internet se utiliza para comunicar a personas en distintos lugares del mundo, para comercio, para la educación, con fines laborales, con fines académicos, entretenimiento, negocios, etcétera, sin embargo, su utilización ha creado nuevos campos en los que las personas pueden verse afectadas en sus bienes jurídicos pudiendo afectárseles en su patrimonio, en su privacidad e intimidad, por ese motivo los Estados deben adoptar medidas efectivas para combatir la delincuencia que pueda surgir en ese ámbito.

Los tipos penales se crean en las legislaciones según las necesidades que surjan, si nuevas acciones u omisiones vulneran bienes jurídicos de las personas, debe de crearse un tipo penal para poder aplicarle una consecuencia jurídica y con eso poder proteger a los sujetos de derecho, con la mala utilización del internet y de la tecnología se realizan determinadas conductas que ameritan ser sancionadas.

El desarrollo del trabajo de la investigación conlleva analizar términos como teoría del tipo penal, iniciando con sus aspectos generales, las diferencias que existen con otras figuras similares como la tipicidad, y tipificar deslindando tajantemente sus similitudes y diferencias; la ciberseguridad en qué consiste, su definición y cuáles son sus alcances, el ciberespacio qué lo constituye la forma de determinarlo y los problemas que surgen para determinar la competencia de los que deban de resolver los conflictos que en él surgen.

Por lo anterior, el objetivo de la investigación se enfoca en determinar la necesidad que exista un tipo penal que establezca los márgenes sobre los cuales los órganos jurisdiccionales

pueden encuadrar determinadas acciones y omisiones realizadas a través del uso de medios tecnológicos para obtener información privada con el objetivo de intimidar, coaccionar y generar pánico al Gobierno de Guatemala o su población. Que conociendo el tipo penal se genere el trámite idóneo para este tipo de delitos que requieren una investigación profesional y tecnológica.

Materiales y métodos

Para el desarrollo de la investigación lo indispensable el acceso a internet y bibliotecas virtuales. El método de investigación va de la mano con el método científico con el fin principal que permita identificar los pasos a realizar dentro del proceso. El método analítico con el cual nos enfocamos en el estudio de cada uno de los conceptos que permiten enriquecer el tema de investigación, se incluye la hermenéutica en la interpretación de la información y por último el método sintético que permite unir los conceptos que de manera individual que se han estudiado y de esta forma unificar los criterios y base para el presente estudio.

Resultados y discusión

El ciberterrorismo tiene un objetivo que consiste en realizar ciberdelitos con la utilización de internet para causar daños graves infundiendo terror, por paralizar servicios esenciales como sistemas bancarios, red telefónica, energía eléctrica y servicios públicos que se utilizan medios tecnológicos.

Martínez Atienza (2019) indica:

> Con la expresión ciberdelito se define a todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las Tecnologías de la Información y la Comunicación o que tiene como fin estos bienes, se caracteriza por ser un delito permanente al precisar de la repetición y el automatismo del hecho; su extensa y elevada lesividad; sus dificultades de averiguación y comprobación; su alto volumen de cifra negra; su mayor frecuencia, diversidad y peligrosidad; su distanciamiento espacio-temporal; y su transnacionalidad (p. 27).

Tal vez uno de los mayores retos que surgen por la comisión de ciberdelitos es la identificación de los responsables, porque los autores utilizan a terceros para que presten sus cuentas bancarias para recibir transacciones de dinero proveniente de los ilícitos, también identificar el lugar donde se realizaron los ciberataques para efectos de determinar la competencia del órgano jurisdiccional y fiscalía del Ministerio Público que deban conocer.

“Durante el año 2018 el Ministerio de Gobernación aprobó y publicó la Estrategia Nacional de Seguridad Cibernética cuyo objetivo es fortalecer las capacidades de la Nación, creando el ambiente y las condiciones necesarias para asegurar la participación, el desarrollo y ejercicio de los derechos de las personas en el ciberespacio.

Dicha estrategia cuenta con cuatro ejes estratégicos:

1) Marcos legales,

2) Educación,

3) Cultura y sociedad y

4) Tecnologías de información.

En esta estrategia se realizó un diagnóstico de la información disponible respecto al tema identificando varias fuentes de información que publican algunos datos y delitos informáticos:

1. Ministerio Público (Dentro del código penal la estrategia identifica un grupo de delitos asociados a cibercrimen)

2. Policía Nacional Civil, Unidad de combate contra los delitos informáticos

3. Superintendencia de Bancos” (Ministerio de Gobernación, 2018).

Los países han implementado diversas estrategias para combatir el cibercrimen y garantizar mayor seguridad a los usuarios de dispositivos móviles y tecnológicos. Las estrategias más efectivas han sido fortalecer el sistema legal del país para combatir el cibercrimen, lo mismo se debe de realizar en Guatemala porque se ha registrado una alto porcentaje de denuncias por estafas mediante la utilización de la tecnología, a continuación se realiza un análisis de la legislación de Latinoamérica en materia de ciberterrorismo y ciberdelitos.

Los países han implementado diversas estrategias para combatir el cibercrimen y garantizar mayor seguridad a los usuarios de dispositivos móviles y tecnológicos. Las estrategias más efectivas han sido fortalecer el sistema legal del país para combatir el cibercrimen, lo mismo se debe de realizar en Guatemala porque se ha registrado una alto porcentaje de denuncias por estafas mediante la utilización de la tecnología, a continuación se realiza un análisis de la legislación de Latinoamérica en materia de ciberterrorismo y ciberdelitos.

Martins Dos Santos (2022):

> El Convenio de Budapest sobre Ciberdelincuencia es un tratado internacional creado en el año 2001 e impulsado por el Consejo de Europa, con el objetivo de incrementar la cooperación internacional y generar marcos legales armónicos entre las naciones con el objetivo de hacer frente a los delitos informáticos y a la actividad criminal en internet.

Guatemala se enfrenta a nuevos retos por la existencia de internet y nuevas tecnologías cuya evolución no tiene precedentes, constituyen un medio para facilitar el intercambio de información en distintos rubros como negocios, seguridad, educación, salud, comercio, etc., sin embargo, algunos países se encuentran más avanzados por la correcta utilización de ese medio, para que suceda lo mismo en Guatemala se debe de investigar y descubrir la correcta utilización de esa herramienta.

La tendencia del mundo a estar más conectado genera muchos riesgos y amenazas en el entorno virtual, que lamentablemente derivan en delitos que afectan los derechos de los seres humanos, la propiedad y en ocasiones su integridad, como la pornografía infantil, la extorsión, el secuestro, la trata de personas etc.

Por los riesgos y amenazas indicados, Guatemala debe de fortalecer su marco jurídico para combatirlos de forma adecuada. En cuanto al desarrollo tecnológico, Guatemala se ha preocupado en buscar distintas medidas para implementar proyectos en esta área, equipando las escuelas con ordenadores, introduciendo la tecnología en las aulas hasta promover proyectos tecnológicos en salud y seguridad.

Conclusión

La expansión de la tecnología constituye una revolución mundial, que se ha extendido a todos los ámbitos de la sociedad, y se ha vuelto imprescindible para la realización de muchas actividades, con el surgimiento de la tecnología de forma paralela surgió un nuevo ámbito de actuación para la delincuencia a la cual se le ha denominado “Ciberespacio”, donde por medio de la utilización de dispositivos tecnológicos se realizan acciones en perjuicios de terceros. Los Estados también han utilizado sus recursos para combatir la denominada “ciberdelincuencia”, las medidas de unos Estados son más efectivas que las de otros, y algunos no le dan la importancia que amerita. Actualmente Guatemala no ha sido objeto de ciberterrorismo, por el avance tecnológico que se atraviesa a nivel mundial podría serlo, lo que generaría una crisis en la economía y otros sectores de importancia. Aunque se han propuestos instrumentos jurídicos que regulan ciberdelitos los mismos no han entrado en vigencia por diversos motivos, en consecuencia, el fortalecimiento del ordenamiento jurídico

con la tipificación de los ciberdelitos más comunes es una medida efectiva para mantener un balance jurídico a nivel interno. Por lo anterior se debe desarrollar legislación que tipifique el delito, que exista el principio de legalidad cuando los órganos jurisdiccionales conozcan un proceso en el cual las acciones u omisiones estén encaminadas al ciberterrorismo y de esta misma cuenta los juzgadores cuenten con certeza jurídica al emitir un fallo; por el otro lado se pueda proteger los derechos del sindicado durante las etapas procesales penales.

Referencias

Evans, D. (2011). Internet de las cosas, San José California. https://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

Fernández Bermejo, D. (2018). Ciberdelitos, Barcelona, Ediciones Experiencia. http://www.revistaruptura.com/index.php/ruptura/article/view/85/40

Fernandez Teruelo, J. G. (2011). Derecho Penal e Internet, Valladolid, Lex Nova. https://indret.com/wp-content/themes/indret/pdf/1172.pdf

Gómez de la Torre, I. B. (1996). Lecciones de Derecho Penal. Parte General. España, Editorial Praxis. S.A https://www.corteidh.or.cr/tablas/30160.pdf

González Amado, I. (2007): “Ciberterrorismo. Una aproximación a su tipificación como conducta delictiva. Derecho Penal y Criminología. Revista del Instituto de Ciencias Penales y Criminológicas, 28(84), 13-46 https://revistas.uexternado.edu.co/index.php/derpen/article/view/960/910

Hava García, E. (2015) El derecho penal como mecanismo de control social, España. https://doctorajuliasaenz.com/wp-content/uploads/2020/04/El-Derecho-Penal-como-mecanismo-de-control-social.pdf

Islas, O. (1998). Análisis lógico de los delitos contra la vida, 4a. México, Editorial Trillas. https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/download/2149/2406/2408

Jiménez Huerta, M. (2003). Derecho penal mexicano, México, Porrúa, Editorial. https://bibliotecavirtualceug.wordpress.com/wp-content/uploads/2017/06/59965379-manual-de-derecho-penal-mexicano-francisco-pavon-vasconcelos.pdf

Martins Dos Santos, B (2022). Convenio de Budapest sobre la Ciberdelincuencia en América Latina. Recuperado de https://www.derechosdigitales.org/18451/convenio-de-budapest-sobre-la-ciberdelincuencia-en-america-latina/#:~:text=Argentina%2C%20Chile%2C%20Costa%20Rica%2C,México%20y%20Brasil%20son%20observadores.

Mezger, E. (2001) Tratado de Derecho Penal, México. https://img.lpderecho.pe/wp-content/uploads/2018/01/Derecho-Penal-Edmundo-Mezger-LP.pdf

Moreno. L. (2020) Ciberseguridad riesgos, avances y el camino a seguir en América Latina y el Caribe. https://es.slideshare.net/slideshow/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-amrica-latina-y-elcaribe/237394241

Ministerio De Gobernación. (2018) Estrategia Nacional de Seguridad Cibernética, Guatemala. https://ogdi.org/ogdi/uploads/2021/08/Estrategia-Nacional-de-Seguridad-Cibernetica.pdf

Palacios Mota, J. (1980) Apuntes de Derecho Penal. Guatemala, Serviprensa Centroamericana. https://www.myrnamack.org.gt/images/publicaciones_fmm/Apuntes%20de%20Derecho%20Penal.pdf

Agradecimientos

Me es imperativo realizar un agradecimiento a través de este espacio a la Doctora Kendy Marisol Pérez Arreaga por ser revisora del trabajo de investigación.

Sobre la autora
Silvia Judith Corado Asencio

Estudiante de la Maestría en Derecho Penal en el Centro Universitario de Oriente de la Universidad de San Carlos de Guatemala y graduada a nivel Licenciatura en Ciencias Jurídicas y Sociales en la extensión en Chiquimula de la Universidad Mariano Gálvez de Guatemala. En el ámbito profesional laboral el aprendizaje lo he desarrollado en pequeños pasos ya que laboré en una empresa de iniciativa privada en la cual la puesta en práctica no la realicé en gran magnitud; actualmente labora en una Institución del Estado en la que se conoce las ramas del Derecho como Laboral, Familia y Civil.

Financiamiento de la investigación

La investigación fue realizada con recursos propios.

Declaración de intereses

Declara no tener ningún conflicto de intereses, que puedan haber influido en los resultados obtenidos o las interpretaciones propuestas.

Declaración de consentimiento informado

El estudio se realizó respetando el Código de ética y buenas prácticas editoriales de publicación.