UNIVERSIDAD ESPÍRITU SANTO

ESCUELA DE POSTGRADO EN DERECHO

TÍTULO:

ANÁLISIS COMPARATIVO ENTRE LOS PROCESOS INVESTIGATIVOS DE ECUADOR Y DE PAÍSES MIEMBROS DEL CONVENIO DE CIBERDELINCUENCIA PARA RESOLUCIÓN DE EXTORSIONES EFECTUADAS POR MEDIOS DIGITALES DESDE EL 2018

TRABAJO DE TITULACIÓN QUE SE PRESENTA COMO REQUISITO PREVIO A OPTAR EL GRADO DE MAGÍSTER EN CRIMINALÍSTICA Y CIENCIAS FORENSES

AUTORES:

ENRIQUE GARCERANT MONROY

RAMIRO ARBOLEDA BERREZUETA

TUTOR:

Mag. SANTIAGO ORTEGA GOMERO

SAMBORONDÓN, 16 DE FEBRERO DEL AÑO 2023

RESUMEN

El presente trabajo busca analizar los actuales procesos utilizados en la investigación de secuestros extorsivos en Ecuador donde los perpetradores utilizan plataformas de internet, tales como redes sociales y/o comunicaciones, con el fin de extorsionar a los familiares de las víctimas. A través de un análisis técnico informático y jurídico, el trabajo destaca las principales mejoras con relación a los avances en la investigación de este tipo de delitos en los últimos años, al igual que los retos que enfrenta el sistema de investigaciones criminales del Ecuador en relación con países miembros del Convenio de Budapest de Cibercrímenes.

Palabras clave: Extorsión digital, Convenio de Cibercrímenes, Secuestro Extorsivo, Investigación Informática Forense, Ciberseguridad.

ABSTRACT

The following paper seeks to analyze the current investigative processes used in extorsive kidnapping situations in Ecuador, where perpetrators use internet platforms such as social networks and/or communications, with the purpose of extorting relatives of the victim. Through both a legal and IT technical analysis, the paper remarks the principal improvements regarding breakthroughs in the investigation of this type of crime in the past years, while at the same time highlighting the challenges that the Ecuadorian criminal investigations system faces compared to other member countries of the Budapest Convention on Cybercrime.

Keywords: Digital extorsion, Cybercrime Convention, Extorsive Kidnapping, Forensic Computer Investigations, Cybersecurity.

INTRODUCCIÓN

Las plataformas digitales para comunicación (mensajería / correo electrónico) y redes sociales han sido masivamente adoptadas por personas en un amplio rango de edades a nivel mundial. Esta adopción, sin embargo, ha dado paso a múltiples debates sobre el manejo de privacidad e información personal. Motivados por este debate, las regulaciones que gobiernan estas plataformas han permitido la creación de cuentas con filtros de privacidad que facilitan el anonimato. Esto, a su vez, ha dado paso a la creación de cuentas que, abusando de este anonimato, se utilizan para el cometimiento de delitos comunes como los secuestros extorsivos, dificultando enormemente la investigación forense.

Para atacar esta problemática, el Consejo de Europa motivó la creación de un convenio para combatir "conductas ilícitas relacionadas con el uso de las computadoras" (Estrada & Somellera, 1998) junto a otros países firmó un convenio conocido como el "Convenio de Budapest". Este convenio, el primero de su clase, sentó la base para que las legislaciones de los países firmantes, y los proveedores de servicios en sus jurisdicciones respectivas, faciliten herramientas a las agencias de la ley para investigaciones judiciales (Novoa Toledo & Venegas Cruz, Herramientas del Convenio de Budapest sobre ciberdelincuencia y su adecuación a la legislación nacional, 2020). Ecuador, hasta el día de hoy, no forma parte de ningún convenio de este tipo, dificultando el acceso a las mencionadas herramientas que permitan la localización de los autores materiales de un delito flagrante ejecutado por medios digitales. Recién en el 2022, se tomaron los primeros pasos en firme para acercarse a una posible adhesión de Ecuador ante el Consejo de Europa.

A partir del mes de enero del 2018, el Consulado General de los EE. UU., mediante su Oficina de Investigaciones Criminales, inició un programa de capacitación a la Policía Nacional sobre las herramientas previamente descritas, y como el sistema de investigación ecuatoriano podría acceder a ellas con las limitaciones del caso por su no pertenencia al Convenio de Budapest. Una de las unidades policiales que más se ha beneficiado con esta capacitación es la

Unidad Anti-Secuestro y Extorsión (UNASE), quienes en los últimos años han demostrado resultados tangibles y positivos, ayudados por este tipo de herramientas.

El presente documento utilizó un enfoque metodológico principalmente de análisis sintético, complementándolo con referencias bibliográficas. Esto con el fin de comprender, en principio, la evolución de los métodos de informática forense implementados en la actualidad por la UNASE – Guayas, responsable de la región sur del Ecuador, para la resolución de casos de secuestro y extorsión en las que se utilizan medios digitales. Consecuentemente, se aplicó un análisis sintético entre los recursos investigativos y judiciales a disposición de la Fiscalía General y la Policía Nacional del Ecuador, y los sistemas investigativos de otros países miembros del Convenio de Budapest. Finalmente, se discute como la no adhesión de Ecuador a este tipo de convenios dificulta la resolución de estos delitos. La investigación evidencia como los procesos investigativos en los casos de secuestro extorsivo han mejorado con el uso de portales informáticos para asistir a agencias de la ley. Estos nuevos mecanismos ayudan a preservar la integridad de las víctimas, y facilitar la pronta captura de los agresores.

MARCO TEÓRICO

La dinámica de un secuestro económico (o secuestro "tradicional"), es su base más sencilla consiste en la retención de forma indebida de una persona donde se exige una suma de dinero o un acto en retribución a cambio de su libertad. En este tipo de secuestro generalmente se tiene contacto con un miembro de la familia, que es con quien se negocia la liberación. (Yam Chale & Trujano Ruiz, 2014, p. 780). Este delito en particular ha evolucionado con el tiempo, logrando sofisticarse en sus métodos con el uso de tecnologías de información y de comunicaciones. Las "cartas de rescate" pasaron de ser un papel con letras cortadas de revistas y pegadas formando frases, a mensajes de texto, audio y video mucho más agresivos y explícitos.

En Ecuador, desde hace ya algunos años, los delincuentes utilizan plataformas como Whatsapp, Facebook, Instagram y Twitter para el cometimiento de extorsiones y estafas. La Policía Nacional reveló que, durante el año 2021, se denunciaron 362 extorsiones entre Guayaquil, Durán y Samborondón. De estas, 140 se ejecutaron usando medios tecnológicos. (Muñoz, 2022). Esta situación, se relaciona con el rápido avance de las tecnologías de información genera una extensa brecha entre el cometimiento de delitos por medios digitales y la capacidad del estado para judicializarlas y sancionarlas. (Clough, 2014).

Lógicamente, corresponde indicar que desde la postura de Morán y Morán (2020), el cambio de visión en materia de telecomunicaciones ha influenciado en el comportamiento humano, por lo que se ha tratado de establecer mecanismos de seguridad informática, pero a la par los delincuentes también han sabido vulnerar dichas seguridades. Es por tal motivo que, Paguay (2020), reconoció a los delitos informáticos como un acto doloso, de carácter antijurídico y con presupuestos de culpabilidad dado al uso indebido de datos informáticos con la intención de perjudicar a terceros. En tal contexto, al observarse lo expuesto por Rodríguez (2018), las redes sociales representan especialmente ese medio más fértil para obtener datos personales que pueden ser aprovechados por delincuentes.

Al considerar lo previamente dicho, según Barrio (2018), el ciberespacio debe contar con mayores medidas de protección, lo que comprende tanto lo jurídico como lo tecnológico. Este criterio estaría refrendado por lo expuesto por Palazzi (2019), quien acotó que la seguridad informática aún es un tema que requiere de mayores prevenciones criminológicas. En tanto que Sain y Azzolin (2017), sugirieron que la captación de información de plataformas digitales no solo debe ser visto como una debilidad técnica, sino también jurídica. En esta perspectiva, Mayer (2016), expuso que los delitos informáticos suponen un grado de conciencia, experticia y dolo. Por su parte, Santos y Teixeira (2020), reafirman que se entenderá por delito cibernético como todo acto contrario a las seguridades informáticas que se produzca en el ciberespacio dado que se sustentan en la evolución de la dimensión tecnológica.

Por lo tanto, se reconoce que el factor constante que prima en el cometimiento del secuestro extorsivo es la necesidad del secuestrador o extorsionador de comunicarse con quienes guarden un interés con el secuestrado, y, por ende, es importante que exista una coordinación estrecha entre los organismos de investigación del estado y los proveedores de servicios de comunicación e internet para asegurar que existan acuerdos que permitan acceder legalmente a la información relacionada con los medios usados por el secuestrador durante las 24 horas inmediatas al secuestro. (Oficina de las Naciones Unidas Contra la Droga y el Delito, 2006)

Para ilustrar de manera más puntual y adecuada la situación precisada en las líneas anteriores, las plataformas de redes sociales más utilizadas en estos actos tienen su base operativa en los Estados Unidos, y se rigen bajo las leyes y regulaciones de ese país. (Novoa Toledo & Venegas Cruz, 2020). El cometimiento de un acto ilícito por medio de estas plataformas requiere, por ende, una acción coordinada entre el sistema investigativo de Ecuador, su contraparte en los EE. UU., y los proveedores de servicios de internet y de la plataforma como tal. Por su complejidad en cuanto a la coordinación interinstitucional e incompatibilidad de las legislaciones, solo una pequeña cantidad de este tipo de delitos son denunciados y/o resueltos. (Redacción El Universo, 2022).

En virtud del antecedente acotado líneas arriba, desde su publicación en el Registro Oficial en el año 2003, Ecuador forma parte de convenios de asistencia mutua en materia penal, y la Fiscalía General del Estado actúa como Autoridad Central para la ejecución de Asistencias Penales Internacionales (API s). (Sanmartin Mora, 2021). Sin embargo, en la práctica, el proceso de API ha demostrado ser muy lento e ineficiente para la resolución de casos que requieren una acción inmediata en flagrancia, como lo es el secuestro extorsivo. En EE. UU., un estudio demostró que en el año 2014 los tiempos de respuesta de APIs para solicitudes de Autoridades Centrales de otros países demoraban entre 6 y 23 meses (Galvagna, 2019).

Por consiguiente, corresponde acotar que El Acta de Privacidad de Comunicaciones Electrónicas de los EE. UU. (ECPA por sus siglas en inglés), prohíbe a las empresas de tecnología que compartan información de "contenido de cuenta" a gobiernos extranjeros fuera del proceso de API. Esto, sin embargo, no impide a las empresas el compartir información que no sea catalogada como "contenido de cuenta". (Galvagna, 2019). Esta información incluye datos básicos del suscriptor cruciales para una investigación de flagrancia, tales como: correos electrónicos, tarjetas de crédito y teléfonos celulares asociados a la cuenta, y direcciones de Protocolo de Internet (IP).

Esta salvedad ha permitido que algunas de estas empresas flexibilicen las solicitudes de información por métodos alternos a la API, creando equipos para respuestas a agencias de la ley (o "LERT" por sus siglas en inglés). Estos equipos aceptan solicitudes mediante portales en línea, y ofrecen respuestas en cuestión de minutos para casos de emergencia y cerca de 1 a 2 semana para casos no emergentes (Galvagna, 2019).

El proceso técnico para la investigación forense donde lo anterior aplica, inicia con el hecho de que las LERT proveen datos técnicos que pueden dar como resultado la localización exacta desde donde se origina la comunicación investigada. Esto requiere obligatoriamente que la legislación local exija que los proveedores de internet retengan los metadatos de comunicaciones privadas durante aproximadamente 1 o 2 años (Becker Castellaro & Viollier Bonvin, 2020).

A partir del mes de enero del 2018, el Consulado General de los EE. UU., mediante su Oficina de Investigaciones Criminales, inició un programa de capacitación a la Policía Nacional sobre las herramientas previamente descritas, y como el sistema de investigación ecuatoriano podría acceder a ellas con las limitaciones del caso por su no pertenencia al Convenio de Budapest. Una de las unidades policiales que más se ha beneficiado con esta capacitación es la Unidad Anti-Secuestro y Extorsión (UNASE), quienes en los últimos años han demostrado resultados tangibles y positivos, ayudados por este tipo de herramientas.

Al considerarse tal aspecto técnico, debe indicarse que la Unidad Anti-Secuestro y Extorsión de la Policía Nacional (UNASE) ha sido una de las primeras en ser capacitadas en el uso de este tipo de herramientas investigativas, gracias a la cooperación cercana con el Consulado General de los Estados Unidos. Entonces, corresponde recalcar que, si bien los métodos investigativos policiales en casos particulares no son generalmente expuestos al público, las herramientas LERT son utilizadas con frecuencia en la resolución de casos de secuestro extorsivo.

Dicho lo anterior, se debe puntualizar que hoy en día, existen instrumentos legales internacionales que encaminan a reducir dramáticamente los procesos de solicitud de información digital. Estos procesos son: El Convenio de Budapest de Ciberdelitos, el acta CLOUD (EE. UU.), la propuesta de e-Evidence (Consejo de Europa) y la Boleta para Acceso de Datos Internacional (ONU). Esta última tiene la particularidad de priorizar los derechos humanos en lo concerniente a privacidad de datos (Galvagna, 2019). Por su parte, la adhesión al Convenio de Budapest es considerado como un importante elemento para la lucha contra la delincuencia. (Guerrero Argote, 2018).

ESTADO DEL ARTE

El secuestro extorsivo ciertamente se ha visto como un delito en auge en los últimos años dentro la sociedad ecuatoriana. Por lo tanto, para poder reconocer los factores que derivan en la manifestación y agravamiento de esta problemática no se puede descuidar el impacto de las tecnologías digitales y perfiles de redes sociales, es por esta razón que se debe abordar por medio de evidencias científicas basadas en estudios rigurosos y actualizados lo concerniente a la relación e impacto de cómo las redes sociales, plataformas digitales y demás páginas y servidores de internet permiten que las redes delincuenciales cuenten con los medios adecuados para ubicar y contactar a sus víctimas, además del vínculo directo que tienen estos medios tecnológicos con el secuestro extorsivo.

En el ámbito ecuatoriano *en la actualidad teórica*, las investigaciones académicas sugieren que las Tecnologías de la Información y la Comunicación (TIC), según lo explicado por Ortíz, (2019), se han convertido en una herramienta sumamente útil para que los delincuentes informáticos instalen programas maliciosos en sitios web o apps para la comisión de actos delictivos. Este acontecimiento lleva identificar que el Ecuador no ha contado hasta la fecha con un adecuado sistema de gestión de seguridad en empresas públicas y privadas, y con menor razón las personas particulares, por lo que no se cuenta con los medios idóneos para mitigar o contener un ataque informático interno o externo. A esto se suma, que los sitios oficiales de las entidades gubernamentales del país que tienen por labor combatir los delitos informáticos no cuentan con estadísticas reales sobre su impacto, esto a sabiendas que los diversos delitos informáticos se valen de distintas herramientas digitales y del internet. Esta problemática está vigente al revisarse puntualmente las estadísticas de delitos de secuestro extorsivo, lo que no es desconocido socialmente por el uso de los mencionados medios del ciberespacio.

En virtud de lo precisado en las líneas precedentes, en cuanto a la *evolución teórica del tema* desde el enfoque de Sanmartín (2021), se tiene en cuenta que el Estado no cuenta con las principales medidas de carácter técnico y legal para proteger, garantizar y regular los datos informáticos, en especial de cara a combatir los delitos informáticos en el país, por lo que se en la actualidad lo que se conoce del tema en el medio jurídico ecuatoriano es que si el país es invitado o llega a formar parte del Convenio de Budapest, deberán llevarse a cabo un proceso de homologación de normas sustantivas y adjetivas para que respondan a los lineamientos del mencionado Convenio.

No obstante, la investigación de Jaramillo (2019), plantea que para una suscripción y adopción eficaz de las directrices del Convenio de Budapest, se debe tener no solo conocimiento, sino que se requiere contar con un amplio nivel de consciencia acerca de la relación e impacto de las TIC y el uso de la tecnología para distintos tipos de delitos, entre estos las extorsiones y los secuestros extorsivos. Es por tal razón que el citado autor estableció que en el Ecuador las estadísticas delictivas registradas por la Fiscalía y la Función Judicial no han contado con la debida observación y valoración para crear e impulsar el diseño y aplicación de políticas de

seguridad informática que respondan a los lineamientos del Convenio de Budapest sobre Ciberseguridad.

Según lo expresado en el estudio de Urbas y Kim-Kwang (2008), la adopción masiva de las TIC no es ajena al mal uso por parte de quienes pretenden utilizarlo con fines ilícitos, llevándonos hacia lo que hoy en día se conoce como crímenes habilitados por tecnología. El rango de crímenes habilitados por tecnología está en constante evolución.

Consecuentemente, el Instituto de Criminología de Australia elocuentemente los describe como los delitos cometidos por medios tecnológicos como: a) Crímenes dirigidos a computadoras y tecnologías asociadas, tales como intrusiones no autorizadas (hackeos), negaciones de servicio (DoS), creación y distribución de malware, etc.; b) Crímenes donde se utilizan computadoras y tecnologías asociadas como instrumentos de apoyo al delito, tales como explotación sexual infantil, acoso, extorsiones, fraude, robo de identidad, etc.; y c) Crímenes donde se utilizan plataformas legítimas de internet para promover bienes y servicios ilícitos, con el uso criminal de la encriptación y/o esteganografía para esconder actividades y evidencia.

Al conocerse los aspectos teóricos de la realidad ecuatoriana que establecen los fundamentos de la relación de los delitos informáticos, del secuestro extorsivo y del Convenio de Budapest para considerar su aplicación en el Ecuador, se debe analizar los fundamentos jurídicos de carácter principal, tanto a nivel del COIP, como del mencionado Convenio. Al empezar por el COIP, en su artículo 162 se establece que el secuestro extorsivo se relaciona con lo dispuesto en el artículo 161 en relación con el secuestro tradicional, donde la privación o arrebatamiento de la libertad en contra de la voluntad de la víctima está relacionada con el propósito de cometer otra infracción, así como obtener de ella o de terceros, sea dinero, bienes títulos, documentos, beneficios, al igual que acciones y omisiones que produzcan efectos jurídicos, lo que realiza a cambio de la concesión de su libertad, lo que tiene una pena privativa de libertad de diez a trece años (Asamblea Nacional de la República del Ecuador, 2014).

Debe indicarse, que dentro del secuestro extorsivo se aplicará el máximo de la pena cuando concurran algunas causales, entre las que principalmente constan: secuestro por más de

ocho días, si se ha cumplido con las condiciones impuestas para la liberación de la persona secuestrada. También se tendrá en cuenta si la persona secuestrada es menor de edad, o persona de la tercera edad, al igual si se trata de una mujer embarazada, o que padezca de alguna discapacidad o enfermedad catastrófica.

Al conocerse la fundamentación legal del secuestro extorsivo en el COIP, corresponde revisar los principales aspectos y consideraciones a nivel jurídico que plantea el Convenio de Budapest y que podrían constituir un respaldo y sustento jurídico para combatir y prevenir el secuestro extorsivo a través de los datos que son aprovechados por las organizaciones de crimen organizado por medio de las plataformas y medios digitales existentes en la web.

El artículo 13 indica que los Estados están en la obligación de establecer las penas para este tipo de ciberdelitos, de modo que se determinen con sanciones efectivas, proporcionales y disuasorias, lo que implica la imposición de penas privativas de libertad. A esto se suma lo previsto en el artículo 14 donde los Estados deberán crear los procedimientos para juzgar este tipo de delitos o infracciones. Se estima conveniente que en cuanto a los artículos 20 y 21 se contemple que los Estados dispongan las medidas necesarias para requerir a los proveedores de servicios con fines investigativos y de orden judicial toda información y procedimiento que se presuma hubiera sido utilizado para la comisión de un delito, de modo especial que esta información tendrá que ser provista en tiempo real.

Al reconocerse los temas de jurisdicción, el artículo 22 en su numeral 1 precisa que cada Estado debe adoptar las medidas legislativas, tanto para establecer su propia jurisdicción en cuanto a los delitos previstos en esta Convención. Para esto, se debe considerar que los ciberdelitos, entre los que se encuentra el secuestro extorsivo como resultado del abuso de seguridades de medios informáticos y digitales, en tanto se cometan en el territorio de alguno de los Estados Parte, cuando se cometan en un buque que enarbole su pabellón, cuando se trate de una nave matriculada según su normativa legal y cuando fuere cometido por alguno de sus nacionales en tanto que el delito sea sancionable en el lugar en que se cometió, o en el caso de que ningún Estado tenga competencia territorial dentro del mismo.

En materia de cooperación internacional, el artículo 23 de esta Convención propone que esta se desarrolle en la mayor medida posible, y que los acuerdos sean conciliables con la legislación interna de los Estados Parte.

En cuando a la asistencia mutua, el artículo 25 como aspectos principales se destaca la cooperación en materia de brindar asistencia en temas de investigación de los delitos previstos en esta Convención, así como de las técnicas y sistemas que contribuyan para los fines investigativos. Tal asistencia, en tal caso deberá guardarse conformidad con las normas y procedimientos de derecho interno del Estado que solicita la cooperación. En tal caso, el Estado que lo requiera podrá comunicar su solicitud de asistencia mutua, para lo cual se deberá esclarecer de qué manera los Estados reconocen la conducta como tipo penal en relación al delito informático cometido. Para esto, se debe reconocer la competencia que prevalezca según este Convenio y las normas de derecho interno para las investigaciones y la sanción de esta conducta sin perjuicio de lo que resulte aplicable de este instrumento internacional.

El artículo 35 de este Convenio contempla la existencia de la denominada Red 24/7, que es como el convenio denomina a la fuerza de tarea interinstitucional de cada país (conocida como Computer Security Incident Response Team o "CSIRT"), la que tiene como propósito establecer un punto de contacto permanente para los Estados Partes en términos de asesoría, comunicaciones y asistencia inmediata en relación con la investigación de delitos vinculados a sistemas y datos informáticos. Para esto se comprende el asesoramiento técnico, la conservación de datos, obtención de pruebas, así como el suministro de información de carácter jurídico y localización de sospechosos.

Paralelamente, se debe considerar lo que indica el Código Penal de los Estados Unidos, en el 18 U.S. Code § 2702. Aquí se describe concepto clave para entender los tiempos de respuesta a las solicitudes de información, tiene su base en el concepto de datos de "contenido" y "no-contenido". En el caso de datos de contenido, se refiere al contenido de la comunicación como tal. Por su parte, los datos de no-contenido se refieren a información *transaccional* de una

comunicación en particular, la cual incluye datos como: origen, destinatario, fechas, horas, direcciones IP, duración de la comunicación, etc.

Gracias a una excepción encontrada en el Acta de Privacidad de Comunicaciones Electrónicas de los Estados Unidos, las empresas proveedoras de servicios y plataformas de internet podrán divulgar, a su propia discreción, datos de no-contenido a gobiernos extranjeros que debidamente lo soliciten. Lo anterior permitió que empresas como Meta, Apple, Google, Twitter, etc., en los Estados Unidos creen los Equipos de Respuesta a las Fuerzas del Orden (o "LERT" por sus siglas en inglés. Los LERT consisten en mesas de servicio 24/7 administrados por cada proveedor (ej: Meta). Este equipo recibe solicitudes de datos de no-contenido por parte de agencias de la ley de todo el mundo, entregando información crucial que permite la localización del equipo donde se originó un ilícito (ej: un mensaje de extorsión). El éxito de las LERT, al no pasar por trámites ni procesos gubernamentales, ha permitido tiempos de respuesta mucho más rápidos. Un sondeo en el 2016 reveló que agencias de la ley europeas realizaron cerca de 120,000 solicitudes a Google, Facebook, Microsoft, Apple, y Twitter, con tiempos de respuesta entre 11 y 30 días. (Galvagna, 2019). Adicionalmente, las LERT proveen servicios "expeditos" en casos donde se determina una emergencia real.

Según lo descrito por Galavagna en su estudio del año 2019, en los Estados Unidos de América, donde se basan los principales proveedores de plataformas de internet, un estudio demostró que en el año 2014 los tiempos de respuesta de APIs para solicitudes de Autoridades Centrales de otros países demoraban entre 6 y 23 meses. Aquellos países no adheridos, como Ecuador, deben acogerse a procedimientos como el de la Asistencia Penal Internacional (API), la cual, por su complejidad, tiempo de elaboración, procesamiento y respuesta, no es útil para la investigación de delitos donde se requiere actuar en flagrancia.

De acuerdo con los estudios previamente revisados, se puede reconocer cómo la comunidad internacional ha destacado la importancia que tienen los diversos medios tecnológicos en la comisión de todo tipo de delitos (delitos comunes y ciberdelitos por igual), por lo que existe una relación directa entre estos medios y los secuestros extorsivos. Tal relación ha

sido determinante según lo revisado para que se haya reconocido y fundamentado la necesidad y la idoneidad de lo establecido en el Convenio de Budapest para prevenir y reaccionar adecuadamente a la problemática que se aborda en esta investigación.

PLANTEAMIENTO DEL PROBLEMA

Se evidencia como problema en el desarrollo de esta investigación el hecho de reconocer que el auge del empleo de los medios tecnológicos para los secuestros extorsivos resulta una realidad, tanto evidente como palpable, para la sociedad ecuatoriana. No obstante, cabe indicar que más allá de esta realidad palmaria, a nivel de la administración de justicia penal, y concretamente, en el desarrollo de las labores criminalísticas y forenses, no se cuenta con los medios técnicos y legales suficientes para combatir esta clase de delito.

Por lo tanto, al abordarse esta problemática, se requiere evaluar cómo el impulso de investigaciones destinadas para ubicar a los responsables de estos delitos con el fin de determinar las respectivas sanciones de acuerdo con el marco legal, en gran medida, depende de fortalecer los procesos técnicos y jurídicos para investigar, procesar y sancionar a los delincuentes que utilicen medios o plataformas digitales para llevar a cabo secuestros extorsivos. En consecuencia, con las falencias y deficiencias actuales en los procesos de investigación de estos delitos, se podría considerar que no se lograría comprender en dimensiones más amplias y reales "cómo" operan las redes delictivas para llevar a cabo este tipo de secuestros, de tal manera que no es posible el generar estrategias completamente efectivas para prevenir y evitar las extorsiones a nivel digital que luego deriven en secuestros, por lo que no se estaría logrando aplicar las estrategias idóneas para proteger a la ciudadanía ante la amenaza de este delito que los coloca como potenciales víctimas de estas conductas antisociales.

De acuerdo con lo previamente planteado acerca de los fundamentos que caracterizan el problema de esta investigación, corresponde la elaboración de la pregunta que habrá de permitir enfocar el propósito por el cual se desarrolla presente labor investigativa. Por consiguiente, la pregunta queda formulada de la siguiente manera:

¿Cuál es la situación actual del Estado ecuatoriano en el marco de las investigaciones de los secuestros extorsivos resultantes del empleo de medios digitales desde el 2018?

ANÁLISIS

Se debe considerar que los secuestros extorsivos en el Ecuador obedecerían a la escasa pericia que tiene el Estado para ubicar e identificar a las redes u organizaciones criminales que se sirven de las distintas plataformas digitales existentes en el internet por medio de distintas aplicaciones, las que en la actualidad cuentan con un uso cada vez más habitual y alarmante como medio de comisión de delitos, tal es el caso de las extorsiones digitales que terminan en secuestros. Efectivamente, desde esta premisa se debe tener muy en cuenta que este delito se ha posicionado y ha ganado espacio inconmensurable en la realidad ecuatoriana, por lo que resulta con mayor frecuencia o continuidad el poder observar y conocer de casos de personas que son contactadas por aplicaciones, llamadas telefónicas, redes sociales o distintas redes de mensajería donde estas son presionadas por grupos delictivos de modo que las víctimas ofrezcan sumas de dinero u otros bienes que representan una utilidad, lucro o ganancia mal habida para fortalecer la economía de estas agrupaciones al margen de la ley.

En tal sentido, conforme transcurre el tiempo, el problema tiende a agravarse en mayor medida. No solo se trata de tener conocimiento que a cualquier persona puede ser contactada por extorsionadores, sino que la realidad en cuestión parece ser más próxima y conocida de lo que se puede estimar a primera impresión. Esta concepción o percepción se justifica por cuanto no es extraño escuchar por parte de amigos, familiares e inclusive que cada individuo desde su experiencia personal afirme haber sido encontrado, contacto y amenazado por grupos extorsivos, incluso considerando el evento que muchas de estas personas ya hayan sido secuestradas por miembros de estas agrupaciones, pudiendo en algunos casos tener consecuencias fatales que lamentar.

Para poder sustentar con mayor argumento lo precisado en las líneas precedentes, se constata que en la información de registros estadísticos brindada por la Fiscalía General del Estado, concretamente por el Sistema Integrado de Actuaciones Fiscales (SIAF) con corte de 23 de diciembre de 2022, se aprecia entre noticias del delito y de delitos consumados como desde el periodo que comprende desde los años 2014 al 2022 existe un incremento bastante alto en cuanto a los delitos de secuestro extorsivo, lo que comprende desde 85 casos en el 2014 desde la vigencia del COIP, aumentando a 212 casos en 2015, 248 en 2016, 186 en 2017, 168 en 2018, 224 en 2019, 172 en 2020, 228 en 221 a la altísima cifra de 560 casos en lo que transcurría del 2022, lo que da un total de 2.083 secuestros extorsivos dentro del determinado periodo. **(Véase anexo 1).**

Por si fuera poco, en el delito de extorsión (en la que indudablemente no se puede excluir el uso de medios o plataformas digitales) se aprecian cifras como 471 casos en 2014, 1.477 en 2015, 1.740 en 2016, 1.504 en 2017, 1.570 en 2018, 1617 en 2019 2080 en 2020, 2.798 en 2021 y la cifra de crecimiento abismal de 8.227 secuestros en lo que corría del 2022, lo que establece como cifra final a 21.484 secuestros.

Al reconocer los registros estadísticos antes mencionados, se puede observar, identificar y reconocer no solo que el problema existe, sino que se está agravando, lo cual es una forma tanto eficaz y a la vez preocupante de demostrar que el secuestro extorsivo se posiciona como uno de los delitos más graves, de mayor frecuencia, mayor nivel de daño y que a su vez cuenta con mayores medios para que se pueda llevar a cabo su comisión. Esto precisamente se atribuiría como el resultado de que el Estado ecuatoriano no cuenta con políticas y directrices plenamente eficaces para poder prevenir, combatir y reducir drásticamente los secuestros extorsivos.

Precisamente, el Estado ecuatoriano al no ser Estado Parte del Convenio sobre la Ciberdelincuencia o Convenio de Budapest, en cuestión se encuentra privado de tener el sustento jurídico supranacional, a la vez vinculante y basado en la cooperación internacional para generar y disponer las medidas técnicas y jurídicas que sean necesarias para poder realizar actividades encaminadas y destinadas a implementar el rastreo de direcciones IP. Al mismo tiempo, no se

puede conformar equipos técnicos que establezcan acciones y estrategias que en el menor plazo posible permitan investigar toda plataforma tecnológica donde se presuma o donde se notifique que existan llamadas o mensajes extorsivos. Esta situación a su vez debe estar establecida normativamente con las definiciones, alcances y límites a los derechos de privacidad de modo tal que se pueda llevar a cabo las investigaciones y pericias informáticas con el mayor marco de operatividad posible que permita cumplir con las actuaciones procesales necesarias para hacer frente a estos delitos y proteger a las víctimas y ciudadanía en general de este tipo de ciberataques y delitos de naturaleza extorsiva.

El uso de los LERT por parte de la Policía Nacional del Ecuador da una leve muestra de los resultados que se podrían obtener, de darse el caso de una adhesión completa de Ecuador al Convenio de Budapest. Ecuador, previo a esta adhesión, tiene que demostrar que tiene la capacidad de perseguir a los autores materiales del hecho mediante un rastreo eficiente de las direcciones IP. En la actualidad, la ley no es clara con respecto a la información que obligatoriamente debe almacenar un proveedor de servicios de internet. No existe claridad sobre "que" información se debe almacenar ni "cuanto tiempo". Adicionalmente, como pudimos observar en las estadísticas técnias precedentes, los mayores proveedores de servicios de internet son las operadoras celulares. Estas, hoy en día, distribuyen las direcciones IP a los dispositivos móviles de su red sin mayor registro. Esto imposibilita realizar un rastreo forense ni establecer una ruta técnica que vincule el cometimiento de un delito con un equipo en particular.

CONCLUSIONES

Se considera como propuesta válida el reformar los procesos técnicos y metodológicos que actualmente implementa el sistema de investigaciones gubernamental. El gobierno del Ecuador debe tomar en cuenta la modernización de sus instrumentos legales, diplomáticos, y técnicos para dos fines principales: servirse de los beneficios del Convenio de Budapest, y servir a los demás estados miembro. Esta simple premisa permite, como meta final, servir al ciudadano común ecuatoriano que hoy en día es una víctima de la delincuencia que utiliza la tecnología

como aliada. La tecnología debe ser utilizada por el estado para atacar a quienes atentan contra la ciudadanía inocente.

Esta investigación permite fundamentar que existe una necesidad de mejorar la capacidad para efectuar rastreo de direcciones IP, tanto con los proveedores de servicio de internet fijo como con los de internet móvil. Este es el primer paso para poder realizar una investigación forense que pueda proporcionar 100% de certeza a la hora de buscar al autor material de un delito cometido por medios tecnológicos, incluyendo el secuestro extorsivo.

Luego de esto, Ecuador puede ofrecer un producto investigativo con la calidad necesaria para adherirse al Convenio de Budapest. Esta adhesión implicará también la conformación de la fuerza de tarea conjunta (Red 24/7 o "CSIRT") de la cual forme parte personal capacitado en este tipo de delitos. Como mínimo, el CSIRT deberá tener presencia de la Judicatura, Fiscalía, Policía Nacional (criminalística, unidades especiales y grupos tácticos), y el Servicio de Criminalística y Ciencias Forenses.

Finalmente, es también importante resaltar que a nivel de Ecuador, la investigación informática-forense debe fortalecerse desde la academia. Hoy en día, las universidades del país ofrecen un currículo insuficiente para preparar a los investigadores asignados a este tipo de delitos. Países asiáticos, por ejemplo, manejan carreras de 4 a 5 años en delitos informáticos. Este fortalecimiento permitirá combatir de manera más efectiva los retos del futuro relacionados con delitos cometidos por plataformas tecnológicas y el computo forense en general.

REFERENCIAS BIBLIOGRÁFICAS

Barrio, M. (2018). *Delitos 2.0.* Wolters Kluwer España.

Becker, S., & Viollier, P. (2020). La implementación del Convenio de Budapest en Chile: Un análisis a propósito del proyecto legislativo que modifica la Ley 19.223. *Revista de Derecho Universidad de Concepción* (248), 75-112. doi:DOI: 10.29393/RD248-13ICSB20013

Clough, J. (2014). A World of Difference: The Budapest Convention On Cybercrime And The Challenges Of Harmonisation. *Monash University law review. Monash University. Faculty of Law* .

Estrada, R., & Somellera, R. (1998). Delitos Informáticos. *Informática y derecho: Revista iberoamericana de derecho informático, ISSN 1136-288X, Nº 27-29*, 423-442.

Galvagna, C. (2019). The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Treaty Reform. *Notre Dame Journal of International & Comparative Law: Vol. 9 : Iss. 2 , Article 5.*

Guerrero Argote, C. (2018). De Budapest a Peru - Analisis sobre el proceso de implementacion del convenio de ciberdelincuencia.

Jaramillo, P. (2019). *Impacto de las Tecnologías de información y comunicación (TICS) en los fraudes informáticos juzgados en el Consejo de la Judicatura de la Provincia de Pichincha.* Pontificia Universidad Católica del Ecuador. Facultad de Ingeniería. Ingeniería de Sistema y Computación. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/17774/Romina_Jaramillo_Tabajo_de_Titulacion.pdf?sequence=1&isAllowed=y

Mayer, L. (2016). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Revista Ius Et Praxis* , 159-206.

Morán, J., & Morán, R. (2020). *Delitos informáticos. Reforma al artículo 190 del COIP en el contexto de la emergencia sanitaria Ecuador 2020.* Universidad de Guayaquil. Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/50908/1/Jonathan%20Mor%C3%A1n%20-%20Ruth%20Mor%C3%A1n%20BDER-TPrG%20227-2020.pdf

Muñoz, G. (2022). Extorsión o estafas bajo la lupa. *Diario Expreso*.

Novoa Toledo, I., & Venegas Cruz, L. (2020). Herramientas del Convenio de Budapest sobre ciberdelincuencia y su adecuación a la legislación nacional.

Oficina de las Naciones Unidas Contra la Droga y el Delito. (2006). *Manual de lucha contra el secuestro.* Vienna.

Ortíz, N. (2019). Normativa legal sobre delitos informáticos en Ecuador. *Revista Científica Hllazgos21, 4*(1), 100-11. Obtenido de https://revistas.pucese.edu.ec/hallazgos21/

Paguay, V. (2020). *Las nuevas perspectivas regulatorias de delitos informáticos en las compras a través de internet.* Universidad Nacional de Chimborazo. Obtenido de http://dspace.unach.edu.ec/bitstream/51000/7607/1/8.-TESIS%20VER%C3%93NICA%20LILIANA%20PAGUAY%20CALDER%C3%93N-DER.pdf

Palazzi, P. (2019). *Delitos contra la intimidad informática.* Editorial Pablo Andrés Palazzi.

Redacción El Universo. (Mayo de 2022). Varios Estados firman el protocolo del Convenio contra cibercrimen.

Rodríguez, C. (2018). *Metodología de clasificación de delitos informáticos en redes soclaes. Su tipificación según las leyes del Ecuador, determinación de vacíos legales y el proceos para propuesta de ley.* Universidad Internacional SEK. Obtenido de https://repositorio.uisek.edu.ec/bitstream/123456789/3220/1/CAROL%20DE%20LAS%20MERCEDES%20RODR%C3%8DGUEZ.pdf

Sain, G., & Azzolin, H. (2017). *Delitos informáticos: investigación criminal, marco legal y peritaje.* Euros B de F.

Sanmartin, W. (2021). *Los delitos informáticos en el Código Orgánico Integral Penal y el Convenio Internacional de Budapest* . Universidad Central del Ecuador. Facultad de Jurisprudencia, Ciencias Políticas y Sociales. Obtenido de http://www.dspace.uce.edu.ec/bitstream/25000/25177/1/UCE-FJCPS-CD-SANMARTIN%20WALTER.pdf

Santos, A., & Teixeira, R. (2020). *Delitos Cibernéticos Nociones Básicas.* SEGEN .

Normas jurídicas

Código Orgánico Integral Penal. Asamblea Nacional de la República del Ecuador. (2014). R.O. Sup. 180 de 10-feb-2014.

Código de los Estados Unidos de América, Título 18, Código Criminal Federal. (2018) Gobierno Federal de los Estados Unidos

Convenio sobre la Ciberdelincuencia- Convenio de Budapest. Council of Europe. (2001). Council of Europe.

Anexo 1 – Estadísticas de Delitos cometidos desde el 2014 hasta el 2022 (Fuente: Fiscalía General del Estado)

FISCALÍA GENERAL DEL ESTADO
ECUADOR

DIRECCIÓN DE ESTADÍSTICA Y SISTEMAS DE INFORMACIÓN

Ciberdelitos

- Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) - ANALÍTICA FGE
- Fecha de corte: 23/12/2022
- Periodo de análisis: 10/08/2014 - 23/12/2022
- Unidad de Análisis: Noticias del delito (incluye en tentativa y consumados)

Tabla 1: Noticias de delito por año de registro

DELITOS	2014	2015	2016	2017	2018	2019	2020	2021	2022	TOTAL
ACCESO NO CONSENTIDO A UN SISTEMA INFORMÁTIC	0	0	0	219	237	241	292	418	348	1755
ATAQUE A LA INTEGRIDAD DE SISTEMAS INFORMÁTICO	0	0	0	87	88	109	92	125	195	696
DELITOS CONTRA LA INFORMACIÓN PÚBLICA RESERVA	6	0	0	14	12	0	5	8	0	45
ESTAFA*	0	28	29	47	69	76	150	130	71	600
FALSIFICACIÓN INFORMÁTICA	0	0	0	0	0	0	0	0	23	23
INTERCEPTACIÓN ILEGAL DE DATOS	0	0	82	62	0	86	71	67	77	445
PORNOGRAFÍA CON UTILIZACIÓN DE NIÑAS, NIÑOS O	0	0	101	106	101	81	119	131	107	746
REVELACIÓN ILEGAL DE BASE DE DATOS	29	0	0	0	47	31	30	27	63	227
TRANSFERENCIA ELECTRÓNICA DE ACTIVO PATRIMON	0	0	0	0	0	0	77	212	112	401
VIOLACIÓN A LA INTIMIDAD	0	0	1523	1673	2076	2034	2003	1880	1697	12886
ACOSO SEXUAL**	0	0	0	0	0	0	0	1	87	88
EXTORSIÓN	471	1477	1740	1504	1570	1617	2080	2798	8227	21484
SECUESTRO	477	1200	935	805	962	893	619	688	862	7441
SECUESTRO EXTORSIVO	85	212	248	186	168	224	172	228	560	2083
TOTAL	**1068**	**2917**	**4658**	**4703**	**5330**	**5392**	**5710**	**6713**	**12429**	**17824**