593 Digital Publisher
CEIT
ISSN 2588-0705

Delito de Ciberextorsicion: Un Análisis Jurídico, y Comparativo en País de Latinoamérica, Perú, Colombia y Ecuador

Crime of Cyberextortion: A Legal and Comparative Analysis in Latin American Countries, Peru, Colombia and Ecuador

Alex Benjamín Quezada-Quizhpe [1]
Pontificia Universidad Católica del Ecuador Sede Manabí
aquezada8085@pucesm.edu.ec

Carla Guadalupe Gende-Ruperti[2]
Pontificia Universidad Católica del Ecuador Sede Manabí
cgende@pucesm.edu.ec

doi.org/10.33386/593dp.2025.1.2893

V10-N1 (ene-feb) 2025, pp 546-556 | Recibido: 31 de octubre del 2024 - Aceptado: 05 de noviembre del 2024 (2 ronda rev.)

1 Estudiante de la maestría en Derecho Penal de la Universidad Pontificia Central del Ecuador sede Manabí.

Cómo citar este artículo en norma APA:A

Quezada-Quizhpe, A., & Gende-Ruperti, C., (2025). Delito de Ciberextorsicion: Un Análisis Jurídico, y Comparativo en País de Latinoamérica, Perú, Colombia y Ecuador. 593 Digital Publisher CEIT, 10(1), 546-556, https://doi.org/10.33386/593dp.2025.1.2893

Descargar para Mendeley y Zotero

RESUMEN

La ciberextorsión se ha convertido en un fenómeno delictivo creciente en América Latina, en países como Colombia, Perú y Ecuador. Este delito, que implica la obtención de dinero o beneficios a través de amenazas realizadas por medios digitales, plantea desafíos significativos para los sistemas penales de cada país.

En Colombia la legislación colombiana contempla la extorsión como un delito tipificado en el Código Penal. Esto ha permitido a las autoridades judiciales avanzar en la persecución de los responsables en un contexto donde las tecnologías de la información juegan un rol crucial. Por su parte en Perú, en su Código Penal sanciona la extorsión, aunque similarmente no existe una mención explícita sobre la ciberextorsión. Sin embargo, la ley ha sido adaptada a las nuevas realidades tecnológicas a través de reformas, que busca abordar delitos informáticos.

En Ecuador, el Código Orgánico Integral Penal (COIP). En su cuerpo normativo tipifica la extorsión como un mecanismo de defensa ante los hechos y ha avanzado en la inclusión de conceptos relativos a los delitos informáticos.

Palabras claves: ciberextrosión Colombia, Perú y Ecuador.

ABSTRACT

Cyberextortion has become a growing criminal phenomenon in Latin America, in countries such as Colombia, Peru and Ecuador. This crime, which involves obtaining money or profit through threats made through digital means, poses significant challenges to each country's criminal systems.

In Colombia, Colombian legislation contemplates extortion as a crime typified in the Penal Code. This has allowed the judicial authorities to make progress in the prosecution of those responsible in a context where information technologies play a crucial role. For its part, in Peru, its Penal Code punishes extortion, although similarly there is no explicit mention of cyberextortion. However, the law has been adapted to the new technological realities through reforms, which seek to address computer crimes.

In Ecuador, the Integral Organic Criminal Code (COIP). In its regulatory body, it typifies extortion as a defense mechanism against the facts and has made progress in the inclusion of concepts related to computer crimes.

Keywords: cyberextortion, Colombia, Peru and Ecuador.

INTRODUCCIÓN

La ciberextorsión se ha convertido en uno de los delitos más preocupantes en el entorno digital contemporáneo, afectando a individuos, empresas e instituciones a nivel global. En países de América Latina como Colombia, Perú y Ecuador, esta problemática ha ido en aumento, motivada por la expansión de la tecnología de la información y la comunicación, así como por la falta de legislación específica y de mecanismos efectivos para combatirla.

La ciberextorsión se ha convertido en un fenómeno delictivo creciente en el contexto de la digitalización y el uso masivo de tecnologías de la información. Este delito consiste en amenazar a una persona o entidad con divulgar información sensible o causar daño a sus sistemas informáticos, a menos que se realice un pago o se cumpla con otras exigencias. A continuación, se ofrece un análisis jurídico y comparativo de la ciberextorsión en Perú, Colombia y Ecuador.

Este estudio tiene como objetivo contribuir a la comprensión del fenómeno de la ciberextorsión. Este delito consiste en amenazar a una persona o entidad con divulgar información sensible o causar daño a sus sistemas informáticos, a menos que se realice un pago o se cumpla con otras exigencias en la región, siendo necesario el reforzar los marcos legales, mejorar la cooperación entre países y fomentar la educación y concienciación sobre la seguridad cibernética. Además, se pretende ofrecer recomendaciones para optimizar la respuesta del estado y la sociedad frente a este delito, que no solo afecta la seguridad individual, sino también el desarrollo económico y social de las naciones.

Preguntas de investigación

¿Cómo se tipifica el delito de ciberextorsión en la legislación de Colombia, Perú y Ecuador?

¿Cuáles son las diferencias de las sanciones o penas del delito de ciberextorsión de estos tres países?

¿Qué medidas debería adoptar la legislación ecuatoriana, para enfrentar el delito de ciberextorcio?

OBJETIVOS

1.2. OBJETIVOS GENERALES

Comparar y Analizar la legislación del delito de ciberextorsión en los países de Colombia, Perú y Ecuador.

Objetivos específicos

Analizar la legislación de los países de Colombia, Perú y Ecuador para determinar la diferencia en la tipificación y penalización del delito de ciberextorsión**.**

Comparar la efectividad de las condenas y determinar si son disuasorias en la práctica.

Proponer el endurecimiento de sanciones más específicas en el Código Orgánico Integral Penal del Ecuador.

2. METODOLOGIA

Diseño de la investigación

El desarrollo del presente Articulo científico será mediante el método comparativo, descriptivo y bibliográfico los cuales nos permitirán realizar un análisis jurídico y comparativo del delito de ciberextorsión en países como Perú, Colombia y Ecuador, se estructurará una metodología adecuada que permita abordar el tema de forma sistemática.

2.2. Método Comparativo

El enfoque comparativo nos permite realizar un fundamentado cotejamiento de las diferentes legislaciones penales de Colombia y Peru, con la legislación ecuatoriana permitiéndonos comprender las similitudes y diferencias del impacto que tiene este delito.

2.3. Método Descriptivo

El método descriptivo nos ha conducido a identificar y detallar las diferentes formas

593 Digital Publisher CEIT ISSN 2588-0705

en que se presenta el delito ciberextorsión en estos países. Para entender la magnitud y las características de dicho fenómeno, se ha requerido una combinación de estos métodos.

Se han empleado únicamente método comparativo y descriptivo en esta investigación, lo que ha permitido la confrontación y recopilación de información de la legislación de estos 3 países, que describen con precisión las diferencias y semejanzas del delito de ciberextorsión.

El uso de este método comparativo y descriptivo ha permitido una evaluación objetiva y detallada del impacto del delito de ciberextorsión, y ha proporcionado una base sólida para endurecer las penas en Ecuador.

3. MARCO TEORICO

3.1. Delito

El delito es una conducta considerada ilícita y que está sancionada por la ley. De forma simplificada, se refiere a cualquier acto u omisión que infringe una norma legal establecida por el Estado y que puede ser castigado con sanciones que van desde reparación integral hasta penas privativas de la libertad "una acción o una omisión prohibida por la ley bajo la amenaza de una pena" (Harris, 1912).

3.2. La extorsión

Para determinar el origen del delito de extorsión, debemos remontarnos a la antigüedad, ya que este delito es tan antiguo como el hombre, pero debemos tomar como punto de partida el derecho romano, según el profesor Soler al hacer la cita romana se refiere "a la fuerza o prepotencia por medio de la cual una persona ora constriñe físicamente a otra a que deje realizar un acto contra su voluntad, ora cohíbe esta voluntad mediante amenazas de un mal para determinarla a ejecutar o a no ejecutar una acción", este delito ha ido evolucionando con el pasar del tiempo a principios del siglo XX, los mafiosos norteamericanos y de Europa de aquella época, convirtieron este delito en una acción prospera, prueba de ellos era el pago que realizaban las personas dueñas de negociosos por seguridad de no ser así los negocios aparecían quemados, dañados por estos grupos delictivos.

La extorsión es un delito por el cual una persona realiza actos de intimidación, chantaje, amenazas a otra, dicho delito afecta bienes jurídicos protegidos como el patrimonio, la vida y la libertad, aunque no se debe tomar de forma estricta la violación de estos derechos ya que también se describen otros derechos reales y personales. "El delito de extorsión consiste en ejercer la violencia e intimidación en contra de una persona, privándole de su libertad ambulatoria, para obligarla a otorgar al autor o a un tercero una ventaja pecuniaria a la que no tenía derecho" (MARTÍNEZ GONZÁLES, 1991).

3.3. Ciberextorsión

La digitalización ha cambiado nuestra vida y trabajo en los últimos años. Sin embargo, ha surgido un aumento significativo en los delitos cibernéticos, entre los cuales la ciberextorsión se ha convertido en una de las amenazas más alarmantes, junto con los beneficios de la tecnología. La ciberextorsión, que se define como el acto de amenazar con dañar a una persona o entidad a cambio de un pago o alguna otra forma de beneficio, ha evolucionado rápidamente y se adapta a la creciente dependencia de los sistemas digitales (Burbano , Correa, & Oviedo, 2020).

Históricamente, la ciberextorsión comenzó con amenazas simples de revelar datos personales o comerciales. Con el tiempo, los métodos se han ido refinando, lo que ha llevado a técnicas como el ransomware, en el que los atacantes encriptan datos importantes y exigen un rescate para que puedan acceder a ellos. Se han registrado numerosos casos a nivel mundial que demuestran la gravedad de este delito. Por ejemplo, "el ataque de ransomware WannaCry en 2017 afectó a más de 200.000 computadoras en 150 países, incluidos hospitales, empresas y sistemas gubernamentales, causando daños económicos estimados en millas de millones de dólares" (Quintero, 2022).

3.4. Evolución de la ciberextorsión a nivel global

Los primeros casos de ciberextorsión surgieron en las décadas de 1980 y 1990, cuando los ciberdelincuentes comenzaron a explotar fallas en los sistemas informáticos para obtener acceso a datos confidenciales y solicitar rescates (O'Malley & Holt, 2020). La extorsión digital comenzó con amenazas de revelar datos comprometidos o virus informáticos que dañaban o bloqueaban archivos. La ciberextorsión aumentó rápidamente con la expansión de internet y el aumento de la cantidad de datos almacenados digitalmente (Centeno & Martínez, 2022).

Desde sus orígenes en las primeras décadas del uso masivo de internet, la ciberextorsión ha evolucionado significativamente. Los actos de extorsión digital eran inicialmente relativamente sencillos y estaban dirigidos a individuos o pequeñas empresas. Los métodos y tácticas utilizados por los delincuentes se volvieron más atractivos y difíciles de rastrear con el tiempo y a medida que avanzaba la tecnología (Chen, Wang, & Lang, 2021). El surgimiento de nuevas tecnologías, el aumento de la conectividad global y la creciente dependencia de los sistemas digitales en todos los aspectos de la vida personal y profesional han contribuido a la evolución de la ciberextorsión (Sugianto & Permana, 2023).

El ransomware se convirtió en una herramienta clave para los ciberextorsionadores durante los años 2000, encriptando datos y solicitando pagos para su liberación. Estas técnicas se han desarrollado y diversificado en los últimos veinte años, incluyendo el uso de criptomonedas para los pagos y la incorporación de redes de bots para aumentar el alcance de los ataques (Moussaileb, Lanet, & Bouder, 2021).

3.4. Situación actual de la ciberextorsión en Latinoamérica

Actualmente, la extorsión en línea se ha convertido en una de las amenazas cibernéticas más importantes en Latinoamérica. La región ha visto un aumento significativo en los ataques de ransomware y otros tipos de extorsión digital, que han afectado a personas, empresas y gobiernos. Los ciberdelincuentes en Latinoamérica realizan estos ataques mediante el uso de malware sofisticado, técnicas de ingeniería social y phishing (Tomalá & Martínez, 2023). La creciente dependencia de los sistemas digitales y la infraestructura tecnológica de la región han favorecido la propagación de la ciberextorsión (Chere, 2021).

En Latinoamérica, la actividad de ciberextorsión tiene múltiples manifestaciones, siendo el ransomware una de las más comunes. Los atacantes encriptan los datos de sus víctimas y luego exigen un rescate para que los liberen. Este tipo de ataque ha tenido un impacto significativo en instituciones gubernamentales, hospitales y grandes corporaciones, lo que ha provocado interrupciones en servicios vitales y pérdidas económicas significativas (Quesada , 2021). El phishing también es utilizado por los ciberdelincuentes para engañar a las personas y obtener acceso a sus sistemas, donde luego instalan malware o roban información confidencial para exigir un pago.

La digitalización y la creciente adopción de tecnologías móviles y en la nube en Latinoamérica han contribuido al aumento de la ciberextorsión. Muchas organizaciones en la zona carecen de medidas de ciberseguridad adecuadas, lo que las hace vulnerables a los ataques (Simonova, 2023) . Además, la falta de especialistas en ciberseguridad complica el problema, ya que las empresas y las organizaciones gubernamentales deben proteger sus activos digitales de amenazas cada vez más complejas.

La ciberextorsión tiene un impacto social y económico. Los servicios de salud, la educación y otros servicios esenciales se ven gravemente afectados cuando se interrumpen. Los casos de ciberextorsión pueden generar desconfianza en el uso de tecnologías digitales y obstaculizar el progreso de la transformación digital en la región (Andrade, 2024). Los gobiernos de varios países latinoamericanos están implementando políticas y programas para reforzar la ciberseguridad,

593 Digital Publisher CEIT ISSN 2588-0705

fomentar la cooperación internacional y aumentar la conciencia sobre las mejores prácticas de seguridad entre los ciudadanos y las organizaciones en respuesta a esta creciente amenaza.

3.5. Contexto legal y regulatorio en Colombia

Colombia tiene una legislación más avanzada en lo que respecta a delitos informáticos, incluyendo la ciberextorsión. La Ley 1273 de 2009 tipifica los delitos informáticos y la Ley 1908 de 2018 se enfoca en el delito de extorsión (Congreso Republica de Colombia, 2009, 24 julio).

La Ley 1273 de 2009, aborda la protección de la información y los datos en el contexto de delitos informáticos. Esta ley modifica e introduce normas al Código Penal colombiano para incluir conductas delictivas que involucran el uso de la tecnología. Algunos de los aspectos más relevantes de esta ley establecen una serie de delitos relacionados con el acceso no autorizado a sistemas informáticos, la interceptación de datos, la suplantación de personas a través de medios electrónicos, y la propagación de virus informáticos, de igual manera se establecen medidas para proteger la confidencialidad, la integridad y la disponibilidad de la información en sistemas tecnológicos, determinando penas y sanciones para los delitos tipificados, así como medidas de prevención y control ((Concreso de la Republica de Colombia, 2009, 5 de enero),CP, Art. 269A, Art. 269B, Art 269C, Art 269D, Art 269E, Art 269F, Art 269G, Art 269I, Art 269J).

La Ley 1908 de 2018, es un intento del Estado colombiano por combatir de manera más efectiva el problema de la ciberextorsión, que afecta a ciudadanos y empresas en el país, y que tiene un gran impacto en la seguridad y convivencia social. ((Congreso de la Republica de Colombia, 2018, 9 de julio), CP, Art 347, Art. 11.)

Las penas para el delito de ciberextorsión puede variar dependiendo de ciertos factores, como la gravedad de la infracción, el daño causado a la víctima y la cantidad de dinero involucrada en la extorsión, pero Las penas pueden ir desde 4 a 8 años de prisión, y en circunstancias más graves, incluso mayores. (Congreso de la Republica de Colombia, 2000)

Este enfoque busca fortalecer la seguridad en el ámbito digital y garantizar la protección de los derechos de los individuos en relación con sus datos personales y su información.

3.6. Contexto legal y regulatorio en Perú

En Perú, la ciberextorsión se encuentra contemplada en el Código Penal, específicamente en los artículos que tipifican los delitos contra el patrimonio. Si bien no se encuentra definida específicamente, la ciberextorsión puede ser encuadrada en los delitos de extorsión y/o chantaje, regulados en los artículos 200 y 201 del Código Penal. (Codigo Penal Peruano, 2024, actualizado).

El código penal establece "el que mediante violencia o amenaza obliga a una persona o a una institución pública o privada a otorgar al agente o a un tercero una ventaja económica indebida u otra ventaja de cualquier otra índole"((Codigo Penal Peruano, 2024, actualizado), Art. 200 y 201), en un contexto generalizado la "amenaza" puede presentarse en formas digitales, como enviar correos electrónicos, mensajes de texto o comunicados a través de redes sociales, donde el extorsionador amenaza a la víctima con la divulgación de información sensible o comprometedora si no se cumple con sus demandas.

Aunque la legislación peruana, no aborda de manera específica la ciberextorsión, en respuesta a este delito a tipificado adicionalmente crea la Ley N.º 30096, que busca prevenir y sancionar los delitos informáticos. ((Congreso de la Republica de Perú, 2013, 22 de octubre), Art. 1, Art. 2, Art. 3, Art. 4, Art. 5 Art. 6 Art. 7, Art. 8, Art. 9, Art. 10, Art. 11 y Art.12).

Las penas por la extorsión, incluyendo la ciberextorsión, pueden variar según la gravedad del delito. Generalmente, las penas pueden

oscilar entre 3 a 10 años de prisión, y en algunos casos, si se utilizan agravantes, las penas pueden ser más severas. Además, si hay una relación de confianza entre el extorsionador y la víctima, esto también puede incrementar la penalización (Codigo Penal Peruano, 2024, actualizado).

3.7. Contexto legal y regulatorio en Ecuador

En Ecuador, el delito de ciberextorsión no se encuentra tipificado específicamente como delito autónomo, pero se lo puede encuadrar dentro de varios tipos penales establecidos en el Código Orgánico Integral Penal (COIP), específicamente en los delitos contra la propiedad y los delitos informáticos "Extorsión.- La persona que, con el propósito de obtener provecho personal o para un tercero, exija u obligue a otro, con violencia o intimidación de cualquier forma o por cualquier medio, inclusive a través de medios digitales, electrónicos o el uso de panfletos, hojas volantes o similares, a realizar u omitir un acto, pago, entrega de bienes, depósitos o negocio jurídico en perjuicio de su patrimonio o el de un tercero" (Asamblea Nacional del Ecuador, 2014, 02, 10).

La pena para el delito de ciberextorsión puede variar según la gravedad del caso y los detalles específicos de la ofensa. Según el COIP, las penas pueden ser de prisión de entre tres a cinco años, aunque estas pueden aumentar si se consideran agravantes, como la participación de varios delincuentes o si la extorsión se realiza a través de medios tecnológicos (Asamblea Nacional del Ecuador, 2014, 02, 10).

3.8. Análisis Comparativo

Al comparar la legislación de estos tres países, se observa que, aunque todos reconocen la ciberextorsión como un delito grave, las penas y el enfoque institucional pueden variar. Perú y Colombia parecen tener un marco más desarrollado en términos de penas y prevención, mientras que Ecuador está en un proceso de consolidación de sus normativas.

Tanto Perú como Ecuador carecen de una legislación específica que tipifique claramente la ciberextorsión como delito autónomo, mientras que Colombia dispone de un marco normativo más completo y específico.

A través del análisis comparativo se destaca que mientras Perú y Colombia han avanzado en la tipificación y respuesta judicial ante el delito de ciberextrosión, Ecuador presenta retos significativos en la implementación efectiva de su normativa. Todos los países enfrentan el desafío de la educación y conciencia pública sobre los riesgos.

La existencia de penas específicas en la legislación Colombiana, para el delito de ciberextorsión actúan como un disuasivo para los delincuentes potenciales, disminuyendo la incidencia de estos delitos, En Perú, en algunos casos, la ciberextorsión se puede enmarcar dentro de delitos más generales como el chantaje o la extorsión, pero no siempre se trata como un delito específico, por otro lado, en Ecuador, el Código Orgánico Integral Penal (COIP) incluye referencias a delitos relacionados con la informática, pero, al igual que en Perú, la ciberextorsión puede no ser abordada de manera concreta. Las penas pueden depender del delito subyacente, como el chantaje, más que de la naturaleza cibernética de la extorsión.

3.9. Iniciativas y colaboraciones internacionales frente a la ciberextorsión

Dado que los ciberdelincuentes frecuentemente operan a través de fronteras, utilizando la globalización y el anonimato de internet a su favor, las iniciativas y colaboraciones internacionales son cruciales en la lucha contra la ciberextorsión (Simonova, 2023). La colaboración internacional implica la colaboración entre gobiernos, empresas privadas, organizaciones de seguridad y expertos en ciberseguridad para compartir información, recursos y estrategias para combatir estas amenazas.

Dando como resultado, La necesidad que Ecuador forme parte del Convenio No. 185 del Consejo de Europa, conocido como el Convenio de Budapest sobre la Ciberdelincuencia, se obtendría múltiples beneficios en el contexto

593 Digital Publisher CEIT ISSN 2588-0705

actual de la seguridad cibernética y la cooperación internacional, fortaleciendo la ciberseguridad, así como el mejoramiento del marco legal.

4. CONCLUSIONES

La Ciberextorsión es un delito complejo que requiere un enfoque integral que involucre el fortalecimiento normativo, la protección de las víctimas, la capacitación de las autoridades y la cooperación internacional. Los vacíos legales en Perú y Ecuador deben ser abordados de manera urgente para crear un entorno más seguro en el ciberespacio.

Colombia ha implementado leyes específicas para combatir la ciberextorsión, como el Código Penal que tipifica este delito y permite aplicar sanciones severas a los responsables. Adicionalmente, el país cuenta con una ley, que modifica el Código Penal y establece medidas para la protección de datos y la seguridad informática, además ha implementado un enfoque integral para la prevención, que incluye campañas de concienciación pública y formación en ciberseguridad.

La legislación peruana no contempla la ciberextorsión como un delito autónomo en el Código Penal, por tal razón no permite sancionar a los ciberdelincuentes de forma directa. Sin embargo, las autoridades peruanas han intensificado la persecución de estos delitos, la aplicación efectiva y la adaptación de las leyes a los nuevos métodos de extorsión digital, pero aun todavía enfrenta retos en la coordinación entre entidades y en la educación del público para prevenir estos delitos.

La ciberextorsión representa un grave reto para el sistema jurídico ecuatoriano, que debe encontrar formas efectivas para abordar este delito en un entorno digital en constante cambio. Esto incluye no solo la aplicación de las leyes existentes, sino también la modernización de la normativa y el fortalecimiento de las capacidades de las fuerzas del orden para investigar y procesar estos delitos. Es fundamental promover la educación y la prevención como herramientas clave para enfrentar la ciberextorsión y proteger a las víctimas potenciales, así como el fortalecimiento de las capacidades de las fuerzas del orden para investigar y procesar estos delitos.

Es indispensable que Ecuador forme parte del Convenio de Budapest, por tanto, en la actualidad continúa siendo un pilar fundamental en la lucha contra la ciberdelincuencia a nivel internacional. la cooperación y la armonización legislativa ha demostrado ser efectiva, su éxito depende de la continua adaptación a la evolución tecnológica y garantizar la protección de los derechos humanos en el proceso. La colaboración entre países, junto con el compromiso de actualizar y fortalecer este marco legal, será crucial para abordar los desafíos de la ciberdelincuencia en la era digital.

5. RECOMENDACIONES

Se siguiere la creación un marco legal específico que tipifique y sancione los delitos informáticos, incluyendo la ciberextorsión, con penas más severas que las previstas para la extorsión tradicional, dada la naturaleza transnacional y la complejidad de los delitos cibernéticos.

Fomentar la capacitación de fuerzas del orden y fiscalías en la investigación de delitos cibernéticos, incluyendo técnicas de ciberforense y legislación internacional en cibercrimen.

Promover la creación de acuerdos de cooperación entre países para el intercambio de información y habilidades en la lucha contra la ciberextorsión, así como la creación de unidades especializadas en delitos cibernéticos dentro de las fuerzas del orden.

Establecer un registro nacional de delitos cibernéticos que permita recopilar datos sobre la incidencia de la ciberextorsión en el país, facilitando estudios y políticas públicas informadas.

Fomentar el desarrollo de capacidades tecnológicas tanto en la policía como en el sistema judicial para la investigación de delitos cibernéticos, incluyendo la formación en técnicas de ciberseguridad.

Crear incentivos para que las víctimas denuncien estos delitos, como líneas directas de ayuda y recursos para garantizar el anonimato.

BIBLIOGRAFICA

Akcora, C., Li, Y., Gel, Y., & Kantarcioglu, M. (2020). BitcoinHeist: Topological Data Analysis for Ransomware Prediction on the Bitcoin Blockchain. *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence*, 4439-4445. doi:https://doi.org/10.24963/ijcai.2020/612

Andrade, W. (2024). Vacunas extorsivas en Ecuador: Un análisis jurídico sobre las tendencias de extorsión en América Latina. *Revista Multidisciplinaria Voces De América Y El Caribe, 1*(1), 432-473. doi:https://doi.org/10.5281/zenodo.11418026

Asamblea Constituyente. (2014). *CODIGO ORGANICO INTEGRAL PENAL, COIP.* REPUBLICA DEL ECUADOR ASAMBLEA NACIONAL. Obtenido de http://181.113.58.211/documentos/LeyTransparencia_2016/mayo/a2/6%20CODIGO%20ORGANICO%20INTEGRAL%20PENAL.pdf

Asamblea Nacional del Ecuador. (2014, 02, 10). *Código Orgánico Integral Penal.* Ecuador: Lexis. Obtenido de file:///C:/Users/Usuario%20iTC/Downloads/Z-ONE-PENAL-CODIGO_ORGANICO_INTEGRAL_PENAL_COIP%20(1).pdf

Borwell, J., Jansen, J., & Stol, W. (2022). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. *Social Science Computer Review, 40*(4), 933-954. doi:10.1177/0894439320983828

Burbano , N., Correa, C., & Oviedo, J. (2020). *Análisis de la efectividad de las políticas públicas frente al delito de extorsión en Cali durante los años 2016-2018.* Obtenido de Universidad Cooperativa de Colombia, Facultad de Ciencias Sociales: https://repository.ucc.edu.co/items/717a5f92-fe5d-4fe9-8e27-8876afbe17d9

Centeno, K., & Martínez, A. (2022). *La criminología como elemento clave para la reestructuración del actual sistema de control social penal en materia de ciberdelincuencia en Nicaragua. Tesis doctoral.* Obtenido de Universidad Nacional Autónoma de Nicaragua-León: http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/9663/1/252836.pdf

Chen, K., Wang, J., & Lang, Y. (2021). Cómo afrontar la extorsión digital: un estudio experimental de las apelaciones a beneficios y las apelaciones normativas. *ERN: Economía del comportamiento (tema)*, 62. doi:https://doi.org/10.2139/ssrn.3423200

Chere, S. (2021). Experiencias de seguridad cibernética en países europeos y latinoamericanos. Apuntes hacia la defensa nacional. *Polo del Conocimiento: Revista científico-profesional, 6*(3), 1251-1273. doi:10.23857/pc.v6i3.2432

Codigo Penal Peruano. (2024, actualizado). *Decreto Legislativo N° 635.* Perú: Editora Perú.

Concreso de la Republica de Colombia. (2009, 5 de enero). *Ley 1273 de 2009.* Colombia. Obtenido de http://www.secretariasenado.gov.co/

Congreso de la Republica de Colombia. (2000). *Ley 599 de 2000.* Colombia: DIARIO OFICIAL. AÑO CXXXVI. N. 44097. . Obtenido de www.suin-juriscol.gov.co

Congreso de la Republica de Colombia. (2018, 9 de julio). *Ley 1908 de 2018.* Colombia. Obtenido de www.funcionpublica.gov.co

Congreso de la Republica de Perú. (2013, 22 de octubre). *Ley N° 30096.* Perú. Obtenido de www.funcionpublica.gov.co

Congreso Republica de Colombia. (2009, 24 julio). *Ley 599 de 2000.* Colombia. Obtenido de www.suin-juriscol.gov.co

Estévez, P., Johnson, S., & Tilley, N. (2021). Are repeatedly extorted businesses different? A multilevel hurdle model

of extortion victimization. *Journal of quantitative criminology, 37*, 1115-1157. doi:10.1007/s10940-020-09480-8

Harris. (1912). *Principles of the criminal law.* Inglaterra: Nabu pres.

Hernandez, J., Cartwright, A., & Cartwright, E. (2020). An economic analysis of ransomware and its welfare consequences. *Royal Society Open Science, 7*, 1-14. doi:https://doi.org/10.1098/rsos.190023

Kethineni, S., & Cao, Y. (2020). El aumento de la popularidad de las criptomonedas y la actividad delictiva asociada. *Revista Internacional de Justicia Penal, 30*, 325-344. doi:https://doi.org/10.1177/1057567719827051

MARTÍNEZ GONZÁLES, M. I. (1991). *El delito de extorsión.* MADRI : Cuadernos de Polítical, NM4, EDERSA.

Moussaileb, R. C., Lanet, J., & Bouder, H. (2021). Una encuesta sobre taxonomía y mecanismos de detección de ransomware basados en Windows. *ACM Computing Surveys (CSUR), 54*, 1 - 36. doi:https://doi.org/10.1145/3453153

O'Malley, R., & Holt, K. (2022). Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. *Journal of interpersonal violence, 37*(1), 258-283. doi:10.1177/0886260520909186

O'Malley, R., & Holt, K. (2020). Los primeros casos de ciberextorsión surgieron en las décadas de 1980 y 1990, cuando los ciberdelincuentes comenzaron a explotar fallas en los sistemas informáticos para obtener acceso a datos confidenciales y solicitar rescates. La extorsión digital come. *Journal of Interpersonal Violence, 37*, 258-283. doi:https://doi.org/10.1177/0886260520909186

Primicias . (27 de Marzo de 2024). Fuerza policial contra la extorsión comienza a operar en cinco zonas del país. Obtenido de https://www.primicias.ec/noticias/seguridad/fuerza-investigativa-extorsion-policia-cinco-zonas-ecuador/

Quesada , B. (2021). *Factores de riesgo y factores protectores relacionados en el delito de extorsión . Tesis doctoral.* Obtenido de Corporación Universitaria Minuto de Dios: https://repository.uniminuto.edu/handle/10656/13447

Quintero, D. (2022). La ciberseguridad y la ciberdefensa frente a los factores de inestabilidad económicos y sociales. *Revista Ciberespacio, Tecnología e Innovación, 1*(1), 41-66. doi:https://doi.org/10.25062/2955-0270.4767

Rivas, H. (2021). *La Ineficacia de la ley 0096 de delitos informáticos en su ampliación para el delito de ciberextorsión en el Perú.* Obtenido de Tesis de pregrado. Universidad Privada San Juan Bautista: https://repositorio.upsjb.edu.pe/handle/20.500.14308/3237

Simonova, L. (2023). Soberanía digital, desafíos y riesgos de la digitalización en América Latina. *Latinskaia Amerika*(11), 6-22. doi:https://doi.org/10.31857/s0044748x0028265-0

Sugianto, A., & Permana, Y. (2023). Análisis de los actos delictivos de interrogatorio y amenazas mediante la difusión de datos personales. *Postulat, 1*(1). doi:https://doi.org/10.37010/postulat.v1i1.1147

Tomalá, D., & Martínez, D. (2023). *Derecho comparado de las legislaciones de Ecuador, Colombia y México en relación al tipo penal de extorsión. Tesis de pregrado.* Obtenido de Universidad Estatal Península de Santa Elena: https://repositorio.upse.edu.ec/handle/46000/10283

Vanegas, C., Ayala, C., Concha, E., Gaeta, I., & Roldán, J. (2015). *Informe experiencias exitosas en prevención de la criminalidad en América Latina. Una perspectiva territorial de las políticas públicas de seguridad ciudadana en América Latina.* Obtenido de Centro Internacional para la Prevención de la Criminalidad (CIPC): https://cipc-icpc.org/wp-content/uploads/2019/08/Informe_Experiencias_exitosas_en_AL_2015_VF.pdf

Vasiu, I., & Vasiu, L. (2020). Forms and consequences of the cyber threats and extortion phenomenon. *European Journal of Sustainable Development, 9*(4), 295. doi:10.14207/ejsd.2020.v9n4p295

Yuste, J., & Pastrana, S. (2021). Avaddon ransomware: análisis en profundidad y descifrado de sistemas infectados. *ArXiv, 109*. doi:https://doi.org/10.1016/j.cose.2021.102388