Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Derecho Digital

Aplicativos *gota a gota* como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales en el Perú

Trabajo fin de estudio presentado por:	Bach. Bertho Arturo Menacho Ortega
Tipo de trabajo:	Trabajo de Fin de Máster
Director/a:	Dr. Wilson Yovanny Merino Sanchez
Fecha:	28-01-2024

Resumen

La investigación reveló que mediante las apps gota a gota se obtiene dinero de procedencia ilícita por la comisión previa de ciberdelitos económicos como la ciberestafa y la ciberextorsión que valiéndose del spyware acceden a las imágenes, vídeos y audios del dispositivo móvil, para efectivizar el pago total de la deuda a cambio de evitar divulgar el material fílmico recabado. En seguida, los ciberdelincuentes encubren la procedencia ilícita del dinero recaudado mediante el ciberblanqueo de capitales por medio de videojuegos y casas de apuestas. Para ello, el estudio estableció de qué manera los aplicativos gota a gota se utilizan como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales. La metodología se conformó por el propósito básico, con enfoque cualitativo y diseño de estudio de casos, cuyo alcance fue exploratorio y el tipo socio jurídico, los datos fueron recogidos por medio de las fichas de análisis documental. El resultado más importarte fue que los países de España y Perú carecen de regulación expresa sobre los aplicativos de préstamos gota a gota, lo que permite que el estudio afronte académicamente la evolución de la cibercriminalidad y las nuevas tecnologías.

Palabras clave: fraude informático, anonimato, lavado de activos, estafa informática y ciberespacio.

Abstract

. The investigation revealed that through drop-by-drop apps, money of illicit origin is obtained through the prior commission of economic cybercrimes such as cyber-fraud and cyber-extortion that, using spyware, access the images, videos, and audios of the mobile device, to make the total payment. of the debt in exchange for avoiding disclosing the film material collected. Cybercriminals then cover up the illicit origin of the money collected through cyber money laundering through video games and betting houses. To this end, the study established how drop by drop applications are used as a concealment instrument for the commission of economic cybercrimes in digital environments. The methodology was formed by the basic purpose, with a qualitative approach and case study design, whose scope was exploratory and the socio-legal type, the data were collected through documentary analysis sheets. The most important result was that the countries of Spain and Peru lack express regulation on drop-by-drop loan applications, which allows the study to academically address the evolution of cybercrime and new technologies.

Keywords: computer fraud, anonymity, money laundering, computer fraud, and cyberspace.

Índice de contenidos

Índice de figuras

Índice de tablas

1. Introducción

El ciberespacio alberga una innumerable variedad de escenarios ciberdelictivos, empero no todos se encuentran debidamente delimitados en un ordenamiento jurídico o reglamento complementario, con ello no se está afirmando que las conductas delictivas carezcan de tipificación, sino que se intenta profundizar el tema con ahínco en la utilización de instrumentos complementarios para la configuración de ciberdelitos como la ciberestafa, la ciberextorsión y el ciberblanqueo. Desde la perspectiva de HAMPTON Y BAIG (2015), citados por WADE (2021, p. 787) se trataría de un —malware de ciberextorsión—, es decir, una subcategoría de los ciberdelitos antes descritos, el cual se desarrolló en las últimas tres décadas como nueva forma de eludir a sus contrincantes los persecutores de la cibercriminalidad.

Ahora bien, en lo que respecta al clásico gota a gota debemos preciar que se trata de una modalidad de préstamo informal que posibilita la entrega de dinero sin mayor exigencia o control, debido a la forma como se realiza la aplicación de los intereses, así como el retorno del patrimonio que puede ser diario, quincenal o mensual. Aunado a lo anterior (CORREIA *et al*., 2022, p. 2) refiere que «Estos préstamos informales son pequeños, de corta duración y de alto costo».

A estas alturas, se tiene que precisar que esta modalidad se realiza en una circunscripción física determinada, en cuanto al desembolso de dinero en efectivo que puede ser en billetes o monedas, la entrega y devolución de la cantidad solicitada que por lo general se realiza en la casa del deudor y el espacio donde se producen las amenazas ante el incumplimiento del pago del capital e intereses (PADRÓN 2023).

De lo anterior se observa que el delincuente todo el tiempo se vale de un espacio definido, lo cual no sucede con los aplicativos gota a gota en los que su alcance delictivo se practica en el ciberespacio donde es posible acrecentar la cantidad de cibervíctimas, intensificar el nivel de impacto sobre los intereses jurídicos penalmente protegidos como el patrimonio, la integridad física y moral que no pueden ser restringidos o violentados sin una causa que lo justifique.

En este instante ingresa a tallar una confluencia bilateral. De un lado, ubicamos la necesidad de liquidez de un grupo de personas que carecen de experiencia crediticia que posibilite un préstamo bancario o financiero. De acuerdo con este fragmento (LE *et al*., 2023, p. 388)

explican que «El sistema bancario en los países en desarrollo está mucho menos desarrollado que en otras partes del mundo; por lo tanto, es más común que los hogares pidan prestado dinero a través de canales informales».

De otro lado, encontramos a un grupo sofisticado dotado de conocimientos informáticos, quienes emplean sus habilidades para cometer delitos, de acuerdo con SARKAR Y SHUKLA (2023) durante los periodos de desmonetización o carencias económicas, se activa la alerta cibercriminal para generar oportunidades ciberdelictivas bajo la utilización de herramientas digitales y el desconocimiento de los cibernautas por la carencia de conciencia social y económica.

Es aquí donde se advierte la creación de *softwares* en forma de aplicativos móviles que con regularidad y sin mayor control se registran en las tiendas virtuales de los dispositivos móviles, que en apariencia deberían garantizar un nivel de seguridad amplio en beneplácito de sus consumidores, para que sean descargados masivamente por sujetos que desconocen las consecuencias delictivas que se pueden generar.

Para tal caso, resulta relevante saber las condiciones y filtros que deben superar los creadores o titulares de estos aplicativos maliciosos, en seguida conocer las formas delictivas que se estarían cometiendo en perjuicio de la sociedad y el rol que habría asumido las autoridades para hacerle frente a este flagelo, habiendo aclarado este punto se plasmó como interrogante académica ¿De qué manera los aplicativos *gota a gota* se utilizan como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales?

En esa línea, el estudio contribuirá con el incremento del acervo cognoscitivo acerca de este fenómeno, permitirá conocer los aplicativos más utilizados en los últimos años, así como su reestructuración en caso de descubrimiento, se develará *ítem criminis* con el que actúan los cibercriminales. Al mismo tiempo, el aporte se circunscribirá a tres entornos claramente definidos, el primero conformado por la sociedad digital quienes podrán conocer de primera mano las alternativas de solución para evitar convertirse en víctimas de este suceso, la colectividad académica porque se nutrirán de todas las posturas teóricas y doctrinarias predominantes sobre el tema y las autoridades debido a que conocerán directamente el modus operandi de estos cibercriminales.

1.1.Justificación del tema elegido

El panorama investigativo debe contener solidez argumentativa y académica, por lo que resulta indispensable desarrollar una serie de apartados encomendados a esclarecer las razones que justifican el desarrollo del presente estudio. En ese orden, se consideró oportuno particionar los aspectos más relevantes ubicados en los linderos teórico y social, emulando a los más destacados trabajos publicados hasta la fecha sobre el tema objeto de análisis, el cual con mayor detalle será expuesto en los próximos párrafos.

Justificación teórica

Es evidente que a la luz de la evolución digital tengamos la enorme responsabilidad de fortalecer y robustecer las vulnerabilidades que el propio diseño del sistema facilita, en nuestro caso como profesionales jurídicos digitales nos corresponde asumir el compromiso de develar las nuevas modalidades delictivas que categóricamente ocupan cada día un espacio más amplio en las mesas de debate congresales. Sin embargo, no es la única forma de contribuir con el conocimiento científico, sino que mediante el análisis de los fenómenos de ocurrencia real y tangible también es posible aportar con la academia sin que ello desmerezca otras formas de atender la problemática. Dicho lo anterior, la justificación desde la perspectiva teórico propugna dar a conocer una nueva forma de cometer delitos en espacios digitales que origina una concurrencia de otros ciberdelitos igualmente lesivos como lo son la ciberestafa, ciberextorsión y ciberblanqueo, por lo que resulta necesario presentar el problema ante la comunidad científica y brindar una serie de reflexiones que permitan reducir el riesgo de comisión ciberdelictivo por medio de la implementación de un *Cybercompliance* en diferentes escenarios ciberdelictivos.

Justificación social

La composición de la sociedad moderna adoptó una conceptualización más prolija, en la que no solo ubicamos a internautas que aprovechan los recursos para satisfacer sus necesidades básicas o de distracción, sino por lo contrario también intentan cubrir necesidades económicas mediante la realización de ciberdelitos económicos como los que giran en torno a la cibercriminalidad económica. Sin embargo, partimos de la premisa que las cibervíctimas juegan un papel primordial en este círculo delictivo, puesto que mediante un arduo trabajo de concientización y exhibición de este fenómeno se conseguirá reducir las tasas de

criminalidad que desbordan diariamente los índices más altos en los medios televisivos. En ese sentido, la justificación social radica en brindar no solo conocimiento científico, sino que también se busca alcanzar un estatus equilibrado en el que todos puedan conocer sobre este fenómeno delictivo por medio de la casuística existente, así como las soluciones o medidas que se deben adoptar para disipar o menguar la cibercriminalidad económica.

1.2. Problema y finalidad del trabajo

En seguida, se debe aterrizar la formulación de los problemas que formarán parte de la indagación sobre el fenómeno que despierta el interés del autor, esto es, el nuevo fenómeno de los aplicativos gota a gota, en un escenario distinto al que nos tenía acostumbrados la modalidad tradicional. En ese orden, se consideró oportuno plantear un problema que engloba el tema central, así como tres problemas específicos que pretenden abarcar las aristas evidenciadas en la realidad social, tal y como se aprecia a continuación.

Problema general:

- ¿De qué manera los aplicativos gota a gota se utilizan como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales?

Problemas específicos:

- ¿De qué forma los aplicativos gota a gota se utilizan como instrumento de encubrimiento para la comisión de ciberextorsión en entornos digitales?
- ¿De qué manera los aplicativos gota a gota se utilizan como instrumento de encubrimiento para la comisión de ciberestafa en entornos digitales?
- ¿De qué forma los aplicativos gota a gota se utilizan como instrumento de encubrimiento para la comisión de ciberblanqueo en entornos digitales?

1.3.Objetivos

Objetivo general:

- Establecer de qué manera los aplicativos gota a gota se utilizan como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales.

Objetivos específicos:

- Establecer de qué forma los aplicativos gota a gota se utilizan como instrumento de encubrimiento para la comisión de ciberextorsión en entornos digitales.
- Describir de qué manera los aplicativos gota a gota se utilizan como instrumento de encubrimiento para la comisión de ciberestafa en entornos digitales.
- Describir de qué manera los aplicativos gota a gota se utilizan como instrumento de encubrimiento para la comisión de ciberblanqueo en entornos digitales.

Supuesto general:

- Los aplicativos gota a gota se utilizan permanentemente como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales, dado que no existen filtros de seguridad sobre el contenido de las aplicaciones y tampoco sobre las plataformas que permiten su registro, entre las principales Play Store y Apple Store, lo que posibilita la comisión de ciberextorsión, ciberestafa y ciberblanqueo.

Supuestos específicos:

- Los aplicativos gota a gota se utilizan continuamente como instrumento de encubrimiento para la comisión de ciberextorsión en entornos digitales, en tanto que los ciberdelincuentes acceden a la totalidad de los dispositivos móviles de los internautas que descargan y registran sus datos en las aplicaciones informales, los cuales solicitan dinero a cambio de evitar compartir imágenes, vídeos o denigrar contra su buena reputación.
- Los aplicativos gota a gota se utilizan reiteradamente como instrumento de encubrimiento para la comisión de ciberestafa en entornos digitales, debido a que al tratarse de préstamos informales se conminan intereses altísimos y con el pasar de los días se convierten en impagables por sus deudores.
- Los aplicativos gota a gota se utilizan a menudo como instrumento de encubrimiento para la comisión de ciberblanqueo en entornos digitales, debido a que la ganancia ilícita obtenida por los ciberdelincuentes tiene que ingresar al flujo regular económico y para ello utilizan los videos juegos y las casas de apuesta para lavar las ganancias obtenidas de ciberdelitos previos.

2. Metodología

Es crucial destacar la relevancia de la estructura metodológica diseñada para este estudio. Su función principal es asegurar el logro de los objetivos establecidos. En base a esta premisa fundamental, se han seleccionado cuidadosamente los enunciados pertinentes. Estos enunciados se han escogido con el propósito de proporcionar una serie detallada de apuntes y reflexiones académicas. Estas reflexiones tienen como objetivo abordar de manera efectiva los problemas de investigación identificados.

En esa línea, esta metodología es esencial para investigar estos delitos, ya que su diseño determinará el abordaje de los objetivos y problemas identificados. En este caso, la selección cuidadosa de enunciados y reflexiones académicas será fundamental para entender la complejidad de estos aplicativos y su utilidad para encubrir y cometer ciberdelitos económicos. Es necesario establecer un análisis detallado que permita comprender estos mecanismos y su utilización para evadir la detección por parte de las autoridades, así como su relación con otros sistemas financieros y tecnológicos, y su influencia en la seguridad digital.

2.1. Propósito

En esta investigación, se buscó cubrir el propósito esencial, como lo expuso (BAENA, 2017), quien define la "investigación pura" como el análisis de un problema con el único fin de buscar conocimiento (p. 32). De acuerdo con esta perspectiva, su objetivo radica en generar nuevos conocimientos o ajustar los principios teóricos existentes para ampliar el campo del saber científico (ESCUDERO Y CORTEZ, 2018, p. 19).

A partir de ello, el análisis de este tema no solo busca comprender la función de estos aplicativos en el encubrimiento de ciberdelitos económicos, sino también generar nuevo conocimiento sobre su utilización en entornos digitales y, posiblemente, ajustar los principios teóricos existentes en el ámbito de la ciberseguridad y el derecho digital. Cabe resaltar que, un objetivo final intrínseco sería expandir el conocimiento científico para abordar y prevenir este tipo de delitos en el contexto tecnológico actual.

2.2. Enfoque

En este espacio, expertos destacados en la investigación, como (HERNÁNDEZ, FERNÁNDEZ Y BAPTISTA, 2014), sostienen que la orientación en la investigación se centra en áreas o temas

significativos. A diferencia de la secuencia común en estudios cuantitativos, donde la claridad respecto a las preguntas de investigación y las hipótesis antecede a la recolección y análisis de datos, en los estudios cualitativos estas interrogantes pueden surgir antes, durante o después de dichos procesos.

En adición a lo mencionado, (CHÁVEZ, COVARRUBIAS Y URIBE, 2013) señalaron que la naturaleza cualitativa de la metodología se enfoca en aspectos fenomenológicos en lugar de buscar generalizaciones. Por ende, su enfoque metodológico es más profundo que amplio, además de ser más enfocado en comprender que en explicar. La metodología cualitativa guarda una conexión directa, estrecha y relevante con la etnografía.

Sobre el particular, conviene indicar que este enfoque difiere del método común en estudios cuantitativos, donde la claridad en las preguntas de investigación y las hipótesis preceden a la recolección y análisis de datos. En estudios cualitativos, estas interrogantes pueden surgir en distintos momentos del proceso, adaptándose dinámicamente a la información obtenida. A su vez, esta metodología se conecta estrechamente con la etnografía, lo que resulta pertinente al explorar los aplicativos "gota a gota" y su integración en entornos digitales, permitiendo una comprensión más profunda de su funcionamiento y su impacto en los ciberdelitos económicos.

2.3. Diseño

Con el propósito de aclarar este punto, se consideró la perspectiva presentada por (PIMIENTA Y DE LA ORDEN, 2017). Ellos explicaron que el propósito de esta aproximación es examinar casos particulares del fenómeno bajo estudio, con la intención de generar una descripción minuciosa del caso o fenómeno desde un ángulo específico.

Siguiendo esta perspectiva, (QUEVEDO, 2021) afirmó que el propósito no reside en indagar las causas de los sucesos, sino en ofrecer una descripción intrínseca del hecho en cuestión. Se centra en detallar las características fundamentales de los fenómenos que están siendo estudiados.

Esta aproximación implica un análisis detallado de casos particulares relacionados con el uso de estos aplicativos en la comisión de ciberdelitos económicos, con el fin de comprender cómo funcionan y cómo pueden encubrir dichos delitos desde perspectivas específicas. Asimismo, al enfocarse en detallar las características fundamentales de los fenómenos estudiados, se

puede examinar estos aplicativos y la forma en la que operan como herramientas de encubrimiento en el contexto de los ciberdelitos económicos, lo que permite una comprensión más profunda y detallada de su funcionamiento y su papel en estos actos ilícitos digitales.

2.4. Nivel o alcance

El nivel exploratorio despliega una relevancia fundamental en el desarrollo de la investigación. Según lo planteado por (VERA, 2021), los estudios exploratorios representan el punto inicial, siendo los más superficiales en términos de profundidad, pero no por ello carecen de rigurosidad científica. Al contrario, sirven como la puerta de entrada al ámbito científico para abordar fenómenos novedosos, poco estudiados o específicos de una población que aún no ha sido ampliamente investigada en ese contexto.

En este escenario, los estudios exploratorios son fundamentales ya que representan el inicio de la indagación sobre fenómenos novedosos, poco estudiados o específicos de una población que aún no ha sido ampliamente investigada. En el análisis de los aplicativos gota a gota como instrumento de encubrimiento para ciberdelitos económicos, la aproximación exploratoria puede ser crucial. Esto se debe a que el fenómeno de estos aplicativos como herramienta de encubrimiento es un tema poco explorado en la investigación, lo que hace que los estudios exploratorios sean esenciales para comenzar a entender su funcionamiento, su alcance y su relación con los ciberdelitos económicos en entornos digitales. Este enfoque inicial, aunque pueda ser superficial en términos de profundidad, establece las bases para una comprensión más amplia y rigurosa en etapas posteriores de investigación.

2.5. Tipo

La travesía investigativa llevó a la definición del tipo de investigación. En este contexto, se consideró la aportación de (TANTALEÁN, 2016), quien amplía al describir que esta investigación, también conocida como sociológico-jurídica, realista-jurídica, empírico-jurídica, material-jurídica, materialista-jurídica o fáctica-jurídica, se enfoca en el análisis de cómo el derecho objetivo funciona dentro de la realidad social.

Esta investigación, se centra en el análisis del funcionamiento del derecho objetivo en la realidad social. Dentro del estudio de estos aplicativos se conocerá la utilización que le brindan los ciberdelincuentes como herramientas de encubrimiento para ciberdelitos económicos. La

comprensión del derecho objetivo se manifiesta y opera en la realidad social, especialmente en relación con estos tipos de delitos digitales. En ese sentido, proporcionaría un marco sólido para analizar aspectos sobre la aplicación de las leyes y regulaciones en entornos digitales, así como la forma en que se enfrentan estos delitos y la manera en que se pueden mejorar las medidas legales y de seguridad digital para abordar este problema emergente.

2.6. Población

Para establecer la composición del grupo seleccionado, es crucial considerar la perspectiva presentada por (ARIAS, 2021). Este autor explica que la población puede abarcar una variedad de elementos, desde individuos hasta máquinas, equipos e infraestructura; en resumen, todos los componentes tangibles que sean observables y susceptibles de evaluación.

En este apartado, se pretende comprender la diversidad de elementos que componen la población, esto podría incluir desde individuos involucrados en el uso y desarrollo de estos aplicativos hasta la infraestructura tecnológica y las herramientas empleadas para llevar a cabo estos delitos. La comprensión de esta diversidad en la población permitirá una investigación más exhaustiva y completa sobre cómo estos aplicativos se utilizan y cómo pueden abordarse desde una perspectiva legal y de seguridad digital.

2.7. Muestra

Basándonos en el punto anteriormente establecido, es relevante considerar la idea expresada por (HERNÁNDEZ Y MENDOZA, 2018). Estos autores explican que una muestra se refiere a un subconjunto de la población o universo de interés, del cual se recopilarán los datos relevantes; esta muestra debe representar de manera adecuada a la población (preferiblemente mediante métodos probabilísticos) para que los resultados obtenidos puedan generalizarse a la totalidad de la población.

La selección adecuada de la muestra es esencial, en tanto que esta debe reflejar con precisión los diversos aspectos relacionados con estos aplicativos, su uso, sus usuarios y el entorno digital donde se aplican. Una muestra representativa permitirá obtener conclusiones y hallazgos que sean aplicables y relevantes para comprender este fenómeno en su totalidad, contribuyendo a la formulación de estrategias legales y de seguridad para abordar esta problemática.

2.8.Técnica

Para la extracción de datos, se empleará la técnica de análisis documental de casuística, como señala (ATENCIÓN PRIMARIA, 1999). Esta técnica implica la utilización del conocimiento cotidiano, el análisis contextual, las opiniones de diversos actores involucrados en el tema y la consulta de fuentes documentales de diversas naturalezas.

Esta técnica de análisis documental de casuística resulta esencial, debido a que permite recopilar datos valiosos, desde la comprensión del contexto socioeconómico y tecnológico hasta las opiniones y experiencias de los individuos relacionados con el uso de estos aplicativos. Esta información variada y detallada será fundamental para comprender cómo se utilizan estos aplicativos como herramientas de encubrimiento en la comisión de ciberdelitos económicos y contribuirá al diseño de estrategias legales y de seguridad digital más efectivas para combatir esta problemática.

2.9. Instrumento

En relación con los instrumentos, se hace referencia a su utilidad para implementar la técnica escogida, que en este caso implica el uso de fichas de análisis documental. Estas fichas se aplicarán específicamente para identificar y extraer los datos más significativos de los casos estudiados en el ámbito casuístico.

3. Marco teórico y desarrollo

En este apartado se abordará las principales corrientes teóricas que intentarán explicar cada una de las categorías, subcategorías e indicadores que en su conjunto representan los hallazgos más significativos sobre el tema de investigación. En seguida, se profundizará la problemática partiendo de los postulados predecesores hasta lograr asumir una postura que permitirá contrastar los supuestos jurídicos formulados como consecuencia de la formulación del problema.

3.1. Aplicativos gota a gota

El tema que vamos a desarrollar tiene un *ex ante* y un *ex post* en la línea de tiempo de la evolución social peruana, es sin duda la teoría del crédito informal la que sustenta una manera disímil o extraoficial de acceder a préstamos dinerarios sin mayores exigencias o requisitos que los básicos en comparación con los créditos formales. Por consiguiente, uno de los estudios más significativos fue elaborado por ALVARADO *et al*. (2001) quienes explican las principales diferencias entre ambos créditos, el formal se encuentra recubierto por las relaciones financieras actuales y los acuerdos adoptados por los sujetos que integran el mercado, mientras que el no formal plantea los límites como consecuencia de las dificultades de los mercados formales y el espacio o contexto donde operan.

Tabla 1

Características del crédito informal en el Perú

Cobertura	Transacciones	Corto plazo	Barreras	Actividades
Este crédito es la fuente más relevante para la colectividad de bajos recursos.	Es el uso intensivo de información recopilada mediante vínculos sociales y económicos.	Se destinan mayormente a las actividades comerciales y de consumo.	No existen barreras para la disposición de créditos en favor de los interesados.	Los prestatarios y prestamistas están relacionados en la vida real por trabajo o vínculos sociales.

Nota. Obtenido de «*El financiamiento informal en el Perú*», ALVARADO *et al*., 2001, pp. 25-26.

En ese orden de aseveraciones, corresponde brindar una aproximación sobre los préstamos gota a gota, desde la perspectiva colombiana y su contraste con la peruana, debido a que en

el primer país mencionado se originó dicha modalidad delictiva. Para Martínez (2023) explica que hay dos clases de prestamistas, la primera se trata de un préstamo económico revestido de informalidad para su obtención y devolución, esta clase de crédito es utilizada por cuatro de cada cinco colombianos que necesitan efectivo, los plazos son de hasta dos meses y los intereses oscilan el 5 y 20 % diario, la premisa utilizada por los delincuentes es que mientras más célere sea el pago, menor será el interés. En lo que respecta a la segunda, se otorga préstamos a grandes comerciantes del país, con cuantiosas sumas de dinero, cuya devolución se realiza en un menor tiempo.

En el segundo país objeto de comparación se mantienen algunos matices de criminalidad similares, para robustecer la premisa conviene mencionar al MINISTERIO DEL INTERIOR DEL PERÚ (2023) quien refirió que esta clase de préstamos se considerada un delito que tiene entre sus principales objetivos establecer relaciones informales entre pares, de un lado los prestatarios quienes carecen de experiencia crediticia para acceder a un crédito formal y de otro lado las organizaciones criminales que por medio de la violencia y la extorsión realizan los cobros con intereses usureros e impagables y en ocasiones atentan contra la integridad física de sus deudores.

En ese orden, aterrizamos en los aplicativos gota a gota, punto concéntrico del estudio, para esclarecer el panorama ciberdelictivo resulta trascendental ubicarnos dentro de la —clasificación incidental de la tecnología de la comunicación e información—, en adelante TIC, planteada por uno de los máximos referentes del cibercrimen, pues nos referimos a MIRÓ (2012) quien divide el comportamiento criminal en tres grandes grupos de ciberataques, entre ellos ubicamos los puros, réplica y de contenido, siendo el segundo el que mejor que acomoda a los préstamos gota a gota en su vertiente digital, para conceptualizar con mayor detalle cada aspecto se ingresó el siguiente organizador visual.

Tabla 2

Incidencias de las TIC en el comportamiento criminal

Ciberataques puros	**Ciberataques réplica**	**Ciberataques de contenido**
Es una conducta criminal que adquiere sentido solo en el ámbito digital, se dirigen contra servicios	Es una conducta delictiva tradicional que no exige el traslado	Es una conducta delictuosa revestida de ilegalidad, empero no

novedosos, bienes o terminales del ciberespacio.	físico, sino una conexión con internet.	del medio que se utiliza, sino del contenido distribuido por internet.

Nota. Obtenido de «*El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*», Miró, 2012.

Al haber definido que los aplicativos de préstamos gota a gota son un ciberataque réplica debido a que se trata de una modalidad tradicional conocida también como préstamos gota a gota en América del Sur con una materialización en internet, no resulta menos importante precisar algunos detalles o diferencias entre ellas para tener más claro el asunto.

Tabla 3

Diferencias entre el gota a gota físico y virtual

Gota a gota tradicional	**Aplicativo gota a gota**
- Se publicitan mediante avisos en las calles. - Captan a personas en negocios y mercados. - Ofrecen sumas dinerarias a mano alzada. - Las exigencias financieras y personales son mínimas para la entrega del dinero. - Son intereses usureros entre 5 a 20 %. - Utilizan plazos cortos para la realización del pago entre 15 a 30 días. - Recapitalizan los créditos sobre el capital para incrementar ganancias. - Emplean la extorsión y la estafa para cobrar el dinero prestado. - Utilizan el blanqueo de capitales para encubrir la procedencia de los intereses. - El pago se realiza a la misma persona que hizo el préstamo.	- Se publicitan en los sistemas Android y iPhone. - Captan a cibernautas que navegan en las redes sociales. - Ofrecen sumas dinerarias mediante depósito, transferencia o giro. - Las exigencias financieras son mínimas, pero las personales son mayores para la entrega del dinero. - Son intereses usureros de 20 %. - Utilizan plazos de 15 o 20 días para efectuar el pago. - Otorgamiento de préstamos indefinidos y sin autorización expresa. - Emplean la ciberextorsión y ciberestafa para cobrar el dinero prestado. - Utilizan el ciberblanqueo de capitales para encubrir la procedencia de los intereses. - El pago se realiza al número de cuenta de una mula.

Nota. Obtenido de «*35 nuevas aplicaciones para el préstamo 'gota a gota': PNP alerta cuáles son*», Chillitupa, 2023.

3.1.1. Cibercriminalidad

Para lograr involucrarnos con el tema, es necesario viabilizar el entendimiento desde todas sus aristas comenzando por la cibercriminalidad, entendida como una forma de criminalidad realizada en un espacio diferente al terrenal, esto es, el ciberespacio. Para lograr ese cometido, no solo basta de uno o más sujetos con altos conocimientos informáticos, sino que también exista un medio tecnológico utilizado como terminal para la comisión del ciberdelito.

En la doctrina podemos encontrar diversos exponentes que brindan una aproximación sobre el particular, empero apostamos integralmente por lo expresado por CHANDRA Y SNOWE (2020, p. 7) al señalar que hablamos de delito cibernético a aquel acto que emplea un ordenador, el sistema tecnológico intrínseco, así como la red que facilita su funcionamiento y habilita la acción delictiva, esta conceptualización permite distinguir un delito cibernético (en línea) y un acto delictivo tradicional (fuera de línea). Aclarado lo anterior resulta pertinente explicar la teoría de la taxonomía de la cibercriminalidad para comprender las capas más resaltantes durante el hecho delictivo.

Tabla 4

Taxonomía de la cibercriminalidad

Capa de nivel	Capa de nombre	Capa de datos	Capa de víctima
Sigue una estructura jerárquica que utiliza el concepto padre-hijo para representar cada categoría de delitos cibernéticos.	Describe e identifica de manera descriptiva cada elemento.	Proporciona información sobre la definición, el vínculo del elemento con su raíz o padre, las características del elemento (como heredadas, evolucionadas o únicas) y el proceso amplio para cometer el delito cibernético.	Vincula cada delito cibernético con su primer impacto directo e inmediato.

Nota. Obtenido de «*Una taxonomía del cibercrimen: teoría y diseño*», CHANDRA Y SNOWE, 2020, p. 7.

Como si fuera poco, exponentes como (MATVEEV *et al*., 2021, p. 209) explican el fenómeno como la concatenación de actos enmarcados en el derecho penal que se externalizan en una circunscripción geográfica determinada y cometidos en el ciberespacio con intenciones de destrucción de sistemas informáticos, entre ellos, las redes y datos de suministro de información. Ahora bien, BUYAGI (2015), citado por MATVEEV *et al*., (2021, p. 205) plantea 4

etapas durante la consumación del ciberdelito, tal y como se observa en el siguiente organizador visual.

Tabla 5

Etapas del fenómeno ciberdelictivo

Etapa preparatoria	Etapa de expansión del delito cibernético	Etapa del cibercrimen transnacional	Etapa moderna del cibercrimen
Abarca el período comprendido entre finales de los años 1960 y principios de los 1970, que es el momento inicial de la comisión de delitos utilizando ordenadores electrónicos.	Abarca el período comprendido entre principios de los años 1970 y 1986. Esta etapa marcó el surgimiento de los piratas informáticos y sus grupos organizados. Terminó con la adopción de la primera ley reguladora sobre delitos cibernéticos y el primer arresto de un hacker.	El período del cibercrimen transnacional y el ciberterrorismo (1994 – principios del siglo XXI).	El surgimiento de nuevas formas de delitos informáticos (siglo XXI).

Nota. Obtenido de «*Regulación jurídica de la lucha contra el ciberdelito: el aspecto teórico y jurídico*», BUYAGI, 2015.

En respaldo a lo anterior, el CONSEJO EUROPEO (2001, p. 1) lo define como la «…acción dirigida contra la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos, así como contra el uso indebido de dichos sistemas, redes y datos…». Siguiendo la misma línea, la EUROPEAN CYBERCRIME CENTRE (2017, p. 18) expresa que «…se puede definir como cualquier delito que sólo pueden cometerse utilizando ordenadores, redes informáticas u otras formas de tecnología de la información y la comunicación (TIC)…».

Al haber esclarecido con suficiencia el fenómeno de la cibercriminalidad conviene adoptar una posición que se circunscribe al conjunto de actividades delictivas cometidas en el ciberespacio mediante la utilización de sistemas informáticos conectados a ordenadores o cualquier medio idóneo. Este flagelo atravesó por diferentes episodios hasta ubicarse en la actualidad en la denominada época moderna que posibilita la comisión de nuevas formas ciberdelictivas como la que se pretende investigar, estos son, los aplicativos gota a gota y la comisión de ciberdelitos económicos.

3.1.2. Ciberextorsión

Para brindar un abordaje completo de este flagelo social, conviene remontarnos a la descripción típica que regula el ordenamiento jurídico sustantivo del Perú, en el que se expresa que para adecuarse a esta conducta es necesario que un sujeto actúe con violencia o amenaza obligando a otra persona para que se le otorgue una ventaja económica indebida o de cualquier otra índole (OBSERVATORIO DE JURISPRUDENCIA PENAL 2022). Adicionalmente, HISCOX ESPAÑA (2023) refiere que se trata de una acción a través de la cual se obliga a una persona mediante la intimidación en plataformas digitales para que realice una acción que la perjudique, siendo la motivación principal el aspecto económico.

Una vez aclarado el concepto tradicional, corresponde situarnos en la aproximación de la ciberextorsión que debe entenderse como el acto que se conduce mediante la violencia o intimidación, empero externalizadas en medios informáticos o plataformas virtuales con el ánimo que la cibervíctima realice una acción en su prejuicio o ajeno, toda esta conducta delictiva se realiza en internet (OCHOA 2023).

Tabla 6

Conductas intrínsecas en la ciberextorsión

Actividades cibercriminales de la extorsión digital
Se realiza el bloqueo del ordenador hasta que se realice el rescate económico
Se pone en práctica el secuestro sobre el acceso a dispositivos móviles
Se paraliza el uso de las cuentas personales como las redes sociales
Se coacciona a las cibervíctimas mediante la amenaza de publicación de información personal
Se envía un texto denigrando a la cibervíctimas con sus familiares o amigos

Nota. Obtenido de «*La policía, cibercrimen y ciberseguridad*», Ochoa, 2023.

A estas alturas comenzaremos por desmenuzar los 5 momentos más importantes del —modus operandi— de la ciberextorsión a la cibervíctima que solicitó el préstamo informal. El primer

paso consiste en el ofrecimiento de créditos informales, dicho de orto modo, de acceso directo, los cuales son difundidos en las plataformas contenidas en redes sociales que redireccionan a las tiendas virtuales Android o iPhone, estos ciberdelincuentes aprovechan que muchas de las personas carecen de historial crediticio en los bancos o entidades financieras y necesitan de manera urgente cubrir necesidades básicas como la alimentación, vestimenta o medicina.

El segundo paso radica en elegir una de las diferentes aplicaciones informales que ofrecen el servicio de préstamo informal, habiéndolo elegido se procede con la descarga del aplicativo, el cual exigirá que el usuario autorice de forma obligatoria conceder el acceso total al dispositivo móvil, apreciándose la aparición del malware en forma de spyware. Además, se le exigirá que complete una serie de datos entre los que resalta los nombres y apellidos, el número de documento de celular y la cuenta de ahorros a la que se le depositará el monto solicitado o no por la cibervíctima.

El tercer paso consiste en transferir el monto requerido o no al número de cuenta proporcionado previamente en la plataforma, indicamos esto último porque se evidenciaron casos en donde solo se completó el segundo paso y sin mayor requerimiento expreso se abonó dinero en la cuenta del usuario con intereses sumamente altos y en un tiempo muy corto para el pago.

El cuarto paso resulta determinante porque permite la externalización de diferentes ciberdelitos como los que expondremos a continuación, teniendo en cuenta que durante la descarga e instalación del aplicativo se concedieron accesos absolutos al dispositivo móvil, los cibercriminales recogen toda la información sobre los contactos, fotos y vídeos personales para empezar con las amenazas por la demora en la devolución de la deuda y los intereses, así como la intimidación de difundir estos archivos privados en redes de fuente abierta, configurándose la ciberextorsión.

El último paso explica el modo en que los cibercriminales ingresan el dinero obtenido de forma ilícita al sistema económico sin levantar sospecha de las autoridades estatales, pese a realizarse movimiento financieros considerables. Recordemos que nunca se realiza el desembolso del dinero desde la cuenta personal del cibercriminal y por consecuencia tampoco se devuelve a una cuenta asociada a este delincuente informático, dado que pare eso usan a receptores denominados por la doctrina como interpósita persona o mulas que brindan sus

cuentas bancarias para transferir y recibir pagos provenientes de actividades criminales, quienes a su vez lo transfieren a otros sujetos hasta que se pierda la pista del receptor final. Luego, para evitar levantar sospechas ingresan el dinero en juegos virtuales, apuesta deportivas o adquieren monedas virtuales para que posteriormente puedan extraer el dinero como retiro o ganancia proveniente de dichas fuentes, con lo que se configura el ciberblanqueo de capitales.

3.1.2.1. Malware

Es una terminología universal utilizada para cualquier —malicious software— creado para infiltrarse en un dispositivo sin accesos o autorizaciones y causar interrupciones o daños en el sistema (BELCIC 2023). Existen diferentes modalidades de *software* que plasman objetivos diferentes, algunos pretenden destruir sistemas informáticos o en su defecto el contenido preexistente a través de los virus, así como los gusanos o troyanos. El recorrido atraviesa el acceso remoto por el sistema de información mediante la red como es el supuesto de los *botnets* o los *rootkits* que colocan en la subrepticiedad a los software maliciosos o en su defecto posibilitan el control del sistema (MIRÓ 2012).

En adición a lo anterior, el malware según lo expresado por KASPERSKY (2023a) «puede infectar computadoras y dispositivos de varias maneras y se presenta en diversas formas, algunas de las cuales incluyen virus, gusanos, troyanos, spyware y más». Sin duda, nos queda claro que estamos frente a un programa elaborado para infectar dispositivos y dañarlo de todas las maneras posibles.

Tabla 7

Las categorías del malware

Tipos de malware	
Ransomware	Es considerada una versión maliciosa del software plasmado como una nota de rescate de un cibersecuestrador, funciona mediante el bloqueo y denegación del acceso a un dispositivo.

Spyware	Se encarga de recabar información sobre un dispositivo conectado a la red para derivárselo al ciberdelincuente, se suele utilizar el programa Pegasus para registrar la actividad y datos personales de una persona.
Gusanos	Se dedica a infectar los equipos para replicar y extender su campo de acción a otros dispositivos adicionales para mantener un estado activo en todos los dispositivos.
Adware	Se usa para bombardear el dispositivo con infección mediante anuncios que uno no autoriza, entre ellos ubicamos a los juegos gratuitos y las barras permanentes en el navegador.
Troyanos	Se utiliza como un tipo de malware de camuflaje, mediante la infiltración en el dispositivo de la cibervíctima aparentando una falsa legitimidad del software.
Botnets	Es una red de equipos compuesta de códigos informáticos que realiza o efectiviza un malware, para ello se empleo a los *bots*, quienes son capaces de responder a órdenes desde un controlador.

Nota. Obtenido de «¿Qué es el malware y cómo protegerse de los ataques?», BELCIC, 2023.

3.1.2.2. Ransomware

En este espacio develaremos que el ransomware es un programa malicioso que fue diseñado con el propósito de extorsionar a los usuarios imposibilitando su acceso a los datos u otros

recursos de las tecnologías de la información, en esencia es un secuestro de datos o recursos que se origina en el ciberespacio (KESHAVARZI Y GHAFFARY 2023).

En sintonía con la anterior, INFOBAE (2023) expresa que es una clase de software malicioso que mediante la encriptación de información en un ordenador solicita un rescate económico para recuperar dichos datos. En el supuesto que la cibervíctima no cumpla con el requerimiento del cibercriminal en un plazo temporal específico, nunca recuperará el material extraído.

3.1.2.3. Spyware

Es una tipo de software que se integra en los ordenadores bajo la subrepticiedad, dado que el usuario no autoriza dicha instalación, es difícil de detectar el momento en que se instala, así como el momento exacto en que se recopila los datos para transferirlos a terceros (BANCO BILBAO VIZCAYA ARGENTARIA 2023). A su vez, KASPERSKY (2023b, párr. 6) precisa que «es un software que se instala sin tu consentimiento informado, ya sea un ordenador tradicional, una aplicación en el navegador web o una aplicación móvil que se encuentra en tu dispositivo». En respaldo a lo anterior, se puede indicar que esta clase de malware puede infectar toda clase de dispositivos sin importar la marca u origen con la finalidad de brindar a los ciberdelincuentes acceso completo a la información confidencial, entre ellas, las contraseñas, datos sobre registros de datos bancarios o la identidad virtual completa (SEGUIN 2020).

Tabla 8

Tipos de spyware

Keyloggers	Adware	Infostealers
Es considerado uno de los más perjudiciales, debido a que registra las teclas que pulsa el usuario des el ordenador, se pueden registrar contraseñas de toda clase.	Es apreciado como el más común debido a que posibilita la generación constante de publicidad emergente denominados pop-ups, permite que se guarde y trasmita información sin autorización del usuario.	Es considerado uno de los más peligrosos, pasa desapercibido por el usuario mientras recopila y transmite indiscriminadamente información del ordenador.

Nota. Obtenido de «*Spyware: qué es, qué tipos hay y cómo se puede eliminar*», BBVA, 2023.

En esa línea, queda claro que de acuerdo con BELCIC (2023, p. 10) «Ningún dispositivo es inmune al malware: los equipos de escritorio, los ordenadores portátiles, los móviles y las tabletas son susceptibles». Es decir, tanto las PC, Mac, iPhone y Android son susceptibles de verse afectados por estas clases de malware, estos últimos dispositivos pueden infectarse mediante los SMS, ataques de correo electrónico, ventanas emergentes y ataques de tipo —drive-by— en sitios web carentes de seguridad.

3.1.2.4. Aplicación de software espía para dispositivos

A estas alturas del estudio tenemos que responder preliminarmente a la interrogante ¿De qué manera los aplicativos gota a gota se utilizan como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales? Es sin duda, una incógnita que debe ser develada en tanto que nos encontramos frente a una aplicación de software espía para dispositivos móviles, estas son desarrolladas para teléfonos inteligentes y posibilitan que el ciberdelincuente pueda monitorearlo de forma oculta, una de las apps más conocidas es '*StealthGenie*' y por la estructura del software es capaz de interceptar llamadas, monitorear conversaciones, mensajes de correo electrónico, texto SMS, correo de voz, libreta de direcciones, fotos y vídeos de la galería (STEALTHGENIE MOBILE DEVICE SPYWARE APPLICATION 2014).

Posteriormente, el cibercriminal que tiene a buen recudo la información de la cibervíctima que accedió a los aplicativos de préstamos informales para solicitar una suma dineraria o simplemente con la curiosidad de conocer como funcionaba, concedió de forma obligatoria sus derechos para que al descargar la aplicación e instalarla tengan acceso total al dispositivo. En un segundo momento, ante la falta de pago empiezan la ciberextorsión mediante el envío de mensajes a los familiares y amigos que encuentren en el directorio de llamadas del celular, así como de las redes sociales, con el propósito de menoscabar la imagen de la víctima y coaccionarla al pago del monto inicial y los intereses inflados.

3.2. Ciberdelitos económicos

El delito cibernético tiene un amplio panorama de interpretación para explicar las conductas delictivas realizadas en el ciberespacio o aquellas que emplean medios tecnológicos que generan repercusiones en el mundo real. En seguida, es importante mencionar que en la actualidad no existe una doctrina uniforme y menos mayoritaria que defina el ciberdelito con

precisión y sea aceptada de manera universal (PHILLIPS ET AL., 2022). No obstante, esta terminología abarca los delitos tradicionales que incrementan su nivel de impacto por medio de las TIC, sumado a ello se plasma la división de estos delitos en ciberdependientes que incluye la piratería informática, la denegación de servicios y el *malware*, así como los cibernéticos que incluye el fraude, la piratería digital y el ciberacoso (CHEN ET AL., 2023).

Por consiguiente, en este estudio se internalizó la —teoría general de la tensión— aplicada a los ciberdelitos económicos, esta forma de análisis agrupa una serie de factores mancomunados como la pobreza, el desempleo, la desigualdad de ingresos, entre otros trastornos sociales que en su conjunto originan transformaciones sociales que posibilitan alguna motivaciones cibercriminales para obtener ingresos ilegales (CAETANO ET AL., 2023). A su vez, el abordaje del estudio permite la inclusión de la teoría de la deformación en tanto que se ubica como una de las más destacadas por presentar tres periodos claves. El primero inicia desde el siglo XIX hasta los inicios del siglo XX y se planteaba como premisa medular que los delitos eran considerados como el resultado de patologías propias de la sociedad o de los valores sociales. El segundo tiene su inicio luego de la segunda guerra mundial, debido a que se experimentó una crisis de depresión económica lo que provocó migraciones masivas, eso posibilitó que los sociólogos identifiquen los principales rasgos de cibercriminalidad, encontrando al desempleo y la pobreza. El tercero periodo comienza en los años 50 en donde se evidenció el desarrollo económico, los niveles de vida estables y el sentimiento optimista sobre un futuro prometedor (ILIEVSKI Y BERNIK, 2016).

En ese orden de afirmaciones, debemos indicar que el ciberdelito económico de manera intrínseca presenta características particulares como la naturaleza no territorial, es decir, carece de fronteras cibernéticas, también se aprecia la complejidad y la creciente sofisticación de estos delitos, la evolución constante y cambiante, así como la obtención de ganancias ilícitas (MENON Y TEO). En consecuencia, los aplicativos gota a gota son una clase de ciberdelito económico debido a que integra a la ciberestafa y el ciberblanqueo de capitales, los cuales son conductas criminales que tienen como propósito principal obtener ganancias ilegítimas y dotarlas de legitimidad para ingresarlas al curso regular del sistema económico y financiero. No cabe duda de que, con el tiempo los goteros mejoraron la forma de captar a sus cibervíctimas, trasferir el dinero, utilizar mecanismos ilegítimos para cobrar los préstamos, mantenerse en la clandestinidad, empero surge una interrogante que debemos responder,

¿cómo se forman esta clase de ciberdelincuentes?, para ello elaboraremos un organizador visual que resume un reportaje realizado en el Perú sobre un centro de formación y captación de extorsionadores.

Figura 1

Escuela de préstamos gota a gota en el Perú

Nota. Adaptado de «Escuela de los préstamos gota a gota: centros de capacitación de la extorsión», PANORAMA, 2023.

Al respecto, debemos realizar una explicación pormenorizada sobre el proceso de instrucción que se realiza en la escuela de préstamos gota a gota. Sin duda resulta atractivo conocer la forma en la que operan estos lugares, más aún conociendo que el término escuela siempre se utilizó para una finalidad lícita y en beneficio del crecimiento de una sociedad. Sin embargo, las nuevas formas ciberdelincuenciales propiciaron que los ciberdelincuentes puedan incrementar y sofisticar sus conocimientos sobre la ciberestafa y ciberextorsión en esta clase de préstamos.

En primer orden, la ciberactividad delictiva comienza con la captación de sujetos mediante la trata de personas, quienes adquieren la denominación de goteros, estos tienen que ser preferentemente colombianos o extranjeros y elegir si se dedicarán a realizar los préstamos de forma presencial o por medio de los aplicativos, o en su defecto preferirá integrar el área de cobros extemporáneos. Seguidamente, una vez alojados en el centro de preparación tienen una capacitación de 5 días en donde se les instruye sobre el manejo de los sistemas informáticos, el pago que recibirán de forma mensual y el horario de ingreso y salida. Luego

de cumplir con esas expectativas, se gradúan y adquieren un kit con herramientas básicas como dinero para el capita de los préstamos, una moto para movilizarse, usuario y contraseña a la aplicación gotera y una ruta sobre los posibles clientes.

En segundo orden, antes que los ciberdelincuentes ingresen al campo, reciben una inducción para afinar aspectos relacionados a la forma en que se recluta a los aspirantes a goteros, la formación que reciben una vez que se integren en las filas de la academia y una orientación útil para la realización de cobros mediante el apersonamiento de su personal que adquiere la denominación de máquinas de aniquilación. En tercer orden, ubicamos al entrenamiento en donde se les conmina a realizar el cobro por lo que días previos a la fecha de pago se ponen en contacto con la cibervíctima extorsionándola y amenazándola que compartirá información personal con sus contactos o denigrará su honor y buena reputación con textos y publicaciones maliciosas. Habiendo esclarecido este fenómeno desde una perspectiva esclarecedora, corresponde desarrollar el marco normativo susceptible de aplicación a casos asociados a estos aplicativos.

3.2.1. Ciberestafa

En este espacio, resulta clave definir con claridad cada uno de los términos asociados a la cibercriminalidad, por ello debemos indicar que la ciberestafa es un ciberdelito que se externaliza en el ámbito digital, denominado por la doctrina mayoritaria como —ciberespacio— lo que implica el uso de la TIC para timar y embaucar a las cibervíctimas con el propósito de obtener beneficios económicos subrepticios e ilegítimos. Es así como, la ciberestafa se caracteriza por ser una forma de estafa o fraude, esto es, un delito tradicional, que se lleva a cabo a través de medios electrónicos, como la mensajería de correos electrónicos y de texto, llamadas telefónicas o plataformas virtuales fraudulentas.

A su vez, debemos tener presente que estas conductas delictivas son cada vez más frecuentes debido al crecimiento incontrolable de las transacciones en línea y al aumento de cibernautas en la red. Este tipo de estafas pueden adoptar diversas formas, como el phishing, donde los atacantes envían correos electrónicos falsos haciéndose pasar por entidades legítimas con el fin de obtener información confidencial como contraseñas bancarias; o la venta fraudulenta en línea, donde se engaña a los compradores mediante la oferta de productos inexistentes o defectuosos (LÓPEZ Y SILES, 2017).

En cuanto a la repercusión de este ciberdelito debemos precisar que no solo afecta a individuos particulares, sino también a empresas e instituciones. Para aterrizar esta idea, se consideró oportuno incluir al informe "*Internet Organized Crime Threat Assessment*" el cual destaca que las organizaciones criminales utilizan técnicas avanzadas para llevar a cabo estafas masivas dirigidas a empresas, tales como el fraude del CEO (CEO Fraud), donde suplantan la identidad del director ejecutivo para solicitar transferencias de dinero (EUROPOL 2020).

3.2.1.1. Estafa

En esta parte de estudio debemos indicar que la estafa en los préstamos "gota a gota" es una modalidad de fraude financiero muy común en algunos países latinoamericanos, donde los delincuentes se aprovechan de la vulnerabilidad económica de las personas para ofrecerles préstamos informales con altas tasas de interés y condiciones abusivas. En esta forma de estafa, los prestamistas ilegales suelen operar sin licencia ni regulación por parte de entidades financieras legítimas. Utilizan métodos coercitivos, amenazas e intimidaciones para obligar a los prestatarios a realizar pagos exorbitantes y mantenerlos atrapados en un ciclo perpetuo de endeudamiento.

El término "gota a gota", tal como lo describe PADRÓN (2023) se fundamenta en el método operativo utilizado por individuos inmersos en este tipo de actividades delictivas. Este modus operandi se caracteriza por la entrega progresiva de pequeñas cantidades de dinero a diario o semanalmente, denominadas metafóricamente como "gota a gota". Cada vez que se efectúa un pago, el receptor del préstamo se ve obligado a suscribir un documento que estipula un elevado interés compuesto. Esta práctica, que se desarrolla al margen de la legalidad, ha desencadenado consecuencias sumamente graves en términos sociales y económicos en diversas comunidades.

Los sujetos sin experiencia crediticia que buscan desesperadamente obtener préstamos rápidos y accesibles acuden a estos prestamistas informales sin poseer un conocimiento exhaustivo de las repercusiones financieras inherentes a este tipo de tratos. Además, lamentablemente, se han reportado numerosos casos donde los prestamistas emplean tácticas de violencia física o psicológica como método para cobrar las deudas impagadas, generando un entorno altamente perjudicial y amenazante para quienes se encuentran inmersos en esta situación.

3.2.1.2. Privacidad de la información

En ese orden de postulados, la privacidad de la información se refiere al acceso no autorizado y uso indebido de datos personales y financieros de las víctimas por parte de los prestamistas ilegales. En este tipo de esquema delictivo, los delincuentes obtienen información confidencial como nombres, direcciones, números de teléfono, números de identificación personal e incluso registros bancarios para extorsionar a las personas que solicitan estos préstamos (UNIÓN INTERNACIONAL DE TELECOMUNICACIONES 2017).

Los prestamistas gota a gota son grupos criminales organizados que operan principalmente en América Latina, especialmente en países como España, Colombia, México y Perú. Estos delincuentes ofrecen préstamos informales con altas tasas de interés y condiciones abusivas. Utilizan tácticas intimidatorias y violentas para asegurar el pago o para obtener más dinero, lo cual puede incluir la divulgación de información personal sensible.

Esta vulneración de la privacidad de la información se realiza mediante métodos fraudulentos como el phishing (suplantación de identidad), el malware (software malicioso) o el hacking (acceso no autorizado a sistemas informáticos). Los delincuentes pueden obtener los datos personales y financieros fácilmente a través de mensajes engañosos, correos electrónicos falsificados o sitios web fraudulentos.

3.2.2. Ciberblanqueo

El ciberblanqueo de capitales es un ciberdelito que implica convertir ganancias obtenidas ilegalmente en activos aparentemente legítimos. El uso de la tecnología y el entorno digital ha facilitado esta actividad delictiva, permitiendo a los criminales mover grandes sumas de dinero rápidamente y con mayor opacidad. Según la CONVENCIÓN DE LAS NACIONES UNIDAS CONTRA EL DELITO ORGANIZADO TRANSNACIONAL [UNTOC] (2000), el ciberblanqueo de capitales se define como la secuencia de acciones mediante las cuales los bienes o productos resultantes de actividades criminales buscan obtener una fachada legal. Este proceso engloba una variedad de actividades, como la manipulación de transferencias electrónicas de fondos, la instauración de entidades empresariales ficticias en entornos virtuales, la utilización de criptomonedas y otras modalidades de pagos digitales con el propósito de disfrazar el rastro financiero que podrían dejar estas operaciones.

En sentido similar, la SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP (2023) hace referencia a un procedimiento específico que tiene como objetivo principal la inserción de fondos o activos (ya sean monetarios, bienes tangibles, efectos financieros o ganancias) que derivan de actividades ilícitas previas (llamadas delitos precedentes) dentro del entramado económico y financiero de una nación. El propósito fundamental de este proceso es camuflar o dar una apariencia legal a estos recursos, ocultando su origen ilegal y permitiendo su integración en el sistema económico de manera aparentemente legítima.

3.2.2.1. Legislación sobre lavado de activos

El delito en cuestión es identificado bajo múltiples designaciones, entre las cuales se incluyen el término de "lavado de activos" o "legitimación de ganancias ilícitas". En el marco del Título XIII, específicamente en el Capítulo XIV, se aborda en detalle el artículo 301, el cual desarrolla el precepto objeto de examen. En el contexto jurídico del Estado peruano, esta conducta delictiva se encuentra especificada en los artículos 1, 2 y 3 del Decreto Legislativo 1106. Con la intención de enriquecer el entendimiento sobre el tema, se ha incorporado el siguiente esquema visual como herramienta complementaria.

Tabla 9

Lavado de activos en España y Perú

Ley Orgánica 10/1995	**Decreto Legislativo n.° 1106**
Art. 301. El que adquiera, posea, utilice, convierta, o transmita bienes, sabiendo que éstos tienen su origen en una actividad delictiva, cometida por él o por cualquiera tercera persona, o realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones a eludir las consecuencias legales de sus actos, será castigado con la pena de prisión de seis meses a seis años y multa del tanto al triplo	Artículo 1.- Actos de conversión y transferencia El que convierte o transfiere dinero, bienes, efectos o ganancias cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso, será reprimido con pena privativa de la libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa.

del valor de los bienes. En estos casos, los jueces o tribunales, atendiendo a la gravedad del hecho y a las circunstancias personales del delincuente, podrán imponer también a éste la pena de inhabilitación especial para el ejercicio de su profesión o industria por tiempo de uno a tres años, y acordar la medida de clausura temporal o definitiva del establecimiento o local. Si la clausura fuese temporal, su duración no podrá exceder de cinco años.	Artículo 2º.- Actos de ocultamiento y tenencia El que adquiere, utiliza, guarda, administra, custodia, recibe, oculta o mantiene en su poder dinero, bienes, efectos o ganancias, cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso, será reprimido con pena privativa de la libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa. Artículo 3.- Transporte, traslado, ingreso o salida por territorio nacional de dinero o títulos valores de origen ilícito El que transporta o traslada dentro del territorio nacional dinero o títulos valores cuyo origen ilícito conoce o debía presumir, con la finalidad de evitar la identificación de su origen, su incautación o decomiso; o hace ingresar o salir del país tales bienes con igual finalidad, será reprimido con pena privativa de libertad no menor de ocho ni mayor de quince años y con ciento veinte a trescientos cincuenta días multa.

Nota. Adecuado de “El Boletín Oficial Español y el Decreto Legislativo 1106”.

3.2.2.2. Bien jurídico en el lavado de activos

El marco legal define el bien jurídico al establecer la protección del orden socioeconómico. Es notoria la postura adoptada por el legislador, dada la discrepancia evidente en el mercado entre empresas que operan con activos legítimos y aquellas que no cumplen con este criterio.

Además, el sujeto activo abarca cualquier individuo cuyas acciones se ajusten al tipo penal establecido, mientras que el sujeto pasivo corresponde al Estado y sus intereses en representación de la sociedad.

3.2.2.3. Objeto material

El elemento material considerado en este delito son los bienes o servicios obtenidos de manera ilegítima a través de actividades delictivas en el ámbito cibernético. Al respecto, la (CONVENCIÓN DE VIENA 2000) establece que se entiende por 'bienes' los activos de diversa índole, tanto tangibles como intangibles, incluyendo bienes corporales e incorporales, muebles e inmuebles, así como los documentos o instrumentos legales que certifiquen la propiedad u otros derechos sobre dichos activos.

De igual modo, en el (CONVENCIÓN DE PALERMO 2000) se establece que la conversión o traslado de bienes, con pleno conocimiento de que dichos bienes derivan de una actividad delictiva, con la intención de encubrir o disfrazar el origen ilícito de dichos bienes. La ocultación o disfraz de la auténtica naturaleza, procedencia, ubicación, disposición, movimiento o titularidad de los bienes o del derecho legítimo.

En coherencia con lo expuesto, en el (REGLAMENTO MODELO DE LA CICAD-OEA 1992) se establece que comete un delito penal aquel individuo que convierta, transfiera o transporte bienes, con pleno conocimiento, debería tener conocimiento o actuando con intención de ignorancia, de que esos bienes son producto de un delito de tráfico ilícito u otros delitos graves. Comete un delito penal aquel individuo que adquiera, posea, detente, utilice o administre bienes, con pleno conocimiento, debería tener conocimiento, o actuando con intención de ignorancia, de que esos bienes son producto de un delito de tráfico ilícito u otros delitos graves. Comete un delito penal aquel individuo que oculte, encubra o dificulte la determinación real de la naturaleza, procedencia, ubicación, destino, movimiento o propiedad de bienes, o de derechos asociados a dichos bienes, con pleno conocimiento, debería tener conocimiento, o actuando con intención de ignorancia, de que esos bienes son producto de un delito de tráfico ilícito u otros delitos graves.

En esta línea, en consonancia con los apartados anteriores, la (DIRECTIVA UE 2015) establece que la conversión o traspaso de bienes, con pleno conocimiento de que estos derivan de una actividad o hecho ilícito, o de la participación en dicha actividad, con el propósito de ocultar

su origen ilícito o asistir a individuos involucrados en eludir las consecuencias legales de sus acciones. También se refiere a la ocultación o encubrimiento de la verdadera naturaleza, origen, ubicación, disposición, movimiento o propiedad de bienes o derechos sobre los mismos, con pleno conocimiento de que derivan de una actividad delictiva o de la participación en dicha actividad. Además, aborda la adquisición, posesión o uso de bienes con conocimiento, al momento de recibirlos, de que provienen de una actividad delictiva o de la participación en dicha actividad.

3.2.2.4. Etapas del delito

Se hace referencia a las fases por las cuales el dinero adquirido de manera ilícita transita, adaptándose en este caso al ámbito cibernético. En primer término, se presenta la fase de colocación, identificada como el prelavado, que consiste en la inversión del dinero procedente de actividades criminales. En segundo lugar, se describe la etapa de intercalación, donde se ejecutan diversas operaciones con el propósito de eliminar cualquier rastro de su origen. En tercer lugar, se menciona la etapa de integración, en la que el dinero se introduce al circuito legal del sistema financiero (LP PASIÓN POR EL DERECHO 2021).

Con el propósito de ilustrar el contexto anterior, es pertinente mencionar que la situación descrita se replica en el ámbito cibernético. La fase de colocación implica la inserción del dinero adquirido a través de delitos cibernéticos, como la ciberestafa o el ciberfraude. En el segundo escenario, se utilizan predominantemente transacciones en monedas virtuales con el fin de eludir la vigilancia de las autoridades. La última etapa demanda la conversión del dinero para su inserción en el mercado legal.

3.2.2.5. Anonimato en el ciberespacio

Se trata de la capacidad conferida a los delincuentes cibernéticos, donde la ciberdelincuencia y la criminología derivan del uso de la tecnología, cuyo aumento genera perjuicios en el patrimonio de individuos u organizaciones. Es necesario distinguir dos aspectos: el primero, relacionado con la ocultación durante la perpetración del delito, y el segundo, referente al anonimato del perpetrador del delito cibernético (UNIR 2020).

Siguiendo esta línea, (UNIR 2022b) señala que las particularidades del entorno virtual permiten la transnacionalidad y la ausencia de una autoridad centralizada que pueda identificar a los individuos que actúan como usuarios en una plataforma virtual específica. Es

crucial considerar la observación de (GUTIÉRREZ 2005) acerca de que el cibercrimen opera en la práctica en un espacio virtual y sin fronteras, el mismo espacio que proporciona Internet, la Red de redes.

3.2.2.6. Lavado de activos

Acorde al término propuesto, debemos explicar que se refiere al proceso mediante el cual los fondos obtenidos ilegalmente a través de actividades delictivas, como la extorsión o el narcotráfico, son introducidos en el sistema financiero legal a través de préstamos informales conocidos como "gota a gota". Estos préstamos suelen caracterizarse por altas tasas de interés y términos de pago abusivos. A su vez, implica ocultar la verdadera naturaleza y origen ilícito de los fondos. Los delincuentes utilizan una variedad de métodos para llevar a cabo este proceso, incluyendo la creación de empresas ficticias, el uso de testaferros y el fraccionamiento de las transacciones financieras para evitar levantar sospechas.

Sin duda, existen diversos autores que brindan diferentes apreciaciones sobre el tema, empero BEDOYA ET AL. (2021) trasciende con su conceptualización refiriendo que esta modalidad delictiva ha proliferado en América Latina debido a la falta de regulación y supervisión efectiva por parte de las autoridades financieras. Además, se señala que el lavado de activos en los préstamos gota a gota puede tener graves consecuencias económicas y sociales, ya que contribuye al fortalecimiento del crimen organizado y genera un alto nivel de endeudamiento y vulnerabilidad entre las personas afectadas.

3.2.2.7. Monedas virtuales

En este punto de la investigación podemos indicar que las monedas virtuales se han insertado en el entramado de los préstamos informales "gota a gota" como una táctica para enmascarar las transacciones financieras y eludir la supervisión de las autoridades y organismos reguladores. Estos préstamos informales, conocidos como "*préstamos express*" o "préstamos informales", representan un tipo de actividad delictiva donde individuos o grupos delictivos ofrecen dinero a tasas de interés desorbitadas y, lamentablemente, recurren con frecuencia a métodos coercitivos para asegurar el reembolso de los fondos.

El auge de monedas virtuales como Bitcoin o Ethereum ha captado la atención de los delincuentes debido a su estructura descentralizada y el carácter pseudónimo que presentan. Estas criptomonedas facilitan transacciones sin intermediarios financieros convencionales,

complicando aún más la identificación de los perpetradores y la trazabilidad de los fondos. Un informe especializado enfocado en las amenazas emergentes relacionadas con las criptomonedas resalta cómo estas monedas digitales abren la puerta a actividades criminales como el lavado de dinero y el fraude financiero. Además, se especifica cómo los delincuentes emplean monedas virtuales en esquemas de préstamos ilícitos, entre ellos los préstamos gota a gota (DE BALTHASAR Y HERNANDEZ-CASTRO 2017).

Por otro lado, un estudio llevado a cabo por expertos en cibercriminalidad puso al descubierto que las transacciones realizadas con Bitcoin en España exhibían patrones asociados a actividades ilegales, tales como el tráfico de drogas a pequeña escala y la ocultación de capitales ilícitos. Aunque este análisis se centró en España, es probable que estas prácticas se reproduzcan en otros países donde estos esquemas de préstamos informales tienen presencia (SALAS Y ALFARO 2022).

3.3.Casuística sobre apps gota a gota en el ciberespacio

3.3.1. Caso 1

Ciberdelincuente	Ciberextorsionadores anónimos	
Cibervíctima	Hombre adulto padre de familia (referido por compañera de trabajo)	
App gota a gota	Eastbay[1]	
Monto de préstamo	400 soles que se convirtieron en 40 000 soles	
Fuente	Canal de noticias 24 horas[2]	
Resumen del caso	**Mensaje extorsivo**	**Ciberamenazas**

[1] INFOBABE. (11 de junio de 2023). 35 nuevas aplicaciones para el préstamo 'gota a gota': PNP alerta cuáles son. https://www.infobae.com/peru/2023/06/11/35-nuevas-aplicaciones-para-el-prestamo-gota-a-gota-pnp-alerta-cuales-son/

[2] 24 Horas (12 de mayo de 2023). Hombre es extorsionado luego que su compañera de trabajo pidiera un préstamo por aplicativo. https://www.youtube.com/watch?v=Jj6tqSqgUPc

Un trabajador de una empresa es víctima de extorsión por simplemente encontrarse en la bandeja de contactos del celular de su compañera de trabajo que realizó un préstamo de 400 soles mediante un aplicativo gota a gota.	No se complique y apóyenos a solucionar esto y si le molesta recibir estos mensajes colabore con el titular de la deuda para que pueda cancelar y quite su número de nuestra base de datos ¡La plata se recupera sí o sí parce!	Recibió amenazas de muerte contra su familia, integrada por sus menores hijos, su cónyuge y él. Además, constantemente recibe llamadas extorsivas exigiéndole el pago de una deuda que no le corresponde.

Apreciación del investigador:

Al respecto, debemos informar que la mayoría de *apps* que realizan préstamos informales muestran ventanas emergentes o *pop ups* que en su contenido solicitan de forma obligatoria su aceptación o consentimiento para recabar información sobre el dispositivo en donde se pretende instalar la aplicación, evidenciándose lo que se indicaba en el marco teórico sobre el *malware* en forma de *spyware*. En ese orden, los ciberdelincuentes acceden a los contactos y ante el incumplimiento de pago del portador del dispositivo móvil proceden con las ciberextorsión a los contactos con los que la usuario tenga mayor afinidad, esto se devela por el registro de llamadas con mayor tiempo de duración o mediante las llamadas telefónicas entabladas de forma reiterativa.

Ahora bien, los préstamos se tornan en impagables debido a que los intereses se convierten en cuantiosas cifras inalcanzables, tal y como se apreció en este caso, en tanto que un monto que en un primer momento era manejable, esto fue la cifra de S/ 400 (cuatrocientos con 00/100 soles), semanas después de evidenció un cambio abrupto que ninguna entidad bancaria o financiera perteneciente al sistema económico se atrevería a exigir, por lo que las cibervíctimas con el temor que se enteren sus contactos en donde se encuentran familiares y amigos, proceden a generar otros préstamos para cubrir lo que exigen los cibercriminales a través de la plataforma virtual.

3.3.2. Caso 2

Ciberdelincuente	Ciberextorsionadores anónimos

Cibervíctima	Hombre joven padre de familia	
App gota a gota	Kcartera y Moneda Come[3]	
Monto de préstamo	180 soles que se convirtieron en préstamos indefinidos no solicitados	
Fuente	Canal de noticias 24 horas[4]	
Resumen del caso	**Mensaje extorsivo**	**Ciberamenazas**
Un sujeto que prefiere no indicar su nombre solicitó un préstamo de S/ 180, dicho monto fue cancelado y el mismo día se entera que le habían generado otro préstamo, pero esta vez no lo solicitó, pese a haber cambiado su número de cuenta antes de que hagan los depósitos.	Estamos buscando a esta persona morosa que no paga sus préstamos. Las notificaciones y llamadas no van a parar hasta que el titular del préstamo pague, ya que brindó este número como referido.	Recibió amedrentamiento a cada uno de sus familiares y amistades. Sumado a ello, los ciberdelincuentes reconocen que nunca se solicitó préstamos después del primer pago que canceló. Sin embargo, indican que los préstamos se depositan de forma automática.

Apreciación del investigador:

En este caso, se observa la misma forma y modo que en el caso anterior. Aunque, debemos centrar nuestra atención en la generación de préstamos en automático, resulta que al descargar la aplicación y aceptar los términos y condiciones ilegales a todas luces, también exigen que se brinde una serie de datos personales, entre los más relevantes encontramos los nombres y apellidos completos, el número de identificación DNI y un número de cuenta al que

[3] INFOBABE. (11 de junio de 2023). 35 nuevas aplicaciones para el préstamo 'gota a gota': PNP alerta cuáles son. https://www.infobae.com/peru/2023/06/11/35-nuevas-aplicaciones-para-el-prestamo-gota-a-gota-pnp-alerta-cuales-son/

[4] 24 Horas (25 de mayo de 2023). Hombre denuncia que pidió préstamo por aplicativo y siguen depositándole sin su autorización. https://www.youtube.com/watch?v=KM8vrGvDXUU&t=12s

se enviará el monto solicitado. El detalle radica en que en ningún momento se especifica que luego del pago en automático se continuarán abonando montos económicos con cifras cada vez mayores.

Aparentemente, la solución sería reportar la tarjeta y cancelarla, también cambiar de dispositivo inteligente y el número asignado, empero al haber accedido a la lista de contactos empiezan a indagar hasta ubicar en redes de fuente pública o privada los nuevos datos personales, originándose un círculo vicioso aparentemente interminable, debido a que todo concluye con la muerte del deudor. En ese orden, la mejor manera de evitar esta clase de situaciones es evitar a toda costa descargar las apps ni por necesidad o curiosidad.

3.3.3. Caso 3

Ciberdelincuente	Ciberextorsionadores anónimos	
Cibervíctima	Mujer joven madre de familia	
App gota a gota	Viva Crédito[5]	
Monto de préstamo	5000 soles que se convirtieron en préstamos indefinidos no solicitados	
Fuente	Canal de América Noticias – Domingo al día[6]	
Resumen del caso	**Mensaje extorsivo**	**Ciberamenazas**
Una mujer necesitada de efectivo sin experiencia crediticia recurre a la app solicitando dinero, para ello le habían indicado que las	Haga llegar la plata que la cobranza se le tiene que hacer a usted, no a sus amigos ni a sus familiares. Por favor, colabore, que la	Recibió mensajes y llamadas de hostigamiento durante todo el día, supuestamente las realizaba un asesor de cobranzas, pero como se

[5] INFOBABE. (11 de junio de 2023). 35 nuevas aplicaciones para el préstamo 'gota a gota': PNP alerta cuáles son. https://www.infobae.com/peru/2023/06/11/35-nuevas-aplicaciones-para-el-prestamo-gota-a-gota-pnp-alerta-cuales-son/

[6] AMÉRICA NOTICIAS (18 de abril de 2023). Nueva modalidad del cobro gota a gota por aplicativos | Domingo al Día | Perú. https://www.youtube.com/watch?v=CpBQIme73ss

cuotas eran bajísimas y se pagaban en 91 días. Al descargar la aplicación solo le ofrecieron S/ 275, que debían devolverse en 7 días, pero un total de S/ 600, dicho monto nunca fue aceptado por la usuario, pese a ello se lo transfirieron a su cuenta bancaria y se convirtió en una suma impagable.	plata que se le presta es para que la devuelva. Deposita o en caso contrario accederemos a tus contactos y le diremos que eres una estafadora.	conoce fue un cibercriminal. Lo peculiar de este caso es que las amenazas no solo provenían de varones colombiano o venezolanos, sino que también están involucradas mujeres de estos países que no superaban los 28 años, quienes conformaban el brazo logístico de la ciberorganización.

Apreciación del investigador:

Sobre el particular, debemos indicar que los pagos siguen una lógica atípica en perjuicio de los usuarios debido a que se realiza el desembolso de un préstamo mínimo de S/ 275 para pagarse en un máximo de 7 días por un total de S/ 600, es decir más del 150 %. Aunado a ello, si alguno de los usuarios se retrasa en el pago diario, se empieza nuevamente como si nunca se hubiese efectuado pago alguno, lo que resulta irracional y desproporcional.

Este escenario nos permite identificar lo que adelantábamos en el marco teórico, esto es la posición que asumen los ciberdelincuentes, por un lado tenemos al prestamista y por el otro al cobrador, mientras que el primero desembolsa el dinero, hace seguimiento de los pagos diarios, advierte situaciones de impago; el segundo comienza su participación ante el impago, es en ese momento en donde empiezan las muestras de ciberextorsión, terminando en la mayoría de situaciones en la muerte del deudor o lesiones severas a los integrantes de su familia.

3.3.4. Caso 4

Ciberdelincuente	Ciberextorsionadores anónimos

Cibervíctima	Comerciantes informales que no acceden a crédito bancarios	
App gota a gota	Rapi Pago, Vs Card, Hicrédito, Ekeko, Misoles, Icori, Más sol, Mi riqueza y Novo Crédito[7]	
Monto de préstamo	5000 soles que se convirtieron en préstamos indefinidos no solicitados	
Fuente	Canal de Latina Noticias[8]	
Resumen del caso	**Mensaje extorsivo**	**Ciberamenazas**
Un grupo de diferentes comerciantes solicitaron diversos montos dinerarios mediante las apps de préstamos informales que aparecen en el encabezado, debido a las ventas bajas no lograron mantener una continuidad en el pago y regresaron a cifra cero, incrementándose el monto en más del 100 % del capital. Los efectivos policiales encontraron su centro de concentración en donde se apreciaron motos, dinero en	Ya que no quieres pagar, iremos a tu casa ahora mismo a meter una sarta de plomo, la plata no se regala, así que ve la manera de hacer tu pago de las 2. Si valoras tu vida te recomiendo que realices tus pagos ahora mismo, recuerda que tenemos todos tus datos y dar contigo nos tomará 5 minutos, espero tu pago, está corriendo el tiempo.	Recibió llamas extorsivas con amenazas de atentar contra el negocio que manejan, así como contra las personas que se encuentran en dicho lugar. Asimismo, le indicaban que contaban con toda la información de sus contactos y que procederían a difundirlo ante la falta de pago.

[7] INFOBABE. (11 de junio de 2023). 35 nuevas aplicaciones para el préstamo 'gota a gota': PNP alerta cuáles son. https://www.infobae.com/peru/2023/06/11/35-nuevas-aplicaciones-para-el-prestamo-gota-a-gota-pnp-alerta-cuales-son/

[8] LATINA NOTICIAS (17 de abril de 2023). Cuidado con los aplicativos que ofrecen dinero rápido, se trataría de préstamos del 'gota a gota'. https://www.youtube.com/watch?v=SUKBfyttlMY

grandes cantidades en el distrito de San Juan de Lurigancho.		

Apreciación del investigador:

En este caso se apreció movimientos diarios de 50 000 soles recaudados solo en intereses por cobranzas usureras e ilegítimas, eso significa que haciendo un promedio mensual obtienen 1 500 000 soles solo en una aplicación de préstamos. Ahora bien, este supuesto permite saber lo que sucede con el dinero obtenido ilegítimamente, en ese aspecto se conoce que termina blanqueado mediante múltiples trasferencias a diferentes cuentas colombianas de Droops o Mulas que reciben el dinero para despistar la persecución de la autoridad competente.

Una de las peculiaridades que trae esta casuística radica en que el pago para la devolución del dinero e interés no necesariamente se realiza a un número de cuenta, sino que aprovechando el apogeo de los monederos virtuales, tales como el yape o plin, se envían el código QR o en su defecto se remite un número telefónico para formalizar el pago, debe quedar claro que el receptor del yapeo o plineo no necesariamente es el ciberdelincuente, debido a que en estos casos se utilizan interpósita personas.

3.3.5. Caso 5

Ciberdelincuente	Ciberdelincuentes anónimos
Cibervíctima	Hombre joven con familia
App gota a gota	Alpacash[9]
Monto de préstamo	50, 70 y 100 soles que se convirtieron en préstamos indefinidos no solicitados

[9] INFOBABE. (11 de junio de 2023). 35 nuevas aplicaciones para el préstamo 'gota a gota': PNP alerta cuáles son. https://www.infobae.com/peru/2023/06/11/35-nuevas-aplicaciones-para-el-prestamo-gota-a-gota-pnp-alerta-cuales-son/

Fuente	Canal de Latina Noticias[10]	
Resumen del caso	**Mensaje extorsivo**	**Ciberamenazas**
Un joven que tenía muchas deudas que cancelar, pero nada de dinero para hacerlo recurre a estas aplicaciones con el ánimo de superar esta valla económica, al descargar la aplicación omitió leer con detenimiento los términos y condiciones, de esta forma permitió el ingreso de los cibercriminales mediante préstamos que en apariencia eran de 100 soles, pero terminaban siendo de 60 soles, es decir, con un descuento de 40 soles por costos administrativos. En este caso no solo se usó la lista de contactos, sino que también se sumó la galería de fotos, vídeos y audios, los cuales fueron enviados a sus contactos para denigrar la	Se le notifica que a partir del día lunes inicia la cobranza domiciliaria ya que su adeudo hasta el día de hoy sobrepasa los 1925 soles. Debido a tu notable negativa de pago. Vamos a visitar tu domicilio a cobrar con cosas materiales la deuda que te niegas a pagar, evita un susto a tu familia. No será nada agradable nuestra visita. Te lo repetimos una vez más, tienes 10 minutos para reflejar tu pago o atente a las consecuencias.	Recibió llamas extorsivas con amenazas de atentar contra el negocio que manejan, así como contra las personas que se encuentran en dicho lugar. Asimismo, le indicaban que contaban con toda la información de sus contactos y que procederían a difundirlo ante la falta de pago.

[10] LATINA NOTICIAS (19 de febrero de 2023). Delincuentes usan app de préstamos al instante para extorsionar y robar información. https://www.youtube.com/watch?v=f2DDv83mloQ

imagen y el honor de los deudores.		

Apreciación del investigador:

A diferencia de los casos anteriores, en este supuesto se registraron más de 350 denuncias en solo un mes, también permite vislumbrar que los ciberdelincuentes no solo tienen acceso a la lista de contactos, sino que albergan las imágenes fotográficas personales y los vídeos íntimos que estén registrados en el dispositivo, esto dejar abierta la posibilidad para cometer otros ciberdelitos, como por ejemplo el deepfake.

Del mismo modo, se observa que no contentos con las descomunales cifras que reciben diariamente solo por intereses, también han creado una modalidad abusiva e ilegítima, esto es el cobro por cargos y gastos administrativos. Se conoce que ninguna de estas "empresas" cuenta con formalidad societaria en tanto que la actividad económica que realizan no se ajustan a los intereses que exige la autoridad competente para su reconocimiento en el mercado, tributaria porque no habría forma de justificar las rentas obtenidas de forma ilegítima, municipal porque ningún ayuntamiento concedería licencias de funcionamiento conociendo la actividad ilícita que realiza, a menos que lo hagan mediante fachadas utilizando otros negocios e intelectual porque no cabe duda que las marcas no cuentan con registros fidedignos ante la entidad competente.

3.4.ASPECTOS RELEVANTES PARA NUEVOS ESCENARIOS CIBERCRIMINALES

3.4.1. Características particulares de los aplicativos gota a gota

En el mundo actual, la tecnología ha revolucionado muchos aspectos de nuestras vidas, incluido el sector financiero. Los avances en la tecnología han dado lugar al surgimiento de nuevos modelos de préstamos y servicios financieros, como los aplicativos "gota a gota". Estas aplicaciones prometen préstamos insuperables en el mercado sin necesidad de ningún aval, tasas de interés aparentemente muy bajas y sin requerir ninguna evaluación crediticia. Sin embargo, es importante destacar que estas características particulares pueden ocultar riesgos significativos para los consumidores, tal y como se observó en la casuística, entre los más importantes encontramos.

1. Préstamos insuperables: Una de las características más llamativas de estos aplicativos es su capacidad para ofrecer préstamos rápidos y accesibles a personas que no calificarían para un préstamo tradicional en una institución financiera convencional. Esto se debe principalmente a la falta de evaluación crediticia rigurosa y requisitos mínimos para acceder a estos préstamos.

2. Ausencia de aval: A diferencia de los préstamos tradicionales que requieren garantías o avales, los aplicativos "gota a gota" permiten obtener fondos sin tener que presentar ningún tipo de aval. Esto amplía el acceso al crédito para aquellos que no tienen propiedades o activos para ofrecer como garantía.

3. Tasas de interés aparentemente bajas: Estos aplicativos suelen publicitar tasas de interés relativamente bajas en comparación con otras opciones disponibles en el mercado. Sin embargo, es importante señalar que estas tasas pueden estar sujetas a cambios y no siempre reflejan el costo real del préstamo. Además, es necesario considerar las condiciones adicionales asociadas con estos préstamos, como comisiones y cargos ocultos.

4. Evaluación crediticia limitada: A diferencia de los préstamos tradicionales donde se realiza un análisis exhaustivo de la capacidad crediticia del solicitante, los aplicativos "gota a gota" suelen requerir una evaluación crediticia mínima o nula. Esto implica que personas con historiales de crédito negativos o insuficientes también pueden acceder a estos préstamos, lo cual puede aumentar el riesgo tanto para los prestatarios como para los prestamistas.

Aunque estas características particulares pueden parecer beneficiosas para aquellos que necesitan acceso rápido a fondos, existen riesgos significativos asociados con los aplicativos "gota a gota". Algunos de estos riesgos incluyen tasas de interés ocultas, debido a que a menudo, las tasas de interés anunciadas en estos aplicativos no reflejan el costo total del préstamo. Pueden existir comisiones y cargos adicionales que incrementan significativamente el costo final para el prestatario.

En esa línea, se aprecian prácticas predatorias porque en algunos casos, los prestamistas que operan a través de estos aplicativos utilizan tácticas coercitivas y abusivas para garantizar el pago puntual de los préstamos. Esto puede incluir amenazas e intimidaciones hacia los prestatarios, generando un ambiente propicio para la explotación financiera. Cabe reseñar que, existe el ciclo perpetuo de endeudamiento, debido a la facilidad de acceso a estos

préstamos y la falta de evaluación crediticia rigurosa, los prestatarios pueden caer en un ciclo perpetuo de endeudamiento. Esto puede llevar a una situación financiera insostenible y dificultar el cumplimiento de las obligaciones financieras.

3.4.2. Informalidad del Perú como atractivo de conductas ciberdelictivas

La creciente adopción de la tecnología y el acceso a internet han generado un aumento significativo en los delitos cibernéticos en todo el mundo. El Perú, no es una excepción, y ha experimentado un incremento preocupante en este tipo de actividades ilegales. En particular, los préstamos informales a través de aplicativos móviles como el "gota a gota" se han convertido en un problema emergente en la sociedad peruana. Este apartado pretende analizar la relación entre la informalidad del país y la proliferación de estas conductas ciberdelictivas, centrándose en la falta de control exhaustivo para su permanencia en Play Store y la inexistente cultura digital.

Una de las principales razones que facilitan la proliferación de los préstamos informales a través de aplicativos móviles es la falta de un control exhaustivo por parte de Play Store, la plataforma oficial para descargar aplicaciones en dispositivos Android. Estos aplicativos son desarrollados y publicados rápidamente sin una supervisión minuciosa que garantice su legalidad y seguridad para los usuarios. Asimismo, la ausencia de mecanismos rigurosos para verificar la legitimidad de estas aplicaciones permite que muchas sean creadas con intenciones fraudulentas o ilegales, incluyendo los préstamos gota a gota. Algunas aplicaciones pueden incluso utilizar nombres similares a entidades financieras reconocidas o utilizan estrategias engañosas para persuadir a los usuarios desprevenidos.

De otro lado, un factor que contribuye a la proliferación de los préstamos gota a gota y otros delitos cibernéticos en el Perú es la inexistente cultura digital. Aunque cada vez más personas tienen acceso a internet, existe una falta de educación y conciencia sobre los riesgos asociados con el uso de aplicativos móviles y las transacciones financieras en línea. Muchos peruanos no están familiarizados con conceptos como phishing, malware o estafas en línea, lo que los hace más vulnerables a ser víctimas de estos delitos. La falta de conocimiento y experiencia en materia de seguridad cibernética dificulta la identificación y protección frente a situaciones fraudulentas.

3.4.3. Spyware como medio para la comisión de deepfake

La cibercriminalidad ha experimentado un crecimiento exponencial en los últimos años, y una de las técnicas más utilizadas por los delincuentes cibernéticos es el uso de malware spyware. Este apartado de investigación pretende analizar la utilización del spyware en aplicativos gota a gota para acceder a imágenes y vídeos, que posteriormente pueden ser utilizados para cometer delitos como el deepfake, en ese orden corresponde reafirmar lo que se indicó en el marco teórico, en esencia es un tipo de software malicioso diseñado para recopilar información personal sin el consentimiento del usuario. Esta información puede incluir datos personales, contraseñas, historial de navegación e incluso acceso a la cámara y al micrófono del dispositivo infectado.

En ese orden, los aplicativos gota a gota son plataformas digitales mediante las cuales se ofrecen servicios financieros no regulados, especialmente préstamos informales con altas tasas de interés. Estas aplicaciones suelen ser descargadas e instaladas en dispositivos móviles, lo que proporciona una oportunidad para que los atacantes instalen spyware sin levantar sospechas. Una vez que el spyware se infiltra en un dispositivo a través de un aplicativo gota a gota, puede obtener acceso no autorizado a las imágenes y vídeos almacenados en dicho dispositivo. Esto se logra mediante la activación silenciosa de la cámara y/o el micrófono del dispositivo o mediante la extracción de archivos multimedia directamente del almacenamiento interno.

Antes de precisar, la asociación entre el deepfake con el spyware en los aplicativos gota a gota resulta oportuno indicar que este primer término es una técnica que utiliza inteligencia artificial (IA) para crear y manipular imágenes y vídeos falsos, con el propósito de engañar a las personas haciéndolas creer que son auténticos. Los programas de IA utilizados en el proceso de deepfake requieren una gran cantidad de datos, como imágenes y vídeos reales, para entrenar sus algoritmos y generar resultados convincentes.

La combinación del spyware en aplicativos gota a gota y los programas de IA utilizados para el deepfake plantea varios riesgos significativos, por ejemplo, los atacantes pueden utilizar imágenes y vídeos obtenidos mediante spyware para crear deepfakes que se utilicen en campañas de suplantación de identidad, lo que puede tener graves consecuencias legales y dañar la reputación de las víctimas, lo que nos permite señalar que mediante el Dec. Leg. N.° 1521 se modifica el artículo 9 precisando que: «El que, mediante las tecnologías **digitales**

suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material, moral **o de cualquier otra índole**…». Este cambio es el insumo normativo que habilita la inclusión del deepfake y su eventual sanción penal dentro del sistema de administración de justicia peruano.

Además, es posible el acceso a imágenes íntimas o comprometedoras a través del spyware puede ser utilizado por los atacantes para chantajear a las víctimas, exigiendo dinero u otros favores a cambio de no divulgar dichos contenidos. Un escenario que ocurre comúnmente en Estados Unidos se relaciona con los deepfakes generados con información obtenida mediante spyware pueden ser utilizados para manipular la opinión pública durante eventos políticos importantes, poniendo en peligro la integridad democrática.

3.4.4. Aparición injustificada de cargas y gastos administrativos

En este espacio se abordará la preocupante tendencia observada en los aplicativos de préstamos conocidos como "gota a gota", donde los ciberdelincuentes están utilizando tácticas engañosas para justificar la reducción del monto inicialmente acordado. Específicamente, se centra en casos en los que se indica un monto inicial de 100 soles, pero al recibir el depósito, solo se entregan 60 soles bajo la justificación de gastos y cargas administrativas. Esto es una clara muestra de estafa perpetrada por ciberdelincuentes que operan a través de aplicativos dedicados al préstamo informal. Estos individuos utilizan técnicas de persuasión y manipulación para convencer a las víctimas de aceptar condiciones desfavorables e injustificadas, aunque en todos los casos obligan a los usuarios a aceptar los términos y condiciones.

El engaño y manipulación aparecen al indicar un monto inicial de 100 soles y luego entregar únicamente 60 soles, los ciberdelincuentes están aprovechándose de la necesidad financiera y vulnerabilidad económica de las personas. Mediante este engaño, buscan obtener beneficios económicos sin proporcionar ningún servicio o valor real, teniendo en cuenta que ninguno de ellos cuenta con respaldo financiero o bancarios. Aunado a ello, se puede rescatar una característica común en estos casos, esto es la falta total de transparencia por parte de los ciberdelincuentes. No brindan información detallada sobre qué conceptos específicos representan esos supuestos gastos y cargas administrativas ni cómo han llegado a la deducción de esas cifras.

Con basta convicción se puede aseverar que existe un impacto económico y social, debido a la aparición injustificada de cargas y gastos administrativos en los aplicativos gota a gota tiene un impacto negativo tanto económico como social. En el ámbito económico, las personas se ven doblemente afectadas, por un lado al recibir montos con intereses sumamente altos y de otro lado al recibir una cantidad inferior a la acordada, lo cual puede degenerar en problemas económicos insuperables. En el ámbito social, se advierte un aspecto positivo para que la sociedad peruana tenga los ojos abiertos, debido a que estas prácticas alimentan la desconfianza hacia los servicios financieros informales, empero el lado negativo es que pueden llevar a situaciones de endeudamiento insostenible.

3.4.5. Préstamos con interés inicial bajo y aumento desproporcional

La cibercriminalidad ha evolucionado de manera significativa en las últimas décadas, adaptándose a las nuevas tecnologías y aprovechando las vulnerabilidades de los usuarios en línea. Uno de los métodos utilizados por los delincuentes cibernéticos es el uso de aplicativos gota a gota para llevar a cabo estafas financieras. Estos aplicativos ofrecen préstamos con intereses iniciales bajos como estrategia para atraer a sus potenciales víctimas. Sin embargo, una vez que la persona cae en esta trampa, los montos a pagar aumentan descomunalmente en futuros préstamos, generando consecuencias económicas devastadoras.

Los delincuentes cibernéticos utilizan diversas tácticas para engañar a sus víctimas y hacerles creer que están obteniendo un préstamo confiable y accesible. Una estrategia común es ofrecer intereses iniciales muy bajos o incluso nulos, lo cual resulta altamente atractivo para las personas necesitadas de dinero rápido. Esta promesa inicial genera una falsa sensación de seguridad y confianza en la transacción.

Sin embargo, una vez que la cibervíctima ha aceptado el préstamo inicial con tasas bajas, se encuentra atrapada en una red de pagos desproporcionados y abusivos. Los delincuentes aumentan drásticamente el monto total del préstamo y establecen plazos extremadamente cortos para el pago, generando una presión insostenible. Estas prácticas fraudulentas se aprovechan de la necesidad y desesperación de las personas por obtener dinero rápido y fácil.

Este tipo de estafa es especialmente peligroso debido a que los ciberdelincuentes detrás de los aplicativos gota a gota operan en la clandestinidad y utilizan métodos sofisticados para ocultar su identidad real. Los cibercriminales se valen de tecnologías como redes virtuales

privadas (VPN) y servidores anónimos para dificultar su rastreo e investigación por parte de las autoridades competentes. Esto crea un entorno propicio para la perpetuación del delito sin consecuencias aparentes.

4. Conclusiones

Primera:

En conclusión, los aplicativos gota a gota se usan para encubrir ciberdelitos económicos. Esta aseveración se basa en la carencia de filtros de seguridad en plataformas como Play Store y Apple Store, lo que facilita la difusión de aplicativos maliciosos. Esta falta de control posibilita actividades ilegales como ciberextorsión, ciberestafa y ciberblanqueo, al permitir a los delincuentes crear aplicaciones fraudulentas bajo apariencia legítima. Además, esta situación propicia el uso de técnicas de ingeniería social para involucrar a usuarios en esquemas fraudulentos, manipulando psicológicamente a las cibervíctimas para obtener el pago del capital e interés usurero.

Segunda:

Se concluye que, la creciente práctica de usar aplicativos gota a gota para encubrir ciberextorsión es común entre ciberdelincuentes. Estas apps informales, disfrazadas como herramientas financieras o préstamos rápidos, capturan datos personales al ser descargadas por usuarios. Una vez dentro de los dispositivos, los delincuentes extorsionan usando información obtenida, solicitando dinero a cambio de no difundir contenido comprometedor o dañar la reputación de las víctimas. Esta actividad criminal explota vulnerabilidades tecnológicas como la falta de precaución al descargar estas aplicaciones, sacando provecho de la confianza depositada para beneficios económicos ilícitos.

Tercera:

En conclusión, en el ámbito de la cibercriminalidad, los aplicativos gota a gota se usan para encubrir ciberestafas de diversas maneras en entornos digitales. Estas plataformas ofrecen préstamos informales con términos poco claros y altos intereses, engañando a usuarios vulnerables y generando ganancias ilegítimas. Los estafadores atraen a las víctimas ofreciendo préstamos sin verificación crediticia ni cumplimiento de regulaciones financieras, atrapándolas en una red de altas tasas de interés diarias o semanales, lo que hace las deudas

impagables rápidamente. Usan tácticas coercitivas, amenazando con consecuencias de violencia. Además, estos aplicativos recolectan información personal sensible, susceptible de usarse en otros fraudes o venderse en el mercado negro digital.

Cuarta:

Se concluye que, los ciberdelincuentes usan los aplicativos gota a gota para integrar sus ganancias ilegales en la economía convencional. Esta estrategia se apoya en dos elementos principales: los videojuegos y las casas de apuestas. Los videojuegos facilitan la transformación de ganancias ilegales en activos virtuales, vendibles por dinero real. Por su parte, las casas de apuestas permiten legitimar las ganancias obtenidas, brindando una apariencia legal para transacciones financieras. La unión entre estos aplicativos, videojuegos y casas de apuestas crea un ambiente propicio para encubrir operaciones de ciberblanqueo, complicando la detección y el rastreo de transacciones fraudulentas.

5. Recomendaciones

Primera:

Se recomienda que, tanto los proveedores de aplicaciones como las autoridades competentes refuercen sus medidas de seguridad y supervisión para prevenir estos delitos y proteger a los usuarios de entornos digitales. A su vez, se debe realizar estudios más exhaustivos sobre la regulación y supervisión de estas plataformas para fortalecer la seguridad digital y combatir el cibercrimen. La cibercriminalidad continuará evolucionando, por lo que es crucial estar alerta y mantenerse informado para evitar convertirse en una víctima de este tipo de estafas.

Segunda:

Se sugiere que, que las autoridades y los usuarios estén conscientes de este riesgo y tomen medidas preventivas adecuadas, como descargar solo aplicaciones confiables desde fuentes seguras y ser cautelosos al proporcionar datos personales en línea. Además, es necesario fortalecer la legislación y las políticas relacionadas con la protección digital, así como promover campañas educativas para aumentar la conciencia sobre los riesgos y las medidas de seguridad en el entorno digital. Solo así podremos combatir eficazmente este tipo de delito y proteger a los usuarios de posibles extorsiones cibernéticas.

Tercera:

Se recomienda, otorgarle más importancia a la protección de la información personal y financiera al utilizar estos aplicativos. Se recomienda investigar y seleccionar cuidadosamente los prestamistas o aplicativos confiables que cumplan con todas las regulaciones pertinentes. Además, contar con asesoría financiera profesional puede ayudar a tomar decisiones informadas sobre el uso responsable del crédito en entornos digitales.

Cuarta:

Se sugiere que, debe reforzarse los controles y regulaciones digitales para prevenir y combatir el ciberblanqueo desde una perspectiva académica e investigativa. Las autoridades deben cooperar a nivel nacional e internacional para identificar y perseguir a los delincuentes que usan estos aplicativos con fines encubridores. Es crucial educar sobre los riesgos de los aplicativos gota a gota y otros métodos de lavado de dinero digital, sensibilizando a los usuarios sobre las implicaciones legales y éticas al participar en actividades vinculadas al blanqueo de capitales.

Quinta:

Se sugiere que, las autoridades colaboren con empresas tecnológicas y plataformas digitales para crear herramientas de inteligencia artificial que analicen automáticamente comentarios fijos en busca de indicios de prácticas depredadoras vinculadas a aplicativos gota a gota. Estas herramientas deben identificar patrones repetitivos de amenazas, coacción o altas tasas de interés, así como palabras clave relacionadas con estos préstamos ilegales. Es esencial establecer medidas legales y regulatorias más rigurosas para combatir la proliferación de estos aplicativos y asegurar la protección de los consumidores en entornos digitales. Esto implica implementar políticas claras sobre préstamos en línea, educar financieramente a los usuarios y aplicar sanciones más severas a quienes promuevan o participen en aplicativos gota a gota.

Referencias bibliográficas

Bibliografía básica

«Delito de lavado de activos: etapas, modalidades, agravantes y atenuantes». *LP PASIÓN POR EL DERECHO*. 18 de diciembre de 2021. Disponible en: https://lpderecho.pe/delito-lavado-activos-etapas-modalidades-agravantes-atenuantes/

ARIAS GONZÁLES, J. Técnicas e instrumentos de investigación científica. Lima: Editorial Ciencia y Sociedad, 2021. https://bit.ly/3wpvLHU

ATENCIÓN PRIMARIA. «El rigor en la investigación cualitativa». *Revista Elsevier*. 1999, vol. 24, núm. 5, pp. 295-300. Disponible en: https://www.elsevier.es/es-revista-atencion-primaria-27-articulo-el-rigor-investigacion-cualitativa-13354

BAENA PAZ, G. *Metodología de la investigación*. 3ª. ed. Ciudad de México: Grupo Editorial Patria, 2017. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf

BEDOYA, J., RÍOS, J., Y ARREDONDO, A. «La coerción extorsiva en Medellín, Colombia». R*evista Latinoamericana de Estudios de Seguridad* [en línea]. 2021, núm. 29, pp. 96-107. [consulta: noviembre de 2023]. ISSN 1390-4299. Disponible en: https://revistas.flacsoandes.edu.ec/urvio/issue/download/199/235

BUSTOS RUBIO, MIGUEL. «La reforma de la ciberestafa y la incorporación de los medios de pago digitales en el Código Penal». *IDP. Revista de Internet, Derecho y Política* [en línea]. 2023, núm. 38, pp. 1-11. [consulta: octubre de 2023]. Disponible en: https://doi.org/10.7238/idp.v0i38.413222

CAETANO, L., GALINARI, L., Y REZENDE, M. «Experiencias estresantes, ira, autocontrol y conducta antisocial en la adolescencia: perspectiva de la Teoría General de la Tensión». *Revista De Psicología PUCP* [en línea]. 2023, vol. 41, núm. 2, pp. 717-761. [consulta: noviembre de 2023]. Disponible en: https://doi.org/10.18800/psico.202302.005

CHANDRA, A., Y SNOWE, M., J. «Una taxonomía del cibercrimen: teoría y diseño». *International Journal of Accounting Information Systems* [en línea]. 2020, vol. 38, pp. 1-20 [consulta:

noviembre de 2023]. ISSN 1467-0895. Disponible en: https://doi.org/10.1016/j.accinf.2020.100467

CHÁVEZ MÉNDEZ, G., COVARRUBIAS, K., Y URIBE, A. *Metodología de investigación en ciencias sociales: Aplicaciones prácticas*. Colima: Editorial Pred, 2013. https://bit.ly/3MaMWUf

CHEN, S., HAO, M., DING, F., DONG, J., JIPING, D., SHIZE, Z., QIQUAN, G., Y CHUNDONG, G. «Exploring the global geography of cybercrime and its driving forces». *Humanit Soc Sci Commun* [en línea]. 2023, vol. 10, núm. 71, pp. 1-10 [consulta: noviembre de 2023]. ISSN 2662-9992. Disponible: https://doi.org/10.1057/s41599-023-01560-x

CORREIA, F., MARTINS, A., Y WAIKEL, A. «Financiamiento en línea sin FinTech: evidencia de préstamos informales en línea». *Revista Economics and Business* [en línea]. 2022, vol. 121, pp. 1-18 [consulta: noviembre de 2023]. ISSN 0148-6195. Disponible en: https://doi.org/10.1016/j.jeconbus.2022.106080

DE BALTHASAR, T., Y HERNANDEZ-CASTRO, J. «An Analysis of Bitcoin Laundry Services». *Revista Springer Link* [en línea]. 2017, pp. 297–312. https://doi.org/10.1007/978-3-319-70290-2_18

Directiva 2015/849/UE de la Comisión, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) no 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32015L0849

ESCUDERO SÁNCHEZ, C., Y CORTEZ SUÁREZ, L. *Técnicas y métodos cualitativos para la investigación científica*. Machala: Editorial UTMACH, 2018. http://repositorio.utmachala.edu.ec/bitstream/48000/14207/1/Cap.1-Introducci%C3%B3n%20a%20la%20investigaci%C3%B3n%20cient%C3%ADfica.pdf

GUTIÉRREZ FRANCÉS, M., L. «Reflexiones sobre la ciberdelincuencia hoy (en torno a la Ley Penal en el espacio virtual)». *Revista Electrónica de Derecho de la Universidad de La Rioja*. 2005, núm. 3, pp. 69-92 [consulta: mayo de 2022]. Disponible en: https://doi.org/10.18172/redur.3858

HERNÁNDEZ SAMPIERI, R., FERNÁNDEZ COLLADO, C., Y BAPTISTA LUCIO, M. *Metodología de la Investigación*. Ciudad de México: McGRAW - HILL, 2014. https://bit.ly/39bRJpZ

HERNÁNDEZ-SAMPIERI, R., Y MENDOZA TORRES, C. *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. Ciudad de México: McGRAW - HILL, 2018. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/SampieriLasRutas.pdf

ILIEVSKI, A., Y BERNIK, I. «Social-economic aspects of cybercrime». *Innovative Issues and Approaches in Social Sciences* [en línea]. 2016, vol. 9, núm. 3, pp. 8-22. [consulta: noviembre de 2023]. Disponible en: https://bv.unir.net:2133/10.12959/issn.1855-0541.IIASS-2016-no3-art1

KESHAVARZI, M., Y GHAFFARY, H., R. «Un marco basado en ontologías para la representación del conocimiento de los ataques de extorsión digital». *Computers in Human Behavior* [en línea]. 2023, vol. 139, pp. 1-16. Disponible en: https://doi.org/10.1016/j.chb.2022.107520

LE PHUONG, X., D., VIET-NGU H., SON HONG N., y CLEVO, W. «Redes sociales con recursos organizativos, confianza generalizada y préstamos informales: evidencia del Vietnam rural». *Revista Economic Analysis and Policy* [en línea]. 2023, vol. 77, pp. 388-402 [consulta: noviembre de 2023]. ISSN 0313-5926. Disponible en: https://doi.org/10.1016/j.eap.2022.11.016

MARTÍNEZ HOLGUÍN, P. J. «Inclusión financiera, pero con negación del crédito. Un paso para el "gota a gota"». *Pluriverso* [en línea]. 2018, vol. 9, núm. 51, pp. 51-61. Disponible en: https://publicaciones.unaula.edu.co/index.php/Pluriverso/article/view/462

MATVEEV, V., NYKYTCHENKO, O., E., STEFANOVA, N., KHRYPKO, S., ISHCHUK, A., Y PASKO, K. «El ciberdelito como discurso de interpretaciones: la semántica del silencio del habla versus la motivación psicológica para problemas reales». *International Journal of Computer Science and Network Security* [en línea]. 2021, vol. 21, núm. 8, pp. 203-211 [consulta: noviembre de 2023]. Disponible en: http://rep.knlu.edu.ua/xmlui/handle/787878787/2670

MENON, S., Y TEO, G. «Key Challenges in Tackling Economic and Cyber Crimes». *Journal of Money Laundering Control* [en línea]. 2012, vol. 15, no. 3, pp. 243-256. [consulta:

noviembre de 2023]. ISSN 1368-5201. Disponible en: https://doi.org/10.1108/13685201211238016

MIRÓ LINARES, F. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons, 2012. https://bit.ly/3ubpe3H

MORO, MANUEL CASTILLO. «Repercusión de Internet y las TIC en las Ciencias Jurídicas: la ciberestafa». *Revista Economist & Jurist* [en línea]. 2022, núm. 263, pp. 16-23. [consulta: octubre de 2023]. Disponible en: https://www.icaoviedo.es/res/comun/biblioteca/4302/ARTICULO%20E&J.pdf

PHILLIPS, K., DAVIDSON, J., FARR, R., BURKHARDT, C., CANEPPELE, S., Y AIKEN, M. «Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies». *Forensic Sciences* [en línea]. 2022, vol. 2, núm. 2, pp. 379-398 [consulta: noviembre de 2023]. Disponible: https://doi.org/10.3390/forensicsci2020028

PIMIENTA, J., Y DE LA ORDEN, A *Metodología de la Investigación*. 3ª ed. México: Pearson, 2017. https://bit.ly/2ZZAmVe

QUEVEDO, F. *Metodología y estadística para proyectos y tesis*. FQ, 2022. https://bit.ly/3L7a2tM

REGLAMENTO MODELO DE LA CICAD (OEA) 1992 relativo al control del abuso de drogas, reglamento modelo sobre delitos de lavado relacionados con el tráfico ilícito de drogas, y otros delitos graves. Disponible en: http://www.oas.org/juridico/spanish/mesicic3_blv_reglamento.pdf

SALAS, L., Y ALFARO, M. «Criptomonedas y su efecto en la estabilidad del sistema financiero internacional: Apuntes para Centroamérica». *Relaciones Internacionales* [en línea]. 2022, vol. 95, núm. 1, pp. 33-77. https://doi.org/10.15359/ri.95-1.2

SARKAR, G., Y SHUKLA, S., K. «Análisis del comportamiento del delito cibernético: allanando el camino para estrategias policiales eficaces». *Journal of Economic Criminology* [en línea]. 2023, vol. 2, pp. 1-26 [consulta: noviembre de 2023]. ISSN 2949-7914. Disponible en: https://doi.org/10.1016/j.jeconc.2023.100034

TANTALEÁN ODAR, R. *Tipología de las investigaciones jurídicas*. Lima: Editorial Derecho y Cambio Social, 2016. https://dialnet.unirioja.es/servlet/articulo?codigo=5456267

UNIVERSIDAD INTERNACIONAL DE LA RIOJA. *Ciberdelincuencia: ¿qué es y cuáles son los ciberdelitos más comunes?* UNIR, 2020. https://www.unir.net/derecho/revista/que-es-ciberdelincuencia/

UNIVERSIDAD INTERNACIONAL DE LA RIOJA. *Derecho Penal Informático y de la Ciberdelincuencia*: *Cibercriminología II*. UNIR, 2022b. https://bit.ly/3wmRAYL

VERA VILLAMIZAR, P. *Manual de introducción a la metodología de la investigación en psicología*. Edición del autor, 2021. https://bit.ly/3N0dNma

WADE, M. «Rehenes digitales: aprovechando los ataques de ransomware en el ciberespacio». *Revista Business Horizons* [en línea]. 2021, vol. 64, pp. 787-797 [consulta: noviembre de 2023]. ISSN 0007-6813. Disponible en: https://doi.org/10.1016/j.bushor.2021.07.014

Bibliografía complementaria

¡Exclusivo! Escuela de los préstamos gota a gota: centros de capacitación de la extorsión. PANORAMA, 7 de mayo de 2023. https://www.youtube.com/watch?v=VpX0VodxRYg

«Prevención del Lavado de Activos». *SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP* [SBS]. 10 de noviembre de 2023, 12:23. Disponible en: https://www.sbs.gob.pe/prevencion-de-lavado-activos/Nociones-basicas-del-sistema-contra-LAFT#:~:text=Lavado%20de%20Activos%20(LA)&text=En%20t%C3%A9rminos%20sencillos%2C%20es%20el,de%20darles%20apariencia%20de%20legalidad.

ALVARADO, J., PORTOCARRERO, F., TRIVELLI, C., GONZALES, E., GALARZA, F., Y VENERO, H. *El financiamiento informal en el Perú*. Perú: Lima, 2001. http://repositorio.iep.org.pe/handle/IEP/541

BANCO BILBAO VIZCAYA ARGENTARIA. «Spyware: qué es, qué tipos hay y cómo se puede eliminar». *BBVA*. 11 de noviembre de 2023. https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/spyware-que-es-que-tipos-hay-y-como-se-puede-eliminar.html

BELCIC, I. «¿Qué es el malware y cómo protegerse de los ataques?». *Infobae*. 19 de enero de 2023. Disponible en: https://www.avast.com/es-es/c-malware

CHILLITUPA, R. «35 nuevas aplicaciones para el préstamo 'gota a gota': PNP alerta cuáles son». *Infobae*. 11 de junio de 2023. Disponible en:

https://www.infobae.com/peru/2023/06/11/35-nuevas-aplicaciones-para-el-prestamo-gota-a-gota-pnp-alerta-cuales-son/

DEPARTAMENTO DE JUSTICIA DE WASHINGTON. «StealthGenie mobile device spyware application». *ProQuest*. 6 de octubre de 2014. Disponible en: https://n9.cl/3orfj

DURAN, I. «Qué es un ransomware y por qué representa una amenaza para las empresas». *Infobae*. 30 de setiembre de 2023. 13:09. Disponible en: https://www.infobae.com/tecno/2023/09/30/que-es-un-ransomware-y-por-que-representa-una-amenaza-para-las-empresas/

EUROPEAN CYBERCRIME CENTRE. *Internet Organised Crime Threat Assessment (IOCTA)*. EUROPOL, 2017. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2017

EUROPEAN CYBERCRIME CENTRE. *Internet Organised Crime Threat Assessment (IOCTA)*. EUROPOL, 2020. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020

HISCOX ESPAÑA. «Ciberextorsión: cómo protegerte». *Hiscox España.* 23 de febrero de 2023. Disponible en: https://n9.cl/x7sk3

KASPERSKY. «¿Qué es el spyware? - Definición». *Kaspersky.* 10 de noviembre de 2023b. 14:27. Disponible en: https://latam.kaspersky.com/resource-center/threats/spyware

KASPERSKY. «Más información sobre el malware y cómo proteger todos tus dispositivos». *Kaspersky.* 10 de NOVIEMBRE de 2023a. 11:27. Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

LÓPEZ, G., Y SILES, R. *Ciberseguridad: amenazas y soluciones*. Barcelona: Ediciones ENI. 2016.

MINISTERIO DEL INTERIOR DEL PERÚ. «Mininter lanza campaña para advertir riesgos de préstamos “Gota a Gota” donde se usa la violencia para cobrar el dinero». *Plataforma digital única del Estado Peruano*. 21 de abril de 2023. Disponible en: https://www.gob.pe/institucion/mininter/noticias/747455-mininter-lanza

OBSERVATORIO DE JURISPRUDENCIA PENAL. «Jurisprudencia del artículo 200 del Código Penal. - Extorsión». *LP – Pasión por el Derecho.* 1 de setiembre de 2022. Disponible en: https://lpderecho.pe/articulo-200-del-codigo-penal-extorsion/

OCHOA RODRIGUEZ, J., E. *La policía, cibercrimen y ciberseguridad*. Policía Local de Granada, 2023. https://escuelapolicia.com/wp-content/uploads/2023/02/La-policia-cibercrimen-y-ciberseguridad.pdf

PADRÓN, S. «Gota a gota: qué son y cómo funcionan los préstamos ilegales ofrecidos por grupos criminales». *El País*. 3 octubre 2023, 14:00. Disponible en: https://elpais.com/america-colombia/2023-10-03/gota-a-gota-que-son-y-como-funcionan-los-prestamos-ilegales-ofrecidos-por-grupos-criminales.html

SEGUIN, P. «Spyware: detección, prevención y eliminación». *Avast*. 20 de febrero de 2020. Disponible en: https://www.avast.com/es-es/c-spyware

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES [UIT]. *Guía para la elaboración de una estrategia nacional de ciberseguridad*. UIT, 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf

Legislación citada

Decreto Legislativo 1106/2012, 19 de abril, *Diario Oficial El Peruano*, 20 de abril de 2012, núm. 464381, p. 1. Disponible en: https://busquedas.elperuano.pe/normaslegales/decreto-legislativo-de-lucha-eficaz-contra-el-lavado-activos-decreto-legislativo-n-1106-778570-3/

Decreto Legislativo 1591/2023, 13 de diciembre, *Diario Oficial El Peruano*, 14 de diciembre de 2023, p. 1. Disponible en: https://busquedas.elperuano.pe/dispositivo/NL/2243815-1

Ley 30171, de 10 de marzo, de la Ley de Delitos Informáticos, Diario Oficial el Peruano, 10 de marzo de 2014, núm. 518568. Disponible en: https://www.leyes.congreso.gob.pe/Documentos/Leyes/30171.pdf

Ley orgánica 10/1995, de 23 de noviembre, del código penal. *Boletín Oficial del Estado*, 24 de noviembre de 1995, núm. 281, p. 33987. Disponible en: https://www.boe.es/eli/es/lo/1995/11/23/10/con

Convenios referenciados

Convención de Palermo relativo a la delincuencia organizada transnacional y sus protocolos, adoptado en Palermo en diciembre de 2000. Disponible en: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

Convenio (núm. 185) relativo al Cibercrimen, adoptado en Budapest el 23 de noviembre de 2001. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Convenio relativo a la delincuencia organizada transnacional y sus protocolos, adoptado en Viena en 15 noviembre de 2000. Disponible en: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

Listado de abreviaturas

1. APP: Aplicativo
2. CDD: Ciberdelito económico
3. CDI: Ciberdelito informático
4. CE: Comisión Económica
5. DD: Delito Digital
6. DDI: Delincuencia Digital Informática
7. ED: Entorno Digital
8. ETIC: Encubrimiento Tecnológico para Infracciones Cibernéticas
9. GAG: Gota a Gota (préstamos usurarios)
10. IDT: Instrumento Digital de Tráfico (para actividades delictivas)
11. IEDD: Investigación en Delitos Digitales
12. ITC: Instrumento Tecnológico Criminal
13. OECDD: Organización para la Cooperación y el Desarrollo Económicos

Anexo A. Matriz de categorización

<table>
<tr><td>Título:</td><td colspan="5">«Aplicativos gota a gota como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales».</td></tr>
<tr><td>Problema</td><td>Objetivos</td><td>Supuestos</td><td>Categoría</td><td>Subcategoría</td><td>Indicadores</td></tr>
<tr><td>Problema general</td><td>Objetivo general</td><td>Supuesto general</td><td>Primera categoría</td><td rowspan="4">Ciberextorsión</td><td>Malware</td></tr>
<tr><td rowspan="3">PG: ¿De qué manera los aplicativos gota a gota se utilizan como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales?</td><td rowspan="3">OG: Establecer de qué manera los aplicativos gota a gota se utilizan como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales.</td><td rowspan="3">SG: Los aplicativos gota a gota se utilizan permanentemente como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales, dado que no existen filtros de seguridad sobre el contenido de las aplicaciones y tampoco sobre las</td><td rowspan="3">Aplicativos gota a gota</td><td>Ransomware</td></tr>
<tr><td>Spyware</td></tr>
<tr><td>Software espía</td></tr>
</table>

		plataformas que permiten su registro, entre las principales Play Store y Apple Store, lo que posibilita la comisión de ciberextorsión, ciberestafa y ciberblanqueo.			
Problemas específicos	**Objetivos específicos**	**Supuestos específicos**	**Segunda categoría**		Estafa

PE_1: ¿De qué forma los aplicativos *gota a gota* se utilizan como instrumento de encubrimiento para la comisión de ciberextorsión en entornos digitales?	**OE_1:** Establecer de qué forma los aplicativos *gota a gota* se utilizan como instrumento de encubrimiento para la comisión de ciberextorsión en entornos digitales.	**SE_1:** Los aplicativos gota a gota se utilizan continuamente como instrumento de encubrimiento para la comisión de ciberextorsión en entornos digitales, en tanto que los ciberdelincuentes acceden a la totalidad de los dispositivos móviles de los internautas que descargan y registran sus datos en las aplicaciones informales, los cuales solicitan dinero a cambio de evitar compartir	Ciberdelitos económicos	Ciberestafa	

		imágenes, vídeos o denigrar contra su buena reputación.			Privacidad de la información
PE_2: ¿De qué manera los aplicativos *gota a gota* se utilizan como instrumento de encubrimiento para la comisión de ciberestafa en entornos digitales?	**OE_2:** Describir de qué manera los aplicativos *gota a gota* se utilizan como instrumento de encubrimiento para la comisión de ciberestafa en entornos digitales.	**SE_2:** Los aplicativos *gota a gota* se utilizan reiteradamente como instrumento de encubrimiento para la comisión de ciberestafa en entornos digitales, debido a que al tratarse de préstamos informales se conminan intereses altísimos y con el pasar de los días se convierten en impagables por sus deudores.		Ciberblanqueo	Lavado de activos
					Bien jurídico

PE_3: ¿De qué forma los aplicativos *gota a gota* se utilizan como instrumento de encubrimiento para la comisión de ciberblanqueo en entornos digitales?	**OE_3:** Describir de qué manera los aplicativos *gota a gota* se utilizan como instrumento de encubrimiento para la comisión de ciberblanqueo en entornos digitales.	**SE_3:** Los aplicativos gota a gota se utilizan a menudo como instrumento de encubrimiento para la comisión de ciberblanqueo en entornos digitales, debido a que la ganancia ilícita obtenida por los ciberdelincuentes tiene que ingresar al flujo regular económico y para ello utilizan los videos juegos y las casas de apuesta para lavar las ganancias obtenidas de ciberdelitos previos.			Objeto material Etapas del delito Anonimato Monedas virtuales

Anexo B. Distribución global de IP de delitos cibernéticos

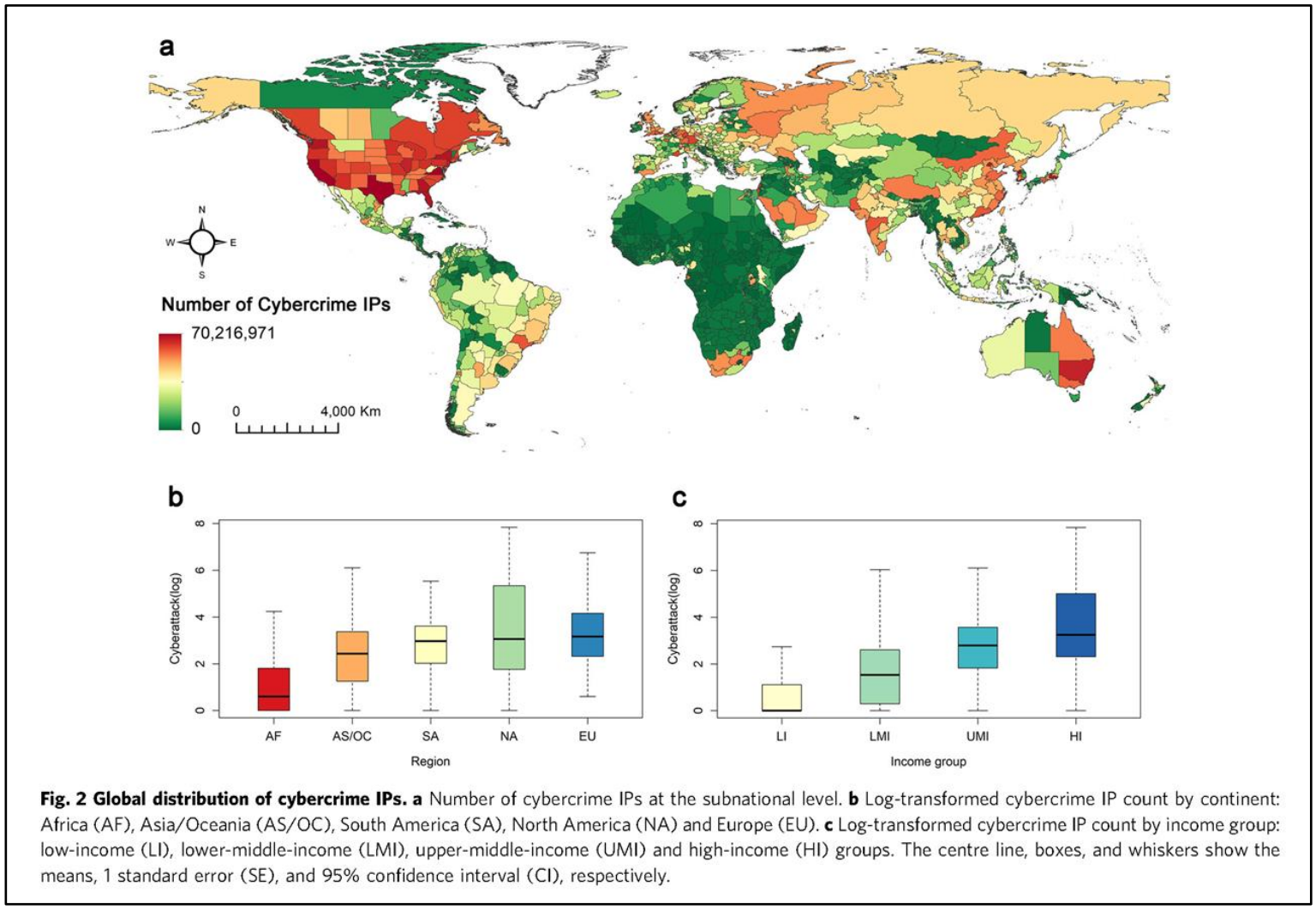

Fig. 2 Global distribution of cybercrime IPs. a Number of cybercrime IPs at the subnational level. **b** Log-transformed cybercrime IP count by continent: Africa (AF), Asia/Oceania (AS/OC), South America (SA), North America (NA) and Europe (EU). **c** Log-transformed cybercrime IP count by income group: low-income (LI), lower-middle-income (LMI), upper-middle-income (UMI) and high-income (HI) groups. The centre line, boxes, and whiskers show the means, 1 standard error (SE), and 95% confidence interval (CI), respectively.