



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América
Facultad de Derecho y Ciencia Política
Escuela Profesional de Derecho

**El artículo 8-A de la ley 30096 frente al fenómeno de
los préstamos extorsivos digitales en el Perú**

TESIS

Para optar el Título Profesional de Abogado

AUTOR

Cristian Guillermo QUIROZ ARAUJO

ASESOR

Dr. Chedorlaomer Rubén GONZALES ESPINOZA

Lima, Perú

2026



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Quiroz, C. (2026). *El artículo 8-A de la ley 30096 frente al fenómeno de los préstamos extorsivos digitales en el Perú*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Derecho y Ciencia Política, Escuela Profesional de Derecho]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Cristian Guillermo Quiroz Araujo
Tipo de documento de identidad	DNI
Número de documento de identidad	75163964
URL de ORCID	https://orcid.org/0009-0004-4003-8270
Datos de asesor	
Nombres y apellidos	Chedorlaomer Rubén Gonzales Espinoza
Tipo de documento de identidad	DNI
Número de documento de identidad	08697908
URL de ORCID	https://orcid.org/0000-0001-6493-1662
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Julio Hernán Figueroa Bustamante
Tipo de documento	DNI
Número de documento de identidad	08248540
Miembro del jurado 1	
Nombres y apellidos	Pedro Enrique Bernui Ore
Tipo de documento	DNI
Número de documento de identidad	06456933
Miembro del jurado 2	
Nombres y apellidos	Jorge Adalberto Pérez López
Tipo de documento	DNI
Número de documento de identidad	08162135
Datos de investigación	

Línea de investigación	Derecho Penal
Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distritos de Lima Metropolitana Latitud: -12.04318 Longitud: -77.02824
Año o rango de años en que se realizó la investigación	2024 - 2026
URL de disciplinas OCDE	Derecho https://purl.org/pe-repo/ocde/ford#5.05.01



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE DERECHO Y CIENCIA POLÍTICA

ACTA DE EXAMEN ORAL PRESENCIAL PARA EL OTORGAMIENTO DEL TÍTULO PROFESIONAL DE ABOGADO CON SUSTENTACIÓN DE TESIS

N° 123

Reunido el Jurado Examinador, constituido por los señores profesores:

- 1.-PRESIDENTE. Mg. JULIO HERNÁN FIGUEROA BUSTAMANTE
- 2.- Mg. PEDRO ENRIQUE BERNUI ORE
- 3.- Mg. JORGE ADALBERTO PÉREZ LÓPEZ
- 4.- Dr. CHEDORLAOMER RUBEN GONZALES ESPINOZA (Asesor)

El bachiller postulante al Título Profesional de Abogado don:

CRISTIAN GUILLERMO QUIROZ ARAUJO

Procedió la sustentación de su tesis titulado:

El artículo 8-A de la ley 30096 frente al fenómeno de los préstamos extorsivos digitales en el Perú

En la redacción del examen escrito de fin de carrera, el graduando fue aprobado con la nota de:

DIECISEIS(16)

Concluida la prueba oral, se practicó la votación correspondiente, resultando el candidato:

Aprobado por unanimidad y menciones honoríficas con la nota de 18 (dieciocho)
Y para constancia se le extiende la presente Acta, en Lima a los VEINTISEIS días del mes de AGOSTO del año 2026

Mg. PEDRO ENRIQUE BERNUI ORE

Presidente del Jurado
Mg. JULIO HERNÁN FIGUEROA BUSTAMANTE

Mg. JORGE ADALBERTO PÉREZ LÓPEZ

Dr. CHEDORLAOMER RUBEN GONZALES ESPINOZA
(Asesor)



UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

CERTIFICADO DE SIMILITUD

Yo, CHEDORLAOMER RUBEN GONZALES ESPINOZA, en mi condición de docente asesor acreditado mediante Dictamen de la Escuela Profesional de Derecho N° 000022-2026-EPD-FDCP/UNMSM de fecha 13 de febrero del 2026, de la Tesis, cuyo título es: El artículo 8-A de la ley 30096 frente al fenómeno de los préstamos extorsivos digitales en el Perú, presentado por el bachiller Cristian Guillermo Quiroz Araujo, para optar el Título Profesional de Abogado.

CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el **5%** de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional**.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para obtención del Título Profesional de Abogado.

Lima, 02 de octubre de 2026

Firma del Asesor:

Nombres y apellidos del asesor: Chedorlaomer Ruben Gonzales Espinoza

08697908

DNI: _____

La vigencia del presente certificado corresponde a un período de noventa (90) días desde la fecha de su emisión; siempre que no haya observaciones en el texto durante el proceso de revisión por el jurado informante o surja alguna contingencia.

Dedicatoria

Dedico el presente trabajo a mis padres, Liliana y Guillermo, por su amor, esfuerzo y apoyo incondicional a lo largo de toda mi vida. Gracias por enseñarme, con su ejemplo, el valor del trabajo, la perseverancia y la honestidad.

A mi hermano, Ricardo, y a mi abuelita, Elva, por su cariño, confianza y por acompañarme siempre, incluso en los momentos más difíciles.

Asimismo, dedico esta tesis a mis amigos y a todas las personas cercanas que, de una u otra manera, fueron parte de este camino. Su apoyo, sus palabras de aliento y su confianza en mí fueron una fuente constante de motivación para no rendirme.

Espero que este logro los haga sentir tan orgullosos de mí como yo me siento agradecido por todo lo que han hecho y continúan haciendo por mí. Mi mayor deseo es poder retribuirles, con mis acciones y mi esfuerzo, una parte de todo lo que me han brindado.

Agradecimientos

Expreso mi más sincero agradecimiento a la Universidad Nacional Mayor de San Marcos, por brindarme la formación académica y los conocimientos que hicieron posible el desarrollo de la presente investigación. A mi asesor, Dr. Chedorlaomer Rubén Gonzales Espinoza, por su orientación, dedicación y valiosos aportes durante la elaboración de esta tesis.

Asimismo, agradezco a mis docentes, quienes contribuyeron a mi formación jurídica y fortalecieron mi vocación por el Derecho, así como a mis compañeros y colegas, por el apoyo y las experiencias compartidas a lo largo de este proceso académico.

Resumen

La presente investigación tiene como objetivo analizar la eficacia del artículo 8-A de la Ley N.º 30096 frente al fenómeno del denominado “gota a gota digital” en el Perú, el cual constituye una modalidad de crédito informal que, mediante el uso de aplicativos móviles, deriva en prácticas extorsivas a través del uso indebido de datos personales.

El estudio adopta un enfoque jurídico-normativo, basado en el análisis doctrinario, legislativo y comparado, considerando experiencias de países como Colombia, México y España; asimismo, se examinan los elementos estructurales del tipo penal previsto en el artículo 8-A, así como su aplicabilidad frente a situaciones en las que la aceptación del préstamo es voluntaria, pero posteriormente se emplean mecanismos de coacción y amenaza para el cobro.

Como resultado, se identifica un vacío normativo, debido a que el tipo penal vigente no contempla adecuadamente los supuestos en los que la extorsión se configura en la etapa posterior a la contratación; en ese sentido, se concluye que no es posible subsumir plenamente el fenómeno del “gota a gota digital” en el marco actual del artículo 8-A, proponiéndose la necesidad de una reformulación normativa que permita una protección efectiva de los bienes jurídicos afectados.

Palabras clave: gota a gota digital, extorsión digital, delitos informáticos, artículo 8-A, crédito informal.

Abstract

This research aims to analyze the effectiveness of Article 8-A of Law No. 30096 in addressing the phenomenon known as “digital loan sharking” (“gota a gota digital”) in Peru, which constitutes an informal lending practice carried out through mobile applications and often results in extortion through the misuse of personal data.

The study adopts a legal-normative approach, based on doctrinal, legislative, and comparative analysis, including experiences from countries such as Colombia, Mexico, and Spain. It examines the structural elements of the criminal offense established in Article 8-A and its applicability to cases where the loan is initially accepted voluntarily, but coercive and threatening practices are later used for debt collection.

The findings reveal a regulatory gap, as the current legal framework does not adequately cover situations where extortion occurs after the contractual agreement. Therefore, it is concluded that the “digital loan sharking” phenomenon cannot be fully subsumed under Article 8-A, highlighting the need for legal reform to ensure effective protection of affected legal interests.

Keywords: digital loan, digital extortion, cybercrime, Article 8-A, informal lending.

Índice

I. Introducción	10
PRIMERA PARTE: ASPECTOS METODOLÓGICOS GENERALES	11
II. PLANTEAMIENTO DEL PROBLEMA	12
2.1. Presentación del Tema y del Problema.....	12
2.2 Formulación del Problema	15
2.2.2. Problemas secundarios	15
III. Hipótesis.....	15
3.1. Hipótesis principal.....	15
3.2. Hipótesis secundarias.....	15
IV. Justificación de la Investigación.....	16
4.1. Justificación Teórica	16
4.2. Justificación normativa	17
4.3. Justificación social.....	17
V. Objetivos del Proyecto de Investigación	18
5.1. Objetivo General	18
5.2. Objetivos Específicos	18
VI. ESTADO DE LA CUESTIÓN	18
6. Antecedentes del Problema.....	18
6.1. Antecedentes nacionales	19
6.2. Antecedentes internacionales	22
VII. METODOLOGÍA	25
7.1. Tipo y diseño de investigación	25
7.2. Métodos de investigación	26
7.3. Técnicas e instrumento(s) de recolección de la información	26
SEGUNDA PARTE: ESTRUCTURA TEÓRICA DE LA TESIS.....	28
CAPITULO I: “ASPECTOS GENERALES”	29
1. Pobreza y exclusión financiera.....	29
2. Dificultades de acceso al crédito en el sistema bancario tradicional	34
3. Digitalización del crédito informal	37
4. El fenómeno “gota a gota”	40
5. Vacíos legales en la legislación penal frente al préstamo informal digital.....	45
CAPITULO II: “DELITOS DIGITALES/CIBERNÉTICOS”	49

1. Conceptualización de los delitos cibernéticos	49
1.1 Bienes jurídicos afectados	54
1.1.1 Información	55
1.1.2 Privacidad	55
1.1.3 Confianza en el entorno digital	56
2. Características de los delitos cibernéticos	57
2.1 Dependencia tecnológica de la víctima	59
2.2 Ejecución a distancia y deslocalización del delito	61
2.3 Anonimato y técnicas de ocultamiento	61
2.4 Transnacionalidad y desafíos jurisdiccionales	62
2.5 Escalabilidad y automatización de los ataques	62
3. La extorsión digital como delito cibernético emergente	63
3.1 Evolución jurídica y tecnológica de la ciberextorsión	64
3.2 Diferencias con la extorsión tradicional	65
3.3 Impacto criminológico y social de la extorsión digital	66
4. Marco normativo nacional aplicable	68
4.1 El artículo 200 del Código Penal y la tipificación de la extorsión	69
4.2 La Ley N° 30096, Ley de Delitos Informáticos	70
4.3 La Ley N° 32183, reconocimiento expreso de la extorsión digital	72
4.4 Vacíos y desafíos del marco normativo	73
5. Marco normativo internacional	75
CAPITULO III: GOTA A GOTA DIGITAL	77
1. Modus operandi del préstamo 'gota a gota' digital	78
1.1. Atracción y reclutamiento de víctimas (publicidad en redes sociales y plataformas móviles)	80
1.2. Extracción de datos sensibles para ejercer presión	81
1.3. Creación de deuda creciente con intereses ocultos y amenazas constantes	82
2. Impacto criminológico y social del 'gota a gota' digital	83
2.1. Impacto individual de la victimización	85
2.2. Impacto colectivo o comunitario	85
3. Necesidad de un tipo penal específico para el 'gota a gota' digital	87
3.1. Insuficiencia de los tipos penales existentes	89
4. Derecho comparado: respuestas legales frente a los préstamos extorsivos digitales	89

4.1 Colombia: alerta de la Superintendencia Financiera sobre el “gota a gota virtual”	91
4.2 México: aplicaciones “montadeudas”	93
4.3. España: regulación y alertas del SERNAC sobre apps financieras con comportamiento extorsivo digital.....	94
CAPITULO IV: PRÉSTAMOS MEDIANTE APLICATIVOS (8-A).....	96
1. La evolución del préstamo informal hacia la digitalización	96
2. Naturaleza jurídica del préstamo mediante aplicativos móviles	100
3. Análisis jurídico del artículo 8-A de la Ley N.º 30096	102
3.1 Elementos del tipo penal: inducción, amenaza, engaño, simulación legal ..	103
4. Extorsión digital como consecuencia del incumplimiento del pago.....	106
TERCERA PARTE: CONTRASTACIÓN DE HIPÓTESIS, TOMA DE POSTURA Y CONSECUENCIAS	107
1. Contrastación de las hipótesis	107
1.1. Análisis e interpretación del problema planteado	108
1.1.1. Hipótesis principal.....	109
1.1.2. Primera hipótesis secundaria.....	110
1.1.3 Segunda hipótesis secundaria	111
2. Presentación de la postura personal	113
3. Propuesta de solución del problema	115
4. Impacto de la implementación de la propuesta	117
5. Consecuencias	119
6. Conclusiones	121
7. Recomendaciones.....	124
REFERENCIAS BIBLIOGRÁFICAS	124

I.Introducción

El avance de la tecnología y la expansión del acceso a internet han transformado profundamente las relaciones económicas y sociales, dando lugar a nuevas formas de interacción, pero también a nuevas modalidades delictivas. Entre ellas destaca el fenómeno del “gota a gota digital”, siendo este una práctica de préstamo informal que se ha trasladado del espacio físico al entorno virtual, utilizando aplicaciones móviles y redes sociales como medios de captación; en ese sentido, este tipo de préstamo se caracteriza por ofrecer dinero de forma rápida y sin requisitos, pero a costa de intereses usurarios y prácticas extorsivas que aprovechan la información personal de las víctimas para realizar el cobro del dinero. De esta manera, la digitalización ha convertido un problema social y financiero tradicional en un delito de naturaleza compleja, donde convergen elementos económicos, tecnológicos y criminológicos.

En el contexto peruano, el Estado ha intentado responder a esta problemática mediante la Ley N.º 32183, que incorporó el artículo 8-A a la Ley N.º 30096 de Delitos Informáticos, tipificando el denominado “préstamo informático extorsivo”; sin embargo, surge la necesidad de analizar si la redacción actual de este artículo permite sancionar efectivamente las conductas que caracterizan al “gota a gota digital” en la realidad social, debido a que en la mayoría de casos, las víctimas no son obligadas desde un inicio a aceptar el préstamo, sino que acceden voluntariamente por necesidad económica, siendo posteriormente objeto de extorsión a través del uso indebido de su información personal.

Por ello, el presente estudio tiene como propósito evaluar la suficiencia del artículo 8-A de la Ley N.º 30096 frente al fenómeno del “gota a gota digital”, identificando los vacíos jurídicos que dificultan su aplicación plena y proponiendo alternativas para su mejora. Desde esa perspectiva, esta investigación adopta un enfoque jurídico-normativo, sustentado en el análisis doctrinario, legislativo y comparado, considerando las experiencias de países como Colombia, México y España, donde también se ha reconocido el impacto penal y social de los préstamos digitales ilegales.

Finalmente, la tesis propone una reflexión crítica sobre la adecuación del marco penal peruano frente a los delitos económicos digitales, partiendo del reconocimiento de que la criminalidad contemporánea evoluciona más rápido que la legislación. De este modo, se busca contribuir al fortalecimiento del derecho penal como herramienta eficaz para la protección de bienes jurídicos fundamentales, proponiendo una respuesta jurídica coherente ante este fenómeno que surge en el espacio digital.

PRIMERA PARTE: ASPECTOS METODOLÓGICOS GENERALES

II. PLANTEAMIENTO DEL PROBLEMA

2.1. Presentación del Tema y del Problema.

En los últimos años, el fenómeno del préstamo informal conocido como “gota a gota” ha experimentado una transformación significativa la cual ha sido impulsada por el desarrollo de tecnologías digitales, esta masificación del uso de teléfonos inteligentes, sumada al fácil acceso a plataformas móviles facilita la aparición de aplicativos de préstamo inmediato, dirigidos principalmente a sectores económicamente vulnerables; como resultado, ha surgido una nueva forma de criminalidad financiera conocida como “gota a gota digital”, caracterizado por el otorgamiento de pequeñas sumas de dinero a través de aplicaciones, con tasas de interés desproporcionadas y mecanismos de cobro extorsivos. Esta nueva modalidad responde al hecho de que muchas personas se encuentran excluidas del sistema bancario tradicional, ya sea por no contar con historial crediticio, empleo formal o ingresos comprobables; en consecuencia, recurren a estas plataformas para afrontar emergencias de salud, alimentación o cubrir gastos básicos, mientras que, por su parte, los aplicativos ofrecen préstamos inmediatos con requisitos mínimos. Sin embargo, esos aplicativos suelen ocultar en su estructura contractual condiciones abusivas e intereses usurarios que terminan perjudicando gravemente al prestatario.

Ahora bien, una vez desembolsado ese dinero, las víctimas suelen enfrentar un sistema de cobro intimidante, debido a que, al instalar la aplicación, los usuarios suelen otorgar permisos que permiten a los prestamistas virtuales acceder a su agenda de contactos, fotografías, documentos de identidad y demás información sensible que se tenga almacenada en el celular, procediendo a realizar una estrategia de presión que incluye amenazas, difamación pública, chantaje emocional y acoso constante ocasionando una grave afectación a la integridad emocional, la vida familiar y la dignidad de las personas agraviadas.

En este contexto, diversos países de América Latina han identificado un preocupante patrón relacionado con el uso de aplicaciones móviles que ofrecen microcréditos rápidos, pero que, en la práctica, funcionan como instrumentos de extorsión digital, de hecho, estas plataformas, conocidas en México como “montadeudas” o “gota a gota virtual”, replican dinámicas similares al fenómeno peruano del “gota a gota digital”, ya que, en todos estos casos, el esquema se

caracteriza por la concesión de un préstamo informal bajo condiciones opacas, seguida por un proceso de hostigamiento tecnológico al deudor, que se activa tras el incumplimiento del pago; por ejemplo, en el caso mexicano, la Revista Jurídica Jalisciense (2023) reportó que se identificaron 679 aplicaciones y sitios web dedicados a esta modalidad, indicando que estas plataformas recurrían a prácticas como la difusión no autorizada de datos personales, amenazas o mensajes intimidatorios, generando un promedio mensual de 972 quejas, principalmente por parte de ciudadanos en la Ciudad de México; de manera similar, en Colombia, la Superintendencia Financiera (2023) alertó que entre enero de 2022 y marzo de 2023 se registraron más de 1 000 denuncias contra plataformas de préstamos informales, señalando que, estas aplicaciones obtenían acceso a la información personal del dispositivo del usuario, la cual era luego utilizada para extorsionar, difamar o amenazar, en lo que la entidad calificó como una evolución digital del tradicional “gota a gota”; asimismo, en Ecuador, la Revista Gestión (2022) documentó el auge del llamado “chulco digital”, una forma de préstamo informal que opera mediante apps móviles, enfatizando que estas aparentes soluciones financieras rápidas encubrían tasas de interés desproporcionadas y prácticas de cobranza coercitivas, generando un nuevo tipo de riesgo digital para los usuarios más vulnerables; por su parte, en Argentina, la firma de ciberseguridad ESET (2023) identificó un incremento en la distribución de aplicaciones maliciosas en Android que se presentaban como servicios de préstamos, señalando que estas apps tenían como objetivo principal acceder a datos sensibles del usuario y utilizarlos para ejercer presión indebida, bajo la apariencia de una relación crediticia legal.

Todos estos casos demuestran que el fenómeno del préstamo informal digital con fines extorsivos no es exclusivo de un país en particular, sino que representa una problemática de alcance regional e incluso global, debido al vacío normativo que existe para su fiscalización efectiva y la sofisticación de sus mecanismos de coacción digital, se exige una revisión urgente de los marcos regulatorios, así como la adecuación de las políticas penales y tecnológicas frente a nuevas formas de criminalidad digital.

En el caso peruano, de acuerdo con la Superintendencia de Banca, Seguros y AFP (SBS), al menos 20 aplicaciones móviles no registradas que ofrecen

préstamos inmediatos con altos intereses y acceso a datos personales han sido identificadas y alertadas como riesgosas para la población, además, muchas de ellas operan sin supervisión legal alguna. Según la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC), se estima que 500 000 peruanos han accedido a este tipo de préstamos “rápidos y fáciles”, y que el negocio ha crecido en un 100 % en los últimos dos años, impidiendo frecuentemente el cumplimiento de los pagos debido al aumento exponencial de la deuda.

Estos datos evidencian que el fenómeno del "gota a gota digital" se traduce en un problema real y cuantificable, ya que, numerosas personas vulnerables recurren a estos préstamos sin regulación financiera y quedan expuestas a métodos coercitivos que comprometen su bienestar y su patrimonio. A pesar de la gravedad de esta práctica, el ordenamiento jurídico penal peruano presenta serias limitaciones para enfrentarla de manera eficaz, si bien el artículo 8-A de la Ley N.º 30096 tipifica como delito informático la extorsión mediante aplicativos, su redacción se enfoca únicamente en aquellos casos en los que la aceptación del contrato de préstamo se produce bajo amenaza, engaño o ardid desde el inicio. Por ende, esta delimitación deja fuera una amplia gama de situaciones reales en las que la aceptación inicial del préstamo es voluntaria, pero los mecanismos de cobranza adoptan formas claramente extorsivas una vez formalizado el acuerdo; dicho de otro modo, esta limitación tipológica genera un preocupante vacío legal, ya que el tipo penal sanciona únicamente la inducción o coacción para contratar, pero no contempla los actos de violencia, amenazas o intimidación que se ejercen en la etapa posterior, ello se traduce en la imposibilidad de calificar como delito la extorsión ejercida durante la cobranza, aun cuando se utilicen métodos coactivos o intimidatorios.

Ante este panorama, resulta indispensable analizar si el fenómeno del “gota a gota digital” puede ser efectivamente subsumido bajo el marco actual del artículo 8-A o si, por el contrario, se requiere una modificación normativa que contemple no solo el carácter usurario del préstamo, sino también los mecanismos extorsivos empleados en su cobro.

En tal sentido, el presente trabajo propone un estudio crítico del artículo 8-A de la Ley N.º 30096, su aplicabilidad frente al fenómeno del “gota a gota digital” y la necesidad de ajustes legislativos que permitan tutelar de forma efectiva e integral

los bienes jurídicos afectados por estas prácticas. Por tanto, este análisis se enfoca en la urgente tarea de adaptar el Derecho Penal a las nuevas dinámicas delictivas que se desarrollan en entornos digitales y que afectan de manera directa a los sectores más vulnerables de la población.

2.2 Formulación del Problema

¿Es posible subsumir el fenómeno denominado “gota a gota” en su modalidad digital en el tipo penal previsto en el artículo 8-A de la Ley N.º 30096 conforme a los principios del sistema penal peruano?

2.2.1. Problemas secundarios

- ❖ ¿Qué características definen al fenómeno denominado “gota a gota” en su modalidad digital como una práctica extorsiva dentro del contexto penal peruano?
- ❖ ¿Cómo se configura la tipicidad del delito previsto en el artículo 8-A de la Ley N.º 30096 a partir de sus elementos estructurales dentro del ordenamiento jurídico peruano?

III. Hipótesis

3.1. Hipótesis principal

No es posible subsumir el fenómeno denominado “gota a gota” en su modalidad digital en el tipo penal previsto en el artículo 8-A de la Ley N.º 30096, toda vez que esta norma sanciona únicamente los préstamos otorgados mediante inducción u obligación con amenaza, intimidación, engaño o ardid para aceptar el contrato, mientras que en el fenómeno “gota a gota” la víctima accede voluntariamente al préstamo, configurándose un problema de atipicidad conforme al principio de legalidad penal.

3.2. Hipótesis secundarias

El fenómeno denominado “gota a gota” en su modalidad digital se caracteriza como una práctica extorsiva porque, si bien el otorgamiento del préstamo es voluntario, los métodos de cobro incluyen amenazas, coacción y hostigamiento digital para obtener el pago, configurando la intimidación propia del delito de extorsión regulado en el artículo 200 del Código Penal.

La tipicidad del delito previsto en el artículo 8-A de la Ley N.º 30096 se configura a partir de la inducción u obligación mediante amenaza, intimidación, engaño o ardid para la aceptación del contrato, excluyendo de su ámbito de aplicación los supuestos en los que la víctima accede voluntariamente al préstamo, aunque posteriormente se ejerzan métodos de cobro extorsivos.

IV. Justificación de la Investigación

4.1. Justificación teórica

La presente investigación se orienta al desarrollo de conceptos teóricos y político-criminales respecto a la punición del “gota a gota” digital, una modalidad delictiva que combina el otorgamiento informal de préstamos mediante aplicaciones móviles con mecanismos de cobranza coactivos y extorsivos. Este hecho, que emerge en el entorno de la criminalidad digital, desborda las categorías típicas del Derecho Penal tradicional como la extorsión, la usura o la estafa, lo que hace imprescindible desarrollar un marco conceptual que permita comprender esta conducta, su estructura y sus implicancias jurídicas en un contexto tecnológico.

Este fenómeno plantea desafíos importantes para los fines preventivos y retributivos del sistema penal, en tanto evidencia la necesidad de revisar críticamente los límites del Derecho Penal; en este marco, la criminalidad digital no solo representa una amenaza individual al patrimonio, sino también una afectación sistemática a la privacidad, la libertad personal y la seguridad económica de sectores vulnerables.

El supuesto de hecho que motiva esta investigación es la creciente proliferación de plataformas digitales que ofrecen microcréditos de forma aparentemente legal, pero que, en realidad, configuran un esquema extorsivo basado en el acceso indebido a datos personales, la intimidación constante y la amenaza de difundir información sensible, lo cual justifica la necesidad de repensar los fundamentos teóricos del Derecho Penal frente a estas nuevas dinámicas delictivas.

4.2. Justificación normativa

Normativamente, la presente investigación es relevante porque evaluará la suficiencia, alcance y adecuación sistemática del artículo 8-A de la Ley N.º 30096, determinando si esta norma cubre las conductas del “gota a gota” digital o si resulta necesaria su modificación, el artículo mencionado anteriormente, sanciona los préstamos informáticos extorsivos cuando la aceptación del contrato es producto de amenaza, intimidación, engaño o ardid; sin embargo, no sanciona los casos en los que la víctima accede voluntariamente al préstamo, pero posteriormente es coaccionada y extorsionada para pagar intereses usurarios o ilegales.

Este vacío normativo genera incertidumbre jurídica y dificulta la labor de los operadores del sistema de justicia penal, quienes se ven limitados para subsumir estas conductas en los tipos vigentes, afectando el principio de protección efectiva de bienes jurídicos como la libertad individual, la seguridad económica y la integridad psíquica de las víctimas; en ese sentido, se busca aportar propuestas normativas de reforma que fortalezcan el sistema penal frente a estas nuevas formas de criminalidad.

Además, la investigación analizará la interpretación de los verbos rectores del artículo 8-A de la Ley N.º 30096, que sanciona a quien “induce u obliga mediante amenaza, intimidación, engaño o ardid” a aceptar el préstamo, este aspecto resulta fundamental en el marco de la teoría del delito, pues permitirá determinar si la acción típica sanciona únicamente el momento precontractual o si debería ampliarse a la etapa de ejecución y cobro cuando la intimidación configura un medio de obtención del monto económico.

4.3. Justificación social

Desde un enfoque social, la presente investigación permitirá visibilizar una problemática que afecta principalmente a personas de bajos recursos, trabajadores informales y microempresarios que, ante la imposibilidad de acceder al sistema financiero formal por las trabas burocráticas y requisitos bancarios, recurren a aplicativos de préstamos digitales para atender emergencias básicas como alimentación, medicinas o deudas urgentes. Estas personas se convierten en víctimas de un sistema de crédito informal digital que no solo cobra intereses usurarios, sino que implementa métodos coactivos y extorsivos, tales como amenazas de daño físico, difusión de fotografías y

llamadas continuas a sus contactos personales y laborales, afectando de esta forma su estabilidad emocional.

En este sentido, la investigación no solo busca un aporte teórico y normativo, sino también generar conciencia y proponer reformas que permitan al Derecho Penal cumplir su finalidad de protección efectiva, asegurando la dignidad y seguridad de las personas frente a delitos que configuran graves vulneraciones de derechos fundamentales.

V. Objetivos del Proyecto de Investigación

5.1. Objetivo General

Determinar si es posible subsumir el fenómeno denominado “gota a gota” en su modalidad digital en el tipo penal previsto en el artículo 8-A de la Ley N.º 30096 conforme a los principios del sistema penal peruano.

5.2. Objetivos Específicos

5.2.1. Desarrollar las características que definen al fenómeno denominado “gota a gota” en su modalidad digital como una práctica extorsiva dentro del contexto penal peruano.

5.2.2. Estudiar la tipicidad del delito previsto en el artículo 8-A de la Ley N.º 30096 a partir de sus elementos estructurales dentro del ordenamiento jurídico peruano.

VI. ESTADO DE LA CUESTIÓN

6. Antecedentes del Problema

Son trabajos de investigación que han abordado la misma situación problemática. Se deben señalar los datos bibliográficos del trabajo, el objetivo o problema general, los instrumentos de recolección de datos utilizados y la conclusión en general, así como los antecedentes y el estado actual de los esfuerzos científicos por la solución del problema planteado en la tesis.

Se debe distinguir entre fuentes nacionales y extranjeras.

6.1. Antecedentes nacionales

6.1.1. TÍTULO: Influencia del delito de extorsión en los préstamos gota a gota, distrito de Villa El Salvador, 2023

AUTOR: Guerrero Alarcón, José Carlos

UNIVERSIDAD: Escuela Universitaria de Posgrado – Universidad Nacional Federico Villarreal

GRADO: Tesis para optar el grado académico de Maestro en Derecho Penal

LUGAR Y AÑO: Lima – Perú, 2024

FUNDAMENTOS:

Esta tesis analiza la manera en que el delito de extorsión influye en los préstamos informales conocidos como “gota a gota” en el distrito de Villa El Salvador durante el año 2023. El autor utiliza un enfoque cuantitativo con diseño no experimental y paradigma positivista, aplicando un método hipotético-deductivo.

Los resultados muestran que una parte significativa de los encuestados reconoce la vinculación directa entre la extorsión y la expansión de estos préstamos, evidenciando que muchas de estas operaciones esconden condiciones abusivas bajo una fachada de accesibilidad financiera. La tesis plantea que estos préstamos, lejos de aliviar la situación económica de los ciudadanos, los exponen a amenazas, coacción y violencia.

LOS APORTES MÁS RELEVANTES QUE ESTA TESIS APORTA A LA INVESTIGACIÓN SON LOS SIGUIENTES:

PRIMERO: El delito de extorsión incide directamente en la proliferación de los préstamos “gota a gota”, afectando la seguridad ciudadana y generando un entorno persistente de temor; asimismo, la violencia vinculada a estos préstamos impide condiciones justas y transparentes para los prestatarios, revelando una clara asimetría en las relaciones económicas informales. **SEGUNDO:** La amenaza, como herramienta de presión, transforma el acuerdo financiero en una dinámica de coacción donde los ciudadanos aceptan condiciones abusivas por miedo a represalias contra ellos o su entorno. **CUARTO:** La obtención de ventajas económicas indebidas a costa de los prestatarios perpetúa ciclos de dependencia, demostrando la necesidad de regulación legal y educación financiera urgente.

FUENTE:

https://repositorio.unfv.edu.pe/bitstream/handle/20.500.13084/9201/UNFV_EUP_G_Guerrero_Alarcon_Jose_Carlos_Maestria_2024.pdf?sequence=3&isAllowed=y

6.1.2. TESIS TÍTULO: *La investigación policial en el delito de extorsión en la Región Policial Callao, período 2013 – 2014*

AUTORA: Nicasio Zapata Suclupe

UNIVERSIDAD: Pontificia Universidad Católica del Perú

GRADO: Tesis para optar el grado de Magíster en Ciencia Política y Gobierno, con mención en Políticas Públicas y Gestión Pública

AÑO: 2016

FUNDAMENTOS:

Este estudio examina las limitaciones operativas, logísticas e institucionales de la Policía Nacional del Perú frente a los delitos de extorsión en la Región Callao. A través de entrevistas a operadores clave, funcionarios y especialistas, se identifican las causas estructurales de la ineficacia policial, como la falta de personal capacitado, equipos, infraestructura adecuada y descoordinación con el Ministerio Público.

La autora analiza fenómenos como la “cifra negra” de extorsiones no denunciadas, que distorsiona las estadísticas oficiales y revela la verdadera magnitud del problema.

LOS APORTES MÁS RELEVANTES QUE ESTA TESIS APORTA A LA INVESTIGACIÓN SON LOS SIGUIENTES:

PRIMERO: El delito de extorsión en el Callao es más grave de lo que reflejan las cifras oficiales, debido a la gran cantidad de casos no denunciados y a su vinculación con redes delictivas desde las cárceles.

SEGUNDO: La política pública de lucha contra la extorsión presenta serias limitaciones estructurales, como la escasez de personal especializado, deficiencia en los recursos logísticos (vehículos, equipos de comunicación, cámaras), e infraestructura inadecuada.

TERCERO: Las fallas en la coordinación entre la Policía y el Ministerio Público generan retrasos significativos en la investigación, lo que favorece la impunidad y desincentiva la denuncia ciudadana.

FUENTE: <http://hdl.handle.net/20.500.12423/4842>

6.1.3. TÍTULO: *Implementación de medidas procedimentales frente al delito de extorsión cometido por bandas criminales en Lima Cercado, durante el periodo 2021 - 2023*

AUTOR: Fidel Martín Cárdenas Castro

UNIVERSIDAD: Pontificia Universidad Católica del Perú

GRADO: Tesis para obtener el grado académico de Maestro en Gobierno y Políticas Públicas

AÑO: 2024

FUNDAMENTOS:

El autor analiza la evolución del delito de extorsión en Lima Cercado, señalando como principales causas la débil respuesta procedimental de los operadores de justicia y la influencia de bandas criminales extranjeras como el “Tren de Aragua”. El estudio propone como solución la modificación del protocolo interinstitucional DS-010-2018-JUS, con el objetivo de acelerar los plazos procesales y fortalecer la investigación penal. Además, se utilizaron entrevistas a policías de la DIRINCRI, fiscales y víctimas, concluyendo que una respuesta rápida y coordinada entre fiscalía y policía puede reducir la capacidad de acción de estas bandas criminales.

LOS APORTES MÁS RELEVANTES QUE ESTA TESIS APORTA A LA INVESTIGACIÓN SON LOS SIGUIENTES:

PRIMERO: La investigación policial se ve obstaculizada por demoras en la remisión de carpetas fiscales, lo que limita la respuesta oportuna ante denuncias de extorsión.

SEGUNDO: La modificación del protocolo interinstitucional permitiría iniciar diligencias en un plazo máximo de 72 horas, mejorando la eficiencia y legalidad en la respuesta penal frente a las organizaciones criminales.

FUENTE: <https://tesis.pucp.edu.pe/server/api/core/bitstreams/1288c4cd-3542-4063-beab-662d7c005d31/content>

6.2. Antecedentes internacionales

6.2.1. TESIS TÍTULO: *Aplicativos gota a gota como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales en el Perú*

AUTOR: Menacho Ortega, Bertho Arturo

UNIVERSIDAD: Universidad Internacional de La Rioja

GRADO: TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE MAGISTER

AÑO: 2022

FUNDAMENTOS:

La investigación examina cómo los aplicativos móviles informales de préstamo tipo “gota a gota” son empleados por ciberdelincuentes como instrumentos de encubrimiento de delitos económicos digitales, como la ciberextorsión, la ciberestafa y el blanqueo de capitales. El autor revela que estas apps utilizan spyware para capturar imágenes, audios y videos del dispositivo de la víctima, que luego son utilizados como medio de presión para cobrar máscaras de deuda. Además, el dinero recaudado es lavado mediante plataformas digitales como videojuegos y casas de apuestas, lo cual dificulta su rastreo.

La metodología fue de corte cualitativo y exploratorio, con estudio de casos y fichas de análisis documental. El enfoque permitió identificar la ausencia de regulación explícita en Perú y España sobre los aplicativos de préstamo de este tipo y cómo esto facilita que estas aplicaciones operen con impunidad bajo apariencia legítima.

LOS APORTES MÁS RELEVANTES QUE ESTA TESIS APORTA A LA INVESTIGACIÓN SON LOS SIGUIENTES:

PRIMERO: 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.

SEGUNDO: 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 comprometedora 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.

FUENTE: <https://renati.sunedu.gob.pe/handle/renati/9235>

6.2.2. TÍTULO: *Impacto financiero causado por los cuentagotas en microempresarios de Villavicencio*

AUTOR: Rodríguez Ladino, José Javier

UNIVERSIDAD: Universidad Nacional de Colombia, sede Manizales

GRADO: Trabajo de grado para optar el título de Magíster

LUGAR Y AÑO: Villavicencio – Colombia, 2015

FUNDAMENTOS:

Esta investigación identifica las causas que impiden a los microempresarios acceder al crédito formal y examina el impacto financiero de recurrir al sistema de préstamo informal conocido como “cuentagotas” o “gota a gota”. Se compara el comportamiento de inversión de los microempresarios que utilizan el crédito formal con aquellos que recurren al informal, y se exploran los principales problemas que enfrentan quienes optan por este último.

Se destaca que muchos recurren a estos préstamos debido a factores como el miedo al embargo, estar reportados en centrales de riesgo, la complejidad de los trámites bancarios y la necesidad urgente de liquidez. También se evidencia que

los altos intereses (20% en promedio) son el mayor problema de quienes acceden a los “cuentagotas”. Pese a esto, muchos los consideran más accesibles y confiables que las entidades bancarias.

LOS APORTES MÁS RELEVANTES QUE ESTA TESIS APORTA A LA INVESTIGACIÓN SON LOS SIGUIENTES:

PRIMERO: El perfil del microempresario que opta por préstamos cuentagotas se caracteriza por bajos niveles de escolaridad, pertenencia a estratos sociales bajos y actividad comercial diaria.

SEGUNDO: El 64% de los encuestados pagó intereses del 20%, pero consideran que los cuentagotas generan menos violencia en Villavicencio que en otras regiones.

TERCERO: Las principales barreras al acceso a la banca formal incluyen el miedo al reporte en centrales de riesgo, trámites burocráticos y falta de cultura financiera.

CUARTO: El 20% de los microempresarios prefiere al cuentagotas por su rapidez, aunque sean conscientes de las condiciones desventajosas. Existe una cultura de préstamo informal que se perpetúa por recomendación entre pares.

QUINTO: Se sugieren políticas públicas que faciliten el acceso a créditos formales de bajo monto, con menos requisitos, más asesoría y mejor difusión de información.

FUENTE:

<https://repositorio.unal.edu.co/bitstream/handle/unal/55146/17330041.2015.pdf?sequence=1&isAllowed=y>

6.2.3. TÍTULO: *Análisis jurídico de la delincuencia organizada en el delito de extorsión en modalidad periódica o repetitiva*

AUTORAS: Camila Maite Abalco Puga – Merlyn Anabella Carrillo Varela

UNIVERSIDAD: Universidad Politécnica Salesiana, sede Quito (Ecuador)

GRADO: Tesis para optar el título de Abogada

AÑO: 2025

FUNDAMENTOS:

Esta investigación se enfoca en el estudio de la delincuencia organizada vinculada al delito de extorsión periódica o repetitiva en el Distrito Metropolitano

de Quito. La tesis examina el fenómeno de las llamadas “vacunas”, una modalidad de extorsión sistemática realizada por grupos delictivos organizados (GDO) que se ha intensificado entre 2023 y 2024.

El trabajo combina análisis jurídico y estadístico, así como una evaluación crítica de la reciente reforma al artículo 185 del COIP, que incorporó nuevas figuras penales para abordar este tipo de extorsión. Asimismo, se propone el fortalecimiento del enfoque interinstitucional y la implementación de políticas públicas para enfrentar las causas estructurales del problema.

LOS APORTES MÁS RELEVANTES QUE ESTA TESIS APORTA A LA INVESTIGACIÓN SON LOS SIGUIENTES:

PRIMERO: La tipificación del delito de extorsión periódica o repetitiva es resultado de una respuesta legal a la evolución de la criminalidad organizada, pero aún presenta vacíos normativos y riesgos de aplicación desigual.

SEGUNDO: El análisis estadístico evidencia un crecimiento del 25% anual en delitos de extorsión vinculados a organizaciones criminales, lo que refleja una amenaza estructural al sistema judicial.

TERCERO: Es imprescindible una armonización normativa, ya que actualmente el mismo hecho delictivo puede ser sancionado por dos normas distintas, lo cual vulnera el principio de legalidad y puede afectar la certeza jurídica.

FUENTE: <https://renati.sunedu.gob.pe/handle/renati/9235>

VII. METODOLOGÍA

7.1. Tipo y diseño de investigación

El presente trabajo adopta un enfoque de investigación jurídica-normativa no exegética, lo que implica un análisis que va más allá de la mera interpretación literal de las normas legales; en ese sentido, en lugar de centrarse únicamente en el texto de la ley, se considera su finalidad, contexto de aplicación, coherencia interna y efectos en la realidad social, por consiguiente, se analizará el contenido del artículo 8-A de la Ley N.º 30096 y su aplicabilidad frente al fenómeno de los préstamos “gota a gota” digitales, atendiendo a los principios del Derecho Penal, así como a elementos doctrinarios y jurisprudenciales relevantes, tanto nacionales como comparados.

El diseño de investigación es no experimental, debido a que no se manipulan variables ni se interviene directamente sobre una población o muestra, en cambio, se basa en la observación y análisis de documentos legales y académicos dentro de su entorno natural, permitiendo describir, comprender y reflexionar sobre los vacíos normativos detectados, sin intervenir activamente en el fenómeno objeto de estudio.

7.2. Métodos de investigación

Se empleará el método inductivo-deductivo, que combina el razonamiento a partir de casos particulares y la aplicación de principios generales a situaciones específicas. El estudio comenzará con la observación y recopilación de datos relacionados con denuncias, noticias, jurisprudencia y prácticas delictivas vinculadas al préstamo “gota a gota” digital. A partir de ello, se procederá a la identificación de patrones y elementos comunes que permitan construir una interpretación general sobre la problemática.

Luego, desde un enfoque deductivo, se aplicarán los principios y categorías del Derecho Penal, especialmente aquellos relacionados con los delitos informáticos y los bienes jurídicos protegidos, para evaluar la pertinencia y suficiencia del artículo 8-A en la tipificación de estas conductas. Finalmente, se formularán conclusiones generales, sustentadas en el análisis normativo y la evidencia empírica revisada, proponiendo ajustes normativos si resultan necesarios.

7.3. Técnicas e instrumento(s) de recolección de la información

Se utilizará la técnica del análisis documental, que consiste en el examen sistemático de documentos jurídicos y académicos, con el fin de identificar categorías relevantes, vacíos normativos, patrones de interpretación y propuestas doctrinarias. Esta técnica permitirá abordar de forma integral el objeto de estudio, combinando fuentes como:

- 7.3.1. Legislación nacional y comparada.
- 7.3.2. Jurisprudencia nacional relevante.
- 7.3.3. Artículos doctrinarios y tesis jurídicas.
- 7.3.4. Informes institucionales o especializados.

El instrumento principal será la ficha de análisis documental, diseñada con categorías predeterminadas que facilitarán la extracción y organización de la información relevante para el estudio.

SEGUNDA PARTE: ESTRUCTURA TEÓRICA DE LA TESIS

CAPITULO I: “ASPECTOS GENERALES”

1. Pobreza y exclusión financiera

La pobreza constituye uno de los fenómenos sociales más persistentes y complejos en la historia de la humanidad, no se trata únicamente de la carencia de ingresos monetarios suficientes para satisfacer las necesidades básicas, sino de una condición multidimensional que implica limitaciones en el acceso a bienes, servicios, oportunidades y derechos fundamentales. De acuerdo con el Banco Mundial (2020), la pobreza debe entenderse como una situación en la que las personas no pueden alcanzar un nivel de vida mínimo, lo que abarca tanto la insuficiencia de recursos económicos como la privación de derechos esenciales como la educación, la salud, el agua potable, la vivienda digna y la seguridad social.

Ahora bien, la pobreza se configura como un problema estructural en la sociedad, pues no se origina únicamente en decisiones individuales, sino en la forma en que se organizan los sistemas económicos, políticos y sociales; de esta forma, factores como la desigualdad histórica, las crisis económicas recurrentes, la exclusión en el acceso a educación de calidad y la debilidad institucional de los Estados contribuyen a reproducir y profundizar estas brechas; como advierte Kliksberg (2000), la pobreza no debe verse como un simple problema de ingresos, sino como una privación múltiple de derechos, siendo este enfoque fundamental para entender que no basta con aumentar los ingresos, sino con generar condiciones que permitan un desarrollo humano real.

En ese sentido, las consecuencias de la pobreza en la sociedad se entienden como múltiples y se reflejan tanto en el ámbito individual como en el colectivo, en el plano personal, estas acarrear problemas de malnutrición, deficiencias educativas, precariedad laboral y vulnerabilidad frente a enfermedades, lo que a su vez perpetúa el círculo de la desigualdad intergeneracional; mientras que, en el plano social, la pobreza genera exclusión, fragmentación y debilitamiento del tejido comunitario, además de propiciar fenómenos como la migración forzada, la informalidad económica y, en algunos contextos, el incremento de la criminalidad. El Programa de las Naciones Unidas para el Desarrollo (PNUD, 2021) señala que las sociedades con altos niveles de pobreza tienden a

presentar también mayores índices de inestabilidad política y social, lo que evidencia que este fenómeno no solo afecta a quienes lo padecen directamente, sino que repercute en el bienestar colectivo y en la cohesión social.

Por otro lado, la comprensión de la pobreza requiere distinguir sus tipos o dimensiones, esto debido a que, tradicionalmente se ha hablado de la pobreza absoluta, la cual se define como la incapacidad de cubrir las necesidades básicas de alimentación, vivienda, salud y educación; y de la pobreza relativa, que hace referencia a la posición de un individuo o grupo en comparación con el nivel de vida promedio de una sociedad determinada; sin embargo, enfoques más recientes como el Índice de Pobreza Multidimensional (IPM) desarrollado por el PNUD y la Iniciativa de Oxford sobre Pobreza y Desarrollo Humano (2010) destacan que la pobreza debe analizarse a partir de múltiples factores, incluyendo el acceso a servicios básicos, la seguridad social, la calidad del trabajo y la protección frente a la vulnerabilidad, en la práctica, esta clasificación revela que la pobreza no es uniforme existiendo sectores que, aun contando con ingresos mínimos, carecen de servicios de salud adecuados, de acceso a internet o de condiciones de vivienda salubre, lo que los ubica en una situación de pobreza multidimensional. A ello se suma la pobreza extrema, entendida como la incapacidad de subsistir con un ingreso menor a 2,15 dólares diarios lo que constituye un límite dramático que afecta todavía a cientos de millones de personas en el mundo (Banco Mundial, 2022).

Por tanto, la pobreza debe ser entendida como un fenómeno estructural, multidimensional y complejo que limita tanto la libertad como las oportunidades de los individuos y que deteriora la cohesión social, siendo que, reconocer sus distintas manifestaciones es fundamental para avanzar hacia políticas públicas más inclusivas y sostenibles, estando su estrecha relación con la exclusión financiera la cual muestra cómo la falta de acceso a los sistemas formales de crédito y ahorro constituye un obstáculo adicional para superar las privaciones, perpetuando la desigualdad y la vulnerabilidad de los sectores más desfavorecidos.

Asimismo, el Banco Mundial (2022) considera que la inclusión financiera es un elemento facilitador clave para reducir la pobreza extrema y promover la prosperidad compartida, enfatizando que el acceso a productos financieros

seguros, asequibles y de calidad debe ser entendido como parte esencial de cualquier estrategia integral de desarrollo, esta afirmación sintetiza que la pobreza no se supera únicamente con transferencias monetarias o asistencia social, sino mediante la creación de condiciones estructurales que permitan a las personas generar, gestionar y proteger sus recursos a lo largo del tiempo. Desde esta perspectiva, la inclusión financiera no solo implica que una persona pueda abrir una cuenta bancaria, sino que esta cuenta le ofrezca condiciones adecuadas para su realidad económica y le conecte con una gama de servicios adaptados a sus necesidades. Esto significa que, para ser efectiva, la inclusión financiera debe ir acompañada de educación financiera y marcos regulatorios que garanticen transparencia y protección al consumidor, ya que, de lo contrario, la mera apertura de cuentas sin acceso real a créditos justos, seguros o medios de pago eficientes no se traduce en un cambio sustantivo en la vida de las personas.

Además, conforme señala el Banco Mundial (2020), el acceso a los servicios financieros contribuye significativamente a mejorar la vida cotidiana de las personas, ya que, les permite planificar tanto sus metas a largo plazo como afrontar imprevistos económicos, es importante porque quienes poseen una cuenta en una entidad financiera tienen mayores posibilidades de utilizar otros instrumentos, como créditos o seguros, que facilitan el emprendimiento, la ampliación de negocios, la inversión en educación y salud, así como la gestión de riesgos y la superación de crisis económicas; en este sentido, el acceso efectivo a servicios financieros constituye un catalizador para el desarrollo integral de las personas y las comunidades y, tal como señala el Banco Mundial, disponer de herramientas como cuentas de ahorro, líneas de crédito o seguros permite no solo cubrir necesidades inmediatas, sino también proyectar objetivos a mediano y largo plazo. Asimismo, el hecho de que una persona sea titular de una cuenta incrementa la probabilidad de que utilice otros servicios financieros complementarios debido a que el acceso a un producto financiero básico abre la puerta a otros más sofisticados que, si están bien diseñados y regulados, pueden potenciar la productividad y la resiliencia económica; por ejemplo, un pequeño agricultor que cobra sus ingresos en una cuenta formal tiene más posibilidades de acceder a un microcrédito para comprar insumos, contratar un seguro agrícola

o recibir pagos electrónicos por sus ventas. De esta manera, la inclusión financiera actúa como una plataforma que integra a las personas en redes económicas más amplias, reduciendo su dependencia de circuitos informales que suelen ser más costosos y riesgosos.

Además, la planificación que permite el acceso a estos servicios no solo beneficia a las familias de manera individual, sino que también fortalece el tejido social y económico de las comunidades, esto se demuestra cuando las personas pueden administrar mejor sus recursos y anticipar gastos, de esta forma disminuye la presión sobre redes informales de préstamo, lo que reduce prácticas usureras y formas de endeudamiento abusivo como el “gota a gota” y esta estabilidad en los hogares se traduce en una mayor capacidad de consumo, inversión y ahorro, impulsando un crecimiento más inclusivo. Por tanto, la inclusión financiera debe dejar de ser un objetivo aislado para convertirse en una estrategia que busca el desarrollo territorial equilibrado de la sociedad; no obstante, este potencial solo se materializa cuando los servicios financieros son realmente accesibles y adecuados para cada segmento de la población, el Banco Mundial (2020) subraya que el diseño de productos debe responder a la realidad económica y cultural de los usuarios, considerando factores como ingresos irregulares, baja alfabetización financiera o limitaciones tecnológicas; en este sentido, la digitalización ofrece oportunidades para ampliar la cobertura, pero también plantea el desafío de garantizar que las personas comprendan y confíen en estas herramientas, por lo que, sin una adecuada formación y sin mecanismos efectivos de protección al consumidor, la inclusión financiera puede transformarse en una trampa que exponga a los usuarios a fraudes, sobreendeudamiento o pérdida de sus recursos.

Finalmente, es importante indicar que no se trata únicamente de proveer acceso físico o digital a los servicios, sino de construir relaciones sostenibles entre los usuarios y las instituciones financieras, exigiendo políticas públicas coordinadas que combinen inversión en infraestructura, incentivos para la innovación financiera responsable, educación continua y una supervisión estatal que proteja los derechos de los consumidores, ya que, solo así el acceso a servicios financieros cumplirá la promesa de mejorar la calidad de vida, fortalecer las

economías locales y generar oportunidades reales para que las personas puedan alcanzar sus metas, incluso en contextos de alta vulnerabilidad.

En cuanto a la exclusión financiera, esta puede manifestarse de diversas formas, como en la ausencia de acceso físico a entidades financieras, desconocimiento o desconfianza hacia los productos financieros, falta de documentación legal para abrir cuentas o solicitar créditos, o bien barreras económicas como comisiones y tasas de interés demasiado altas; en este sentido, la pobreza no solo es una consecuencia de la exclusión, sino también una de sus principales causas, ya que las instituciones financieras tradicionales suelen considerar a las personas de bajos ingresos como clientes de alto riesgo, restringiendo su participación en el sistema.

En el contexto peruano, según el Instituto Nacional de Estadística e Informática (2024), al tercer trimestre de 2023, el 57,9 % de la población de 18 años a más tenía al menos una cuenta en el sistema financiero; sin embargo, un 42 % de adultos aún permanece fuera de este sistema, con una exclusión más severa en zonas rurales, donde solo el 38 % accede a estos servicios. Esta brecha revela que el desarrollo del sistema financiero peruano no ha alcanzado de manera equitativa a toda la población, generando un terreno fértil para la proliferación de mecanismos informales de financiamiento.

Las consecuencias de esta exclusión se hacen evidentes en el uso recurrente de prácticas crediticias informales, muchas veces abusivas debido a la urgencia de cubrir necesidades básicas o emergencias económicas lleva a las personas a aceptar condiciones de endeudamiento desfavorables, que incluyen intereses desproporcionados y mecanismos de cobranza coercitivos, contemplando esto el caso de los préstamos digitales “gota a gota”, que se han expandido en el país aprovechando vacíos normativos, la falta de educación financiera y la necesidad de liquidez inmediata, logrando imponer condiciones extorsivas, en las que el incumplimiento conlleva hostigamiento o amenazas.

El vínculo entre pobreza, exclusión financiera y dependencia de mecanismos informales se ve reforzado por factores estructurales como la informalidad laboral, ya que, en el Perú, según el Instituto Nacional de Estadística e Informática (2024), más del 70 % de la población ocupada trabaja en condiciones informales, sin acceso a beneficios sociales ni a historial crediticio,

lo que dificulta que las instituciones bancarias evalúen su capacidad de pago y les otorguen crédito formal, perpetuando un sistema en el que los más vulnerables son los más propensos a recurrir a soluciones de alto riesgo.

En esa línea, como señala Roca (2023), el acceso de las personas a los servicios financieros mejora su bienestar, específicamente, en el ámbito económico, puesto que permite planificar gastos, invertir en oportunidades de generación de ingresos y reducir la vulnerabilidad ante crisis, siendo la inclusión financiera un instrumento para garantizar la igualdad de oportunidades y la justicia social.

No obstante, como advierte la Superintendencia de Banca, Seguros y AFP (2022): “el Perú muestra un desarrollo desigual por género, nivel de ingreso, ámbito rural urbano y grupo etario, en los que las brechas que registra el país son más grandes que el promedio de la región”, reflejando de esta forma la urgencia de implementar políticas públicas diferenciadas que consideren las particularidades de cada segmento de la población, a fin de cerrar las brechas de acceso. Ello implica, entre otras medidas, el desarrollo de infraestructura y financiera en zonas rurales, programas de educación financiera a trabajadores informales y regulación efectiva del crédito digital.

En conclusión, la pobreza y la exclusión financiera limitan las posibilidades de desarrollo individual y colectivo, y que en el caso peruano requiere una intervención integral suponiendo no solo ampliar la cobertura y calidad de los servicios financieros, sino también prevenir que la falta de acceso derive en la exposición a esquemas abusivos como el préstamo informal digital, esta respuesta debe articular políticas públicas inclusivas con reformas legales que fortalezcan la protección del consumidor financiero y sancionen de forma específica las prácticas ilícitas que afectan a los sectores más vulnerables, evitando que la pobreza siga siendo la puerta de entrada a mecanismos crediticios coercitivos, ya que, no se contempla solo un asunto de desarrollo económico, sino también el garantizar derechos fundamentales, en tanto habilita a las personas a participar plenamente en la vida económica y social del país.

2. Dificultades de acceso al crédito en el sistema bancario tradicional

El acceso al crédito constituye un pilar fundamental para el desarrollo económico y social de las personas, ya que les permite cubrir necesidades inmediatas; sin

embargo, para amplios sectores de la población, especialmente aquellos que se encuentran en situación de pobreza o vulnerabilidad, este acceso continúa siendo limitado o inexistente debido a una serie de barreras estructurales que perpetúan la exclusión financiera; conforme a ello, la capacidad de obtener financiamiento en condiciones justas no solo se vincula con el bienestar económico individual, sino que también incide directamente en la movilidad social, pues quienes carecen de acceso a crédito formal quedan relegados a mecanismos de subsistencia que difícilmente les permiten mejorar su situación a largo plazo. No obstante, en el sistema financiero tradicional, la exigencia de garantías constituye uno de los principales obstáculos para que amplios sectores de la población puedan acceder al crédito formal, ya que, los bancos, al priorizar la seguridad de sus operaciones, imponen requisitos como hipotecas, avales sólidos o un historial crediticio positivo, condiciones que gran parte de los trabajadores informales o de bajos ingresos no puede cumplir, si bien tomando esta precauciones se protege a las entidades frente al riesgo de impago, las mismas terminan excluyendo sistemáticamente a los denominados “sujetos de riesgo”, quienes precisamente son los que más requieren mecanismos de financiamiento para cubrir necesidades básicas o emprender actividades productivas. En palabras de la CEPAL (2019), la banca tradicional opera bajo un modelo de inclusión “excluyente”, en el que el acceso está condicionado por parámetros que la mayoría de los pobres no puede satisfacer, lo que genera un círculo vicioso de marginación financiera; asimismo, este excesivo garantismo no solo limita las oportunidades de los sectores más vulnerables, sino que también fomenta su dependencia hacia formas de financiamiento informal, como prestamistas usureros o esquemas ilegales de crédito.

Entonces, la desconfianza de los bancos frente a los “sujetos de riesgo” genera, en la práctica, una transferencia de costos hacia quienes menos capacidad tienen de soportarlos, pues deben recurrir a créditos con tasas abusivas o condiciones extorsivas, como advierte el Banco Mundial (2022), las políticas crediticias centradas exclusivamente en la solvencia patrimonial del prestatario ignoran dimensiones fundamentales de la inclusión financiera, tales como la potencialidad productiva, la disciplina de pago o el capital social del individuo y de este modo, el garantismo bancario, lejos de mitigar los riesgos, los traslada y

profundiza en la base de la pirámide social, ampliando la brecha de exclusión financiera.

La informalidad laboral, que en el Perú supera el 70 % de la población económicamente activa como se ha señalado anteriormente, constituye uno de los principales factores que explican esta exclusión, ya que la mayoría de entidades financieras exigen ingresos formales y comprobables para otorgar un préstamo, desconociendo la existencia de economías domésticas que, aunque productivas, no cumplen con los estándares formales de documentación. A ello se suma la falta de historial crediticio, un requisito que en la práctica se convierte en un obstáculo circular porque para acceder a un crédito se necesita un historial, pero para tener historial se requiere haber accedido previamente a un crédito, entonces, esta situación excluye a jóvenes, emprendedores informales o personas que nunca han utilizado servicios financieros formales. También los requisitos de garantías reales, como la hipoteca de un bien inmueble o la presentación de avales, resultan inviables para quienes no poseen patrimonio suficiente, reforzando la exclusión y manteniendo el acceso al crédito como un privilegio restringido.

En el caso peruano, estas barreras son especialmente evidentes en zonas rurales, donde la presencia física de bancos y cooperativas de ahorro y crédito es limitada, pues la concentración de la infraestructura financiera en áreas urbanas genera un acceso desigual, obligando a las personas a desplazarse largas distancias para realizar trámites o, en muchos casos, a desistir de la idea de solicitar un préstamo, entonces este centralismo en la oferta de servicios financieros no solo es una manifestación geográfica de la desigualdad, sino que también refleja una falta de adaptación del sistema bancario a las realidades socioculturales y económicas de la población rural.

Los datos del Instituto Nacional de Estadística e Informática(2024), muestran que cerca del 8 % de los hogares urbanos recurrieron a créditos informales en 2023, y lo más alarmante es que el 40 % de estos hogares ya había utilizado un crédito informal anteriormente, esto evidencia que no se trata de casos aislados, sino de una tendencia persistente que responde a la ausencia de alternativas sostenibles en el sistema formal y la magnitud del problema se incrementa si consideramos que el 49 % de los créditos informales presentan tasas anualizadas que superan

el 500 %, lo que constituye un costo financiero exorbitante y prácticamente impagable en comparación con las tasas reguladas por entidades supervisadas, provocando estas situaciones desproporcionadas un endeudamiento crónico y una dependencia casi inevitable de estos mecanismos, atrapando a las familias en un ciclo de deuda que consume sus ingresos y limita cualquier posibilidad de ahorro o inversión productiva.

Más allá de las cifras, este escenario revela una falla estructural del mercado ya que, las instituciones financieras tradicionales han desarrollado productos y requisitos pensados principalmente para un segmento de población con ingresos formales, estabilidad laboral y capacidad de ofrecer garantías, dejando fuera a quienes más necesitan financiamiento; asimismo, en el plano de las políticas públicas, la falta de incentivos para que los bancos amplíen su cobertura y flexibilicen sus criterios de evaluación ha permitido que la brecha crediticia se mantenga, mientras que los programas de crédito estatal no alcanzan a cubrir la demanda real. Por otro lado, la urgencia de liquidez que experimentan las personas en situación de pobreza o vulnerabilidad incrementa su exposición a opciones de alto riesgo, como los préstamos informales tradicionales o los más recientes préstamos digitales “gota a gota”. En ambos casos, el acceso es rápido y sin mayores requisitos, pero las condiciones de pago, las tasas de interés y las prácticas de cobranza son abusivas, llegando en ocasiones a incluir amenazas, acoso o violencia física que lejos de ofrecer una solución real, profundiza la exclusión financiera y genera un impacto negativo no solo en el ámbito económico, sino también en la seguridad y la integridad de las personas.

En definitiva, resulta urgente implementar reformas que promuevan productos financieros adaptados a la realidad de la economía informal, que fortalezcan la educación financiera y amplíen la cobertura territorial del sistema formal, de manera que el crédito deje de ser un privilegio y se convierta en una herramienta real de inclusión y movilidad social, siendo así posible reducir la dependencia de mecanismos informales que, aunque accesibles, comprometen gravemente el bienestar y la estabilidad de quienes recurren a ellos.

3. Digitalización del crédito informal

Durante la última década, el avance de la tecnología y la masificación del acceso a internet han generado cambios estructurales en prácticamente todos los

sectores de la economía, este proceso de transformación digital no se ha limitado al sistema bancario formal, sino que también ha alcanzado de manera significativa al sector crediticio informal, el cual ha adoptado herramientas digitales para expandir su alcance y optimizar sus métodos de captación de clientes. De esta forma, prácticas que anteriormente se desarrollaban en entornos físicos y locales, como los préstamos presenciales en mercados, barrios o espacios comunitarios, han migrado progresivamente hacia entornos virtuales, especialmente aplicaciones móviles y plataformas en línea que operan al margen de la regulación, este cambio ha permitido que los prestamistas informales lleguen a segmentos poblacionales que antes se encontraban fuera de su radio de acción, de esta forma Rodríguez, Fernández & Bautista (2023) señalan que: "La combinación de acceso masivo de teléfonos inteligentes, acceso más económico a planes de datos móviles y creciente familiaridad de la población con el uso de aplicaciones ha configurado un terreno fértil para que surjan nuevos modelos de oferta crediticia no regulada porque las redes sociales se han convertido en un referente global de las relaciones interpersonales, al integrar correo electrónico, mensajería, blogs y álbumes digitales en un mismo espacio de interacción". De esta manera, se advierte que, aunque estas plataformas facilitan la gestión de la identidad y la comunicación, también exponen a los usuarios a riesgos significativos, y es de esta forma, que los prestamistas informales aprovechan canales como redes sociales, anuncios publicitarios en buscadores y videos en plataformas digitales, además de estrategias de marketing en aplicaciones de mensajería instantánea, para atraer potenciales prestatarios apelando a las necesidades urgentes de liquidez, ofreciendo préstamos inmediatos, sin necesidad de historial crediticio, sin avales y sin procesos burocráticos, lo que resulta particularmente atractivo para personas excluidas del sistema financiero tradicional o que enfrentan una emergencia económica.

No obstante, detrás de esta aparente facilidad de acceso se ocultan prácticas abusivas que históricamente han caracterizado al crédito informal, estos préstamos digitales suelen imponer intereses excesivos que, en términos anualizados, pueden alcanzar cifras desproporcionadas e insostenibles. Además, persiste la ausencia de transparencia en las condiciones del contrato,

con cláusulas poco claras o directamente inexistentes, lo que coloca al prestatario en una situación de completa desventaja frente al prestamista.

Una de las prácticas más preocupantes es el acceso masivo e indiscriminado a la información personal del prestatario que se realiza cuando una persona descarga la aplicación de un prestamista informal, ya que, esta suele solicitar permisos excesivos que van más allá de lo estrictamente necesario para otorgar un crédito y, tal como ha advertido la Superintendencia de Banca, Seguros y AFP del Perú (SBS, 2023), muchos de estos aplicativos exigen al usuario conceder acceso al directorio de contactos, así como a carpetas privadas que contienen fotografías, videos o documentos personales, y adicionalmente monitorean su actividad en el dispositivo, constituyendo no solo una invasión a la privacidad, sino que se convierte en una herramienta de coacción digital, ya que los prestamistas pueden amenazar con difundir esta información entre familiares, amigos o compañeros de trabajo en caso de retraso o impago; de hecho, distintos reportajes periodísticos y alertas institucionales han documentado que las aplicaciones de préstamo digital emplean mecanismos de cobranza intimidatoria que incluyen llamadas y mensajes masivos dirigidos a los contactos del prestatario, difusión de información personal en redes sociales y manipulación de imágenes con fines de difamación y presión psicológica (Infobae Perú, 2025; Perú21, 2024; Agencia Andina, 2023).

Estas estrategias no requieren la presencia física del cobrador, pero generan un impacto igual o mayor en la víctima, que se ve expuesta a un acoso persistente y difícil de detener debido a la falta de supervisión legal sobre estas operaciones.

La digitalización del crédito informal también ha modificado la escala y velocidad de este mercado, porque mientras que en el modelo tradicional un prestamista debía invertir tiempo y recursos para identificar y captar clientes dentro de un entorno físico limitado, las plataformas digitales permiten llegar simultáneamente a miles de personas, incluyendo a usuarios de distintas regiones del país e incluso del extranjero, significando que el riesgo de sobreendeudamiento y de expansión de estas redes es mayor, ya que la intermediación tecnológica aumenta su capacidad de respuesta ante nuevas solicitudes.

Por otra parte, organismos como el Banco Mundial (2020) han señalado que las plataformas digitales pueden reducir costos, ampliar la cobertura y facilitar la

entrada de sectores históricamente excluidos al sistema financiero formal; sin embargo, en el caso del crédito informal digital, esta potencialidad se ha desvirtuado, pues en lugar de integrar a las personas a circuitos seguros y regulados, las expone a nuevas modalidades de explotación y abuso, sin garantías legales ni mecanismos efectivos de reclamación. La falta de regulación específica sobre estas prácticas es un factor determinante en su proliferación, ya que, aunque en el Perú la SBS (2023) haya emitido advertencias públicas sobre el uso de aplicativos no autorizados, el marco legal actual no contempla mecanismos suficientemente ágiles para investigar, bloquear o sancionar estas operaciones, dejando a las víctimas en una situación de desprotección, ya que las posibilidades de presentar una denuncia efectiva son escasas.

En definitiva, la digitalización del crédito informal representa un desafío urgente para las políticas públicas, las autoridades regulatorias y la sociedad en general, debido a que, si bien la tecnología puede y debe ser aprovechada para mejorar la inclusión financiera, resulta indispensable establecer controles que garanticen la transparencia, la protección de datos personales y la seguridad del usuario. De lo contrario, el espacio digital seguirá siendo un terreno fértil para prácticas abusivas que, bajo la apariencia de modernización, perpetúan y amplifican los riesgos del crédito informal tradicional.

4.El fenómeno “gota a gota”

El préstamo “gota a gota” es una modalidad de financiamiento informal que ha cobrado fuerza en varios países de América Latina, incluido el Perú, caracterizándose por su aparente facilidad de acceso y sus métodos coercitivos de cobro. Este fenómeno afecta principalmente a las poblaciones en situación de vulnerabilidad, especialmente aquellas que viven en zonas rurales o periurbanas donde la presencia del sistema financiero formal es escasa, según Menacho Ramírez (2024):

“Estos préstamos inciden mayormente en localidades alejadas y empobrecidas. De esta manera, son dos los factores que convierten a sus pobladores en sujetos pasivos perfectos: por un lado, las barreras burocráticas que los bancos exigen para acceder a un crédito; y por otro, la deficiente seguridad ciudadana que el Estado ofrece. En consecuencia, los pobladores optan por la informalidad crediticia al no tener otra opción.”

La afirmación de Menacho Ramírez es clave porque evidencia que el “gota a gota” no es un fenómeno aislado ni producto exclusivo de decisiones individuales imprudentes, sino la manifestación visible de un problema estructural más profundo; en primer lugar, las barreras burocráticas del sistema bancario formal como la exigencia de comprobantes de ingresos estables, historial crediticio positivo o garantías hipotecarias excluyen sistemáticamente a quienes trabajan en la economía informal, que, como se ha indicado anteriormente, en el Perú representan alrededor del 70% de la población económicamente activa. Este sector, al no contar con mecanismos formales de respaldo financiero, queda en un estado de permanente exclusión que lo hace más proclive a buscar soluciones rápidas, aunque estas impliquen altos riesgos.

En segundo lugar, la deficiente seguridad ciudadana en muchas localidades rurales y periurbanas genera un vacío que es aprovechado por redes de prestamistas informales, en estos contextos, la ausencia de la autoridad policial y judicial no solo facilita la instalación de estas redes, sino que impide que las víctimas denuncien por temor a represalias. Así, los prestatarios se encuentran atrapados en un ciclo donde el acceso al dinero implica también una pérdida de libertad y seguridad, pues el cobro del préstamo se ejecuta mediante amenazas, hostigamientos o incluso violencia física.

Este entramado estructural de exclusión financiera más inseguridad ciudadana configura un terreno fértil para que el “gota a gota” prospere y se normalice como parte de la vida económica local y el problema se agrava porque en muchas de estas comunidades el préstamo informal no es percibido inicialmente como un acto ilícito, sino como un servicio necesario, al que se recurre de forma recurrente para financiar gastos de emergencia, cubrir necesidades básicas o invertir en actividades de subsistencia.

En síntesis, lo que plantea Menacho permite comprender que el “gota a gota” no es solamente una práctica abusiva de carácter individual, sino un síntoma de la falla simultánea del sistema financiero, que no logra integrar a toda la población, y del sistema estatal, que no garantiza un marco mínimo de seguridad y protección para sus ciudadanos. Por tanto, mientras estas condiciones persistan, el “gota a gota” seguirá siendo, para muchas personas, no la peor opción, sino la única, debido a que el atractivo del mecanismo de funcionamiento del “gota a

gota” se basa en ofrecer sumas de dinero de entrega inmediata, sin requisitos formales ni verificación de historial crediticio; sin embargo eso se acompaña de intereses diarios extremadamente altos, lo que provoca que la deuda crezca de forma acelerada y, en muchos casos, se vuelva impagable, sumado a la amenaza constante hacia los prestatarios y sus familias, quienes suelen ser objeto de hostigamiento así como violencia física o psicológica.

La Superintendencia de Banca, Seguros y AFP (SBS, 2023) ha advertido que el fenómeno llamado “gota a gota” no constituye una forma legítima de financiamiento y que, en la mayoría de los casos, las personas que acceden a estos préstamos terminan pagando montos muy superiores al que recibieron originalmente, según un pronunciamiento de esta entidad (2022), “estas prácticas ponen en riesgo la integridad física y económica de los prestatarios, generando situaciones de violencia, extorsión y hostigamiento”, lo cual evidencia que el problema excede el ámbito financiero, ya que no se trata únicamente de deudas impagables, sino de un entramado de amenazas y agresiones que comprometen la seguridad y el bienestar de las víctimas.

La presión ejercida por el pago diario, la cual es una característica central de este fenómeno, drena de forma constante los recursos de pequeños comerciantes y trabajadores independientes, impidiéndoles acumular capital o reinvertir en sus actividades; en consecuencia, se perpetúa un círculo vicioso en el que la falta de liquidez conduce a la búsqueda recurrente de nuevos préstamos, generando una dependencia crónica del crédito informal. Esto no solo afecta a nivel individual, sino que también debilita el tejido económico local, pues el capital generado por pequeños negocios es transferido de manera continua a redes ilegales que operan al margen de cualquier tributación o control.

Adicionalmente, el impacto psicológico de estas prácticas resulta igualmente devastador debido al constante hostigamiento, sumado a la incertidumbre y al temor de represalias, puede provocar altos niveles de ansiedad, depresión y estrés en los prestatarios, lo que a su vez afecta su productividad y sus relaciones personales. En contextos de inseguridad ciudadana y ausencia de mecanismos de protección eficaces, el “gota a gota” se consolida como una de las expresiones más agresivas de la exclusión financiera y social.

Por ello, el combate a este fenómeno exige una estrategia integral que no se limite a la persecución penal, sino que también aborde sus causas estructurales como son la desigualdad en el acceso al crédito formal, la falta de educación financiera y la escasa presencia del Estado en territorios vulnerables. Solo mediante un enfoque que combine represión del delito y creación de alternativas financieras legítimas será posible disminuir la incidencia de esta práctica y proteger a las comunidades que hoy se ven atrapadas en su dinámica abusiva.

A nivel internacional, la problemática del “gota a gota” ha sido reconocida por organismos como la Oficina de las Naciones Unidas contra la Droga y el Delito (2022) al indicar que se ha alertado sobre la relación de este tipo de financiamiento con el lavado de activos y la expansión de redes delictivas transnacionales. En este sentido, abordar el “gota a gota” requiere no solo un enfoque regulatorio y de persecución penal, sino también estrategias de inclusión financiera que ofrezcan alternativas reales y seguras a la población vulnerable, pues si las personas no cuentan con opciones de crédito asequibles y transparentes, las redes de “gota a gota” seguirán encontrando terreno fértil para operar, reproduciendo un ciclo de endeudamiento abusivo y exclusión financiera.

En los últimos años, esta modalidad ha experimentado un proceso de digitalización que ha potenciado su alcance y complejidad. Según la Oficina General de Comunicación Social e Imagen Institucional del Ministerio del Interior (2023), estas modalidades suelen captar a las personas ofreciendo préstamos rápidos y sin requisitos, mediante anuncios en redes sociales, páginas web o aplicaciones móviles. No verifican antecedentes crediticios ni solicitan garantías, ya que operan fuera del sistema financiero supervisado por la Superintendencia de Banca, Seguros y AFP (SBS). Para acceder al dinero, el usuario debe instalar una aplicación desde una tienda virtual, lo que permite a los delincuentes acceder a la información almacenada en el dispositivo. Posteriormente, utilizan esos datos para extorsionar al prestatario, amenazando con difundir entre sus contactos la supuesta deuda pendiente.

Esta situación pone en evidencia cómo las redes criminales han aprovechado el desarrollo tecnológico para perfeccionar sus mecanismos de control y coacción, extendiendo el daño más allá del ámbito económico hacia la esfera personal y

social de las víctimas. La digitalización ha hecho posible que los prestamistas informales ya no necesiten una presencia física para captar usuarios, pues pueden operar a distancia y de manera masiva, llegando incluso a sectores que antes estaban fuera de su alcance. El empleo de plataformas virtuales y aplicaciones móviles ha disminuido considerablemente los costos y tiempos de operación, al mismo tiempo que ha incrementado el anonimato y la dificultad de rastrear a los responsables.

Por otro lado, la ausencia de mecanismos de verificación o consultas en centrales de riesgo, que podría parecer una facilidad para el solicitante, en realidad representa un riesgo mayor. Si bien elimina las barreras para acceder al dinero, también expone al prestatario a condiciones abusivas y a prácticas de extorsión que resultan imposibles de revertir dentro del marco normativo vigente. El hecho de que estos servicios operen fuera del sistema financiero regulado por la Superintendencia de Banca, Seguros y AFP (SBS) deja al usuario sin ningún tipo de respaldo institucional, totalmente vulnerable ante la voluntad del prestamista.

Uno de los elementos más alarmantes de esta modalidad digital es el uso indebido de los datos personales de las víctimas. Al otorgar permisos excesivos al descargar las aplicaciones, los usuarios permiten el acceso a su lista de contactos, fotografías, videos y ubicación, convirtiendo su propio teléfono en una herramienta de vigilancia y chantaje. Con esta información, los prestamistas ejercen presión psicológica y social, amenazando con difundir supuestas deudas o datos privados a familiares, amigos o compañeros de trabajo. Esta forma de coacción digital genera un alto nivel de estrés emocional y puede provocar aislamiento social, pérdida de reputación y deterioro de los vínculos personales.

En consecuencia, la digitalización del préstamo informal no ha significado un progreso hacia una mayor inclusión financiera, sino una evolución de las prácticas abusivas tradicionales, ampliando el alcance del problema y dificultando su persecución. Aunque el crédito “gota a gota” clásico ya era perjudicial, su versión digital incorpora un nuevo nivel de riesgo, pues la víctima no solo enfrenta intereses usureros, sino también la amenaza de exposición pública y vulneración de su intimidad. Así, la tecnología, lejos de servir como

herramienta de democratización financiera, se transforma en un instrumento que incrementa la vulnerabilidad del prestatario.

Finalmente, aunque este fenómeno tiene su origen en la exclusión crediticia y en la falta de acceso al financiamiento formal, su expansión actual también se debe a la carencia de una regulación efectiva sobre las operaciones digitales. Los requisitos exigidos por las entidades financieras como garantías, historial crediticio o ingresos demostrables empujan a un sector significativo de la población hacia estas alternativas informales que prometen rapidez, pero que en la práctica generan deudas desproporcionadas y difíciles de solventar.

En el contexto peruano, el “gota a gota” ha encontrado terreno fértil debido a la combinación de factores como la exclusión financiera que margina a millones de personas del acceso al crédito formal, la insuficiente cobertura de seguridad ciudadana que deja a las comunidades desprotegidas, y la facilidad tecnológica para establecer vínculos anónimos y rápidos entre prestamistas y prestatarios. Este escenario convierte al fenómeno en un problema de múltiples dimensiones, que involucra aspectos económicos, sociales, legales y tecnológicos, y que requiere de un abordaje integral que vaya más allá de la simple represión policial.

En suma, el “gota a gota” representa una amenaza creciente para la estabilidad financiera y la seguridad personal de amplios sectores de la población. Su erradicación pasa por implementar políticas públicas que combinen el fortalecimiento de la inclusión financiera, el desarrollo de sistemas de microcrédito regulado, el incremento de la seguridad ciudadana y la educación financiera, especialmente en las zonas más vulnerables. De lo contrario, este fenómeno seguirá expandiéndose y adaptándose a las nuevas realidades tecnológicas, perpetuando ciclos de endeudamiento abusivo y violencia.

5. Vacíos legales en la legislación penal frente al préstamo informal digital

El vertiginoso avance de las tecnologías de la información y la comunicación ha transformado múltiples aspectos de la economía, incluyendo el acceso al crédito; sin embargo, esta innovación también ha abierto espacios para que prácticas ilegales se adapten y evolucionen más rápido que los marcos regulatorios, según la Superintendencia de Banca, Seguros y AFP (SBS, 2023), el uso de plataformas digitales financieras crece a un ritmo más rápido que la capacidad

normativa del Estado, generando riesgos de fraude y extorsión digital y el préstamo informal digital, que es operado a través de aplicaciones móviles, es un ejemplo claro de cómo la ley puede quedarse rezagada frente a la realidad tecnológica, ya que, si bien muchos países, incluido el Perú, cuentan con normativas para supervisar y sancionar la usura, la extorsión o la estafa, en la práctica existen vacíos que dificultan la persecución penal de estas modalidades.

Uno de los principales problemas que plantea el fenómeno del préstamo informal digital, conocido como gota a gota digital, es la dificultad de encuadrar jurídicamente la conducta en un único tipo penal, lo que genera vacíos y ambigüedades en la respuesta penal, esta situación deriva en gran medida de la posible configuración de un concurso ideal de delitos entre figuras como la extorsión, la coacción y la estafa, que se solapan en la dinámica de estos hechos.

En primer lugar, la estafa aparece como delito de base en estas operaciones cuando el usuario, atraído por la promesa de préstamos rápidos y sin requisitos, entrega voluntariamente sus datos personales y financieros, aceptando términos que suelen estar diseñados de manera engañosa configurando así un engaño idóneo para inducir a error a la víctima, quien, convencida de que accede a un crédito legítimo, se obliga a condiciones abusivas que no fueron informadas claramente.

En segundo lugar, la dinámica del “gota a gota digital” muestra rasgos propios de la coacción, pues las aplicaciones no se limitan al engaño inicial, sino que recurren a presiones posteriores para forzar el pago, ya que, estas presiones incluyen el envío masivo de mensajes intimidatorios, el contacto constante a través de llamadas o chats, e incluso la amenaza de difundir información privada obtenida del celular de la víctima. Tales conductas se adecuan al tipo de coacción previsto en el artículo 151 del Código Penal peruano, que sanciona al que “impide a otro hacer lo que la ley no prohíbe o lo obliga a hacer lo que no quiere” y en este caso, la finalidad es doblegar la voluntad de la víctima para forzar el pago de deudas artificialmente incrementadas.

Finalmente, se manifiestan características de la extorsión, ya que el cobro se produce mediante amenazas graves dirigidas contra la integridad, el honor o la tranquilidad de la víctima y de sus allegados al advertir que si no se paga el dinero se divulgarán fotos íntimas, se contactará a familiares o se difundirá

información difamatoria en redes sociales, encajando estos casos plenamente en el tipo penal de extorsión porque, a diferencia de la coacción, aquí la amenaza se proyecta con un contenido patrimonial al obtener la entrega de dinero mediante intimidación, lo que agrava la ilicitud de la conducta.

En ese sentido, uno de los principales problemas radica en que las normas actuales fueron diseñadas para un contexto predominantemente físico y presencial, por lo que no contemplan con claridad supuestos en los que el acoso, la coacción o el fraude se ejecutan mediante aplicaciones móviles, redes sociales o sistemas de mensajería instantánea. Esto genera dificultades tanto para la identificación de los autores como para la tipificación precisa de sus conductas, lo que a su vez debilita la capacidad del Estado para ofrecer una respuesta efectiva.

Tal como advierte Catalina Salvador Ramírez (2024), No se trata únicamente de una manifestación común del delito, sino de una forma de criminalidad compleja y sofisticada, cuyas consecuencias resultan aún más graves. Las víctimas pueden ser tanto personas en situación de vulnerabilidad —como adultos mayores, menores de edad o individuos con escasos conocimientos tecnológicos— como también usuarios con alto poder adquisitivo o amplia actividad bancaria; en consecuencia, nadie se encuentra completamente exento de ser afectado por esta modalidad delictiva tecnológica. lo cual evidencia que el fenómeno no discrimina en cuanto a sus víctimas, pues su alcance va desde sectores en extrema vulnerabilidad hasta personas con recursos, demostrando así que el riesgo no se limita a un grupo específico, sino que se proyecta sobre toda la sociedad.

A esta complejidad se suma la dificultad para individualizar a los responsables, un obstáculo que se erige como uno de los mayores vacíos operativos en la persecución penal; bajo este enfoque, Ramírez (2024) sostiene que, cuando el Ministerio Público no logra identificar o individualizar a los autores de los delitos informáticos, la investigación no puede avanzar y, en consecuencia, debe ser archivada. Así, la principal causa de impunidad en este tipo de delitos radica precisamente en la imposibilidad de determinar quién es el sujeto activo. Ello se desprende del numeral 1 del artículo 336 del Código Procesal Penal, que establece que la formalización de la investigación solo procede, entre otros

supuestos, cuando el investigado ha sido debidamente individualizado. En la práctica, esto significa que el anonimato digital, facilitado por redes privadas virtuales, servidores ubicados en jurisdicciones sin tratados de cooperación judicial y el uso de identidades falsas, opera como una barrera que frena el avance de los procesos y la problemática se agrava cuando los fondos obtenidos mediante prácticas extorsivas o usurarias son canalizados a través de cuentas bancarias de terceros. Aunque estas cuentas puedan ser identificadas por las autoridades, ello no garantiza que su titular sea el autor material o intelectual del delito, pues a menudo actúan como intermediarios inconscientes o como participantes menores dentro de una estructura criminal más amplia. De este modo, el rastro del dinero se fragmenta y diluye, dificultando la trazabilidad y reduciendo la probabilidad de una condena.

En consecuencia, la combinación de vacíos normativos y barreras técnicas produce un efecto de impunidad que incentiva la expansión del préstamo informal digital, demostrando que, sin una reforma legal que contemple de forma específica estas conductas, fortalecida por herramientas tecnológicas de investigación criminal y acuerdos internacionales de cooperación en materia de ciberdelincuencia, las posibilidades de sancionar efectivamente a los responsables seguirán siendo mínimas, no solo perpetuando en el daño económico y psicológico a las víctimas, sino que también envía un mensaje de permisividad que refuerza la percepción de que este tipo de delitos es de bajo riesgo para los infractores.

En el caso peruano, la legislación penal no contempla de forma específica las particularidades del préstamo informal digital, porque este tipo de operaciones, al desarrollarse en un entorno virtual y con prestamistas que muchas veces se encuentran fuera del territorio nacional, escapan a los mecanismos tradicionales de investigación y sanción; además, el hecho de que los contratos sean inexistentes o se basen en simples interacciones digitales complica la recopilación de pruebas sólidas que permitan judicializar los casos.

La Superintendencia de Banca, Seguros y AFP (SBS, 2023) ha reconocido que, Aunque estas conductas pueden encuadrarse dentro de tipos penales ya existentes, resulta imprescindible modernizar la legislación para hacer frente a las nuevas modalidades de criminalidad financiera. Tal como señala la entidad

en su comunicado, la dimensión digital y transnacional de estas operaciones exige reforzar la cooperación internacional y adecuar los instrumentos jurídicos a fin de garantizar una persecución penal efectiva.

A nivel global, organismos como el Banco Mundial y la Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2020) Se ha destacado la necesidad de que la normativa financiera avance al mismo ritmo que la innovación tecnológica, incorporando mecanismos de protección al consumidor en los entornos digitales y fortaleciendo las facultades de supervisión de las autoridades competentes. Estas propuestas no solo buscan sancionar las conductas irregulares, sino también prevenir que los sectores más vulnerables sean captados por esquemas abusivos que se aprovechan de la falta de educación financiera y de la necesidad urgente de obtener liquidez.

En suma, la ausencia de disposiciones penales claras y adaptadas al fenómeno del préstamo informal digital representa una amenaza creciente para la seguridad económica y personal de los ciudadanos. Mientras la ley no se actualice para contemplar las particularidades de este tipo de operaciones, su carácter anónimo, transnacional, digital y muchas veces no documentado, las víctimas seguirán enfrentando enormes dificultades para denunciar y obtener justicia. Por ello, abordar este vacío legal requiere una estrategia integral que incluya reformas legislativas, cooperación internacional, fortalecimiento de capacidades policiales y fiscales, así como campañas masivas de educación financiera y digital.

CAPITULO II: “DELITOS DIGITALES/CIBERNÉTICOS”

1. Conceptualización de los delitos cibernéticos

La acelerada expansión de las tecnologías de la información y la comunicación ha transformado de manera radical la forma en que los individuos interactúan, realizan transacciones y acceden a la información; sin embargo, junto a estas oportunidades también han surgido riesgos y amenazas que han dado lugar a una nueva categoría de comportamientos ilícitos: los delitos cibernéticos. Estos constituyen conductas tipificadas por la ley en las que la informática, las redes de comunicación y los sistemas electrónicos participan como medio, instrumento o fin del acto criminal. En consecuencia, pueden definirse como aquellas

acciones ilícitas en las que los sistemas informáticos, las telecomunicaciones o los datos digitales se convierten en el medio, el objeto o la finalidad de la acción delictiva. Ahora bien, la terminología empleada para designar los delitos cometidos en el ciberespacio no ha sido uniforme. Mientras que en España se utilizaron expresiones como delitos informáticos o criminalidad informática, el término que ha prevalecido en el ámbito internacional es el de cibercriminalidad, adoptado oficialmente en el Convenio de Budapest de 2001. Como sostiene Miró (2012), esta denominación expresa con mayor exactitud el carácter social y transfronterizo de las conductas que se producen en el entorno digital, diferenciándose de la concepción más limitada de lo 'informático', vinculada exclusivamente a los aspectos técnicos.

En este contexto, Villavicencio (2014) sostiene que los llamados delitos informáticos suelen asociarse con la comisión de ilícitos a través de computadoras, internet u otros dispositivos tecnológicos. Sin embargo, subraya que estos medios no determinan por sí mismos la existencia del delito, sino que actúan únicamente como instrumentos que facilitan su comisión. De esta manera, lo digital no configura en esencia un nuevo delito, sino que constituye un entorno en el que las conductas tradicionales se reproducen y se amplifican gracias a factores propios del ciberespacio como la inmediatez, el anonimato y la transnacionalidad. Por lo tanto, esta distinción resulta fundamental porque permite comprender que el problema jurídico no se limita a la creación de nuevas figuras penales, sino que exige adaptar las ya existentes a un escenario tecnológico en constante transformación.

En consecuencia, es necesario evitar la confusión frecuente entre el medio utilizado y la naturaleza jurídica del delito, ya que el hecho de que una conducta ilícita se materialice mediante una computadora o una red de telecomunicaciones no significa que estos dispositivos sean el origen del ilícito, sino que deben entenderse como herramientas que potencian la capacidad de acción del infractor. Así, el ordenador y el internet cumplen un rol semejante al de un arma en un robo o un vehículo en un transporte ilegal, resultandos relevantes únicamente como medios comisivos y no como elementos constitutivos del delito en sí mismo.

Del mismo modo, conviene señalar que el desarrollo de esta criminalidad se encuentra directamente vinculado con el uso masivo de la tecnología informática. Al respecto, puede recordarse que, así como en su momento la invención de la imprenta generó problemas legales inéditos en torno a la falsificación de documentos y la vulneración de los derechos de autor, la informatización de la vida social ha creado escenarios igualmente nuevos para la comisión de ilícitos. La diferencia, sin embargo, es que en el entorno digital los efectos se multiplican exponencialmente debido a la inmediatez de las comunicaciones, el alcance global de las redes y la dificultad de rastrear a los responsables, lo que introduce una complejidad mayor para el derecho penal.

Por todo ello, los delitos cibernéticos comprenden aquellas conductas delictivas que dependen de manera esencial de la utilización de sistemas informáticos o redes de datos para concretarse, siendo lo característico no únicamente el daño ocasionado, sino sobre todo la dependencia tecnológica para su materialización. Bajo esta lógica, ilícitos como el fraude, la extorsión, el espionaje o incluso la trata de personas encuentran en el ciberespacio un terreno fértil para expandirse y complejizarse, lo cual demuestra que, aunque la modalidad de comisión se transforme, el núcleo del ilícito puede estar previsto en el derecho penal desde hace décadas, adaptándose solamente en sus medios de ejecución.

Ahora bien, la naturaleza expansiva del cibercrimen genera también un desfase normativo, en la medida en que muchas conductas no se encuentran contempladas de manera explícita en los códigos penales. Este desfase responde a que la innovación tecnológica avanza mucho más rápido que la capacidad del legislador para tipificar nuevos comportamientos, razón por la cual la interpretación judicial y la cooperación internacional resultan indispensables para llenar dichos vacíos y ofrecer respuestas eficaces a estas nuevas formas de criminalidad digital.

En conclusión, los delitos cibernéticos constituyen una categoría de criminalidad que debe comprenderse, por un lado, desde su carácter instrumental, al servirse de medios tecnológicos como vehículos de comisión, y, por otro, desde su autonomía conceptual, al configurar fenómenos que amplifican y transforman los riesgos delictivos tradicionales. Tal como señala Miró Llinares (2012), El cibercrimen no debe concebirse como un fenómeno completamente nuevo, sino

como la transformación de delitos tradicionales al ámbito digital. Su rasgo distintivo radica en que las tecnologías de la información funcionan como herramientas que facilitan y amplifican la ejecución del delito, otorgándole mayor alcance gracias a la inmediatez, el anonimato y la dimensión global que proporciona Internet. De esta manera, aunque la esencia del ilícito se mantiene, el contexto de ejecución se modifica radicalmente, lo que exige un replanteamiento jurídico en su conceptualización. En consecuencia, no basta con trasladar mecánicamente las figuras jurídicas tradicionales al ciberespacio, sino que resulta necesario reconocer que la tecnología redefine los bienes jurídicos afectados y obliga al derecho penal a reformular sus categorías, con el fin de asegurar una protección adecuada frente a los desafíos emergentes de la sociedad digital.

Una de las clasificaciones doctrinales más influyentes en la criminología del ciberespacio es la que diferencia entre delitos cibernéticos puros e impuros, propuesta por Miró Llinares en 2012. Este autor parte de la premisa de que No todos los delitos perpetrados mediante el uso de las tecnologías de la información y la comunicación presentan el mismo grado de vinculación con el entorno digital. Puede diferenciarse entre aquellas conductas que surgen exclusivamente a partir del ciberespacio y aquellas que, aunque preexistentes en la delincuencia tradicional, utilizan este medio como un canal más eficiente y de mayor alcance para su ejecución.

En primer lugar, se consideran delitos cibernéticos puros aquellos cuya existencia depende de manera exclusiva del ámbito digital. Es decir, son conductas que no podrían tener lugar en un entorno físico o analógico. Ejemplos son el hacking o acceso no autorizado a sistemas, la creación y propagación de malware, los ataques de denegación de servicio (DoS), la suplantación de direcciones IP (spoofing), entre otros. Estos, sin la existencia de redes telemáticas y sistemas informáticos interconectados, simplemente no serían posibles, por lo que su esencia está ligada intrínsecamente al ciberespacio. Desde esta perspectiva, se puede afirmar que los delitos puros representan la manifestación más genuina del cibercrimen, pues responden a riesgos criminógenos nuevos creados por la tecnología.

En segundo lugar, se encuentran los delitos cibernéticos impuros, que son aquellos en los que el ciberespacio actúa únicamente como medio o facilitador. En este caso, la conducta delictiva ya existía en la realidad física en delitos como fraudes, extorsiones, amenazas, estafas patrimoniales o delitos sexuales como la pornografía infantil y el grooming. La diferencia radica en que, al trasladarse al ámbito digital, estos delitos adquieren una mayor dimensión debido a características propias del ciberespacio, como la inmediatez, el anonimato del autor, la multiplicación de las víctimas potenciales y la dificultad de persecución transnacional. Dicho en otras palabras, se trata de delitos que pueden existir tanto fuera como dentro de la red, pero que en esta última encuentran un escenario idóneo para maximizar su alcance y efectividad.

Esta diferenciación no es meramente teórica, sino que tiene consecuencias prácticas relevantes. Por un lado, los delitos puros exigen la creación de tipos penales nuevos, ya que el ordenamiento jurídico tradicional no estaba preparado para sancionar conductas que no podían imaginarse antes de la era digital. Por otro lado, los delitos impuros suponen una reconfiguración de tipos penales clásicos, adaptándolos a la modalidad digital y ampliando su punibilidad. Así, mientras el fraude siempre existió en la vida social y económica, la irrupción de las nuevas tecnologías ha originado figuras como el phishing, el pharming o las estafas a través de aplicaciones móviles, que constituyen una expresión digital de un delito patrimonial clásico.

En este marco, el “gota a gota digital” debe ser calificado como un delito cibernético impuro debido a que la práctica del préstamo usurario, basada en la entrega de dinero bajo condiciones abusivas acompañadas de amenazas para forzar su devolución, existía ya en el mundo físico desde hace décadas, especialmente vinculada a dinámicas de criminalidad organizada. Sin embargo, al trasladarse al entorno digital, esta modalidad se transforma y se potencia a través de aplicaciones móviles de préstamos fáciles, publicidad en redes sociales y la recopilación ilícita de datos personales de los usuarios, los prestamistas ejercen un control más sofisticado y permanente sobre las víctimas. La coacción no se limita a la intimidación presencial, sino que se extiende al hostigamiento digital constante, al uso de fotografías o contactos del dispositivo

de la víctima para amenazarla y a la difusión de información privada como método de presión.

El “gota a gota digital”, en consecuencia, conserva el núcleo delictivo clásico de la usura y la extorsión, pero se reviste de un carácter tecnológico que lo convierte en un delito impuro. Esta condición es importante para los efectos de la política criminal, pues evidencia que no siempre es necesario crear nuevos tipos penales para enfrentar fenómenos digitales; muchas veces, como en este caso, basta con adaptar figuras ya existentes, considerando que lo novedoso es el medio de comisión más que la conducta en sí misma.

1.1 Bienes jurídicos afectados

Mientras que en los delitos tradicionales el ataque suele dirigirse contra la vida, la integridad física o el patrimonio, en el ciberespacio las vulneraciones recaen principalmente sobre bienes de carácter inmaterial. En consecuencia, desde la perspectiva criminológica, el ciberespacio debe entenderse como un nuevo ámbito de oportunidad delictiva. Siguiendo la teoría de las actividades cotidianas, Miró Llinares explica que en este entorno se reproducen los elementos del triángulo del delito que son el agresor motivado, el objetivo vulnerable y la ausencia de guardianes capaces. Por lo tanto, esta estructura convierte a Internet en un espacio propicio para el surgimiento de conductas ilícitas, donde la prevención debe orientarse a la reducción de oportunidades mediante estrategias situacionales y al refuerzo del papel activo de las potenciales víctimas (Miró, 2012, pp. 161-194).

En este contexto, los bienes jurídicos afectados adquieren una dimensión distinta respecto de los delitos convencionales. Entre los más relevantes se encuentran la información, la privacidad, la seguridad de los sistemas informáticos y, en un plano más amplio, la confianza en el entorno digital. De hecho, Miró (2012) resalta que la información y la confianza en el entorno digital representan los fundamentos esenciales que se ven afectados por la comisión de ciberdelitos, ya que de ellos depende tanto la estabilidad de los sistemas informáticos como la legitimidad de las relaciones sociales y económicas que se desarrollan en línea destacando que el daño derivado de estos delitos no siempre se traduce en pérdidas económicas directas, sino que se manifiesta en la erosión de la seguridad en los sistemas y en el debilitamiento de la percepción de fiabilidad de

las redes digitales. Así, la afectación de la confianza colectiva no solo mina el funcionamiento de la sociedad de la información, sino que también compromete la legitimidad de la economía digital y, con ello, la estabilidad de las relaciones jurídicas y sociales que dependen de la tecnología.

1.1.1 Información

La información constituye uno de los bienes jurídicos más sensibles en el ámbito digital, hoy en día es considerada un recurso estratégico no solo para las personas, sino también para las organizaciones y los Estados. Su importancia es tal que puede equipararse a un activo patrimonial material, pues la manipulación, alteración, sustracción o eliminación ilícita de datos produce perjuicios comparables a los que ocasiona la pérdida de bienes físicos.

En este sentido, Villavicencio (2014) Se señala que la información no debe concebirse de forma aislada, sino como parte de un sistema de valores interrelacionados. Por un lado, comprende los datos que son almacenados, procesados y transmitidos mediante sistemas automatizados; y por otro, involucra bienes jurídicos que pueden resultar afectados a través de ella, como la intimidad, la integridad sexual o la seguridad en las comunicaciones. Esto evidencia que la información supera el ámbito meramente económico, constituyéndose en un componente esencial de la autonomía, la dignidad y la identidad personal.

En consecuencia, proteger la información supone preservar su confidencialidad, integridad y autenticidad, ya que en ella descansa gran parte del aspecto probatorio en la sociedad actual. Por ello, los delitos informáticos pueden impactar de manera simultánea en distintos bienes, vulnerando la intimidad cuando invaden la esfera privada de los individuos y dañan la seguridad jurídica al falsificar documentos o manipular pruebas digitales.

1.1.2 Privacidad

En un contexto donde gran parte de la vida cotidiana transcurre en línea, la intimidad de los individuos se encuentra expuesta de manera constante a accesos no autorizados, vigilancia ilícita o difusión indebida de información personal. Este derecho, adquiere en el entorno digital una nueva dimensión, ya que, no se limita a proteger espacios físicos privados, sino que abarca el

resguardo de correos electrónicos, mensajes instantáneos, historiales de búsqueda, datos médicos y financieros, así como cualquier otra información que defina la vida personal.

En esa línea, Acurio (2003) advierte que la expansión de Internet ha generado nuevos riesgos que amenazan la privacidad de millones de usuarios, dado que la información que circula en el entorno digital puede ser manipulada o empleada con propósitos ilícitos. Entre estos riesgos se incluyen el seguimiento de la actividad en redes sociales para crear perfiles comerciales o delictivos, el espionaje informático con fines políticos y la compraventa de bases de datos sin la autorización de sus titulares. Además, la privacidad digital no solo se vincula con el derecho a mantener en reserva la vida personal, sino también con la libertad de decisión. La filtración de datos sensibles puede generar chantajes, discriminación o limitaciones en el acceso a servicios. Por ejemplo, cuando una empresa de seguros accede sin autorización a la información médica de un cliente, puede negarle una cobertura o imponerle condiciones abusivas. En este sentido, proteger la privacidad significa también garantizar que las personas conserven el control sobre su propia información y sobre la forma en que esta se comparte o utiliza.

De igual modo, debe destacarse que la vulneración de la privacidad en el entorno digital tiene un efecto multiplicador, pues la información personal robada puede difundirse de manera masiva e inmediata, escapando al control del afectado y generando un daño prácticamente irreparable, convirtiendo a la privacidad en un bien jurídico particularmente frágil, cuya protección requiere mecanismos normativos y tecnológicos sólidos.

1.1.3 Confianza en el entorno digital

La economía electrónica, las transacciones comerciales y la interacción social en línea dependen de que los usuarios perciban que sus derechos serán respetados y que los sistemas son seguros. Cada ataque informático, fraude electrónico o filtración de datos erosiona esa confianza colectiva, debilitando la credibilidad de las instituciones y frenando la innovación tecnológica.

Como advierte Acurio (2003), Detrás de la afectación a bienes jurídicos individuales se encuentra, además, un daño social de mayor envergadura: la

pérdida de confianza en el correcto funcionamiento de los sistemas informáticos. En tal sentido, no se trata únicamente de la lesión de intereses particulares, sino del deterioro de un valor colectivo fundamental que sustenta la cohesión y el dinamismo de la vida digital contemporánea. Cuando se produce una vulneración de estas estructuras, las consecuencias no solo impactan a individuos o empresas, sino también a la colectividad, especialmente si se trata de infraestructuras críticas como servicios financieros, telecomunicaciones, sanidad o seguridad pública.

En esta perspectiva, la Convención de Budapest sobre Ciberdelincuencia (2001) resalta que la protección de los sistemas y datos informáticos constituye un objetivo esencial dentro de la cooperación internacional frente a la criminalidad digital, en tanto su estabilidad resulta indispensable para el funcionamiento seguro de los servicios esenciales en la sociedad contemporánea.

2. Características de los delitos cibernéticos

La ciberdelincuencia se configura como un fenómeno con rasgos propios que la distinguen radicalmente de la criminalidad tradicional, razón por la cual requiere un análisis diferenciado en el ámbito jurídico, criminológico y tecnológico. No se trata únicamente de un traslado de conductas ilícitas clásicas al espacio digital, sino de un entorno que transforma de manera sustancial la forma en que los delitos se conciben, se cometen y se investigan.

Las características de los delitos cibernéticos se encuentran directamente relacionadas con el medio en el que se desarrollan: el ciberespacio. Este ámbito carece de fronteras físicas o geográficas, lo que genera un entorno descentralizado y global en el cual los actos ilícitos pueden perpetrarse desde cualquier lugar y en cualquier momento. En contraste con el delito común, cuya comisión suele estar delimitada territorialmente, el cibercrimen se distingue por la deslocalización de sus acciones y por la simultaneidad de sus efectos, que pueden afectar a múltiples jurisdicciones al mismo tiempo.

En este contexto, la doctrina criminológica ha elaborado clasificaciones que permiten comprender la diversidad de delitos cometidos en entornos digitales. Así, Miró (2012) suele distinguir entre tres tipos de ciberataques: los puros, referidos a acciones técnicas directas contra sistemas informáticos (como el

hacking, el empleo de malware o los ataques de denegación de servicio); los mixtos o de réplica, que implican el aprovechamiento de medios digitales para cometer delitos tradicionales como el fraude electrónico, el phishing o la ciberextorsión; y los de contenido, relacionados con la difusión ilícita de información o materiales en línea, tales como la vulneración de derechos de autor, la pornografía infantil o los discursos de odio. Asimismo, algunos autores proponen una clasificación adicional basada en la finalidad del ataque, distinguiendo entre motivaciones económicas, sociales o políticas. En conjunto, estas categorías permiten comprender que el cibercrimen no es un fenómeno uniforme, sino un conjunto de conductas en constante transformación, condicionado tanto por la evolución tecnológica como por los usos sociales de la red.

Además, la ciberdelincuencia se caracteriza por su rapidez de ejecución y alcance masivo debido a que un solo ataque informático puede afectar a millones de usuarios en cuestión de segundos, lo que convierte al cibercrimen en un fenómeno de escala global. Esta capacidad multiplicadora no solo incrementa los daños patrimoniales, sino que también amplifica la afectación a bienes jurídicos intangibles como la intimidad, la seguridad informática y la confianza en el entorno digital.

Otro rasgo distintivo es la invisibilidad de la conducta delictiva porque a diferencia de un robo, una agresión o un fraude presencial, en el ciberespacio los agentes del ilícito pueden pasar desapercibidos durante largos periodos de tiempo. Muchas veces, la víctima desconoce quien ha sido el infractor de un ataque debido al anonimato del mismo por las técnicas de ocultamiento en el espacio digital. Asimismo, otro rasgo distintivo es la invisibilidad de la conducta delictiva, porque, a diferencia de un robo, una agresión o un fraude presencial, en el ciberespacio los agentes del ilícito pueden pasar desapercibidos durante largos periodos de tiempo. De hecho, muchas veces la víctima desconoce quién ha sido el infractor de un ataque debido al anonimato que posibilitan las técnicas de ocultamiento en el espacio digital. En esta línea, Miró Llinares (2012) explica de manera detallada ciertas características distintivas de los delitos informáticos, entre ellas el anonimato, la deslocalización y la transnacionalidad. Señala que el anonimato complica la identificación de los responsables, la deslocalización hace

posible agredir a las víctimas sin necesidad de presencia física y desde distintos puntos del planeta, mientras que la transnacionalidad genera problemas de competencia entre jurisdicciones, lo cual dificulta la investigación y sanción penal de estas conductas. Otro punto que debe subrayarse es que la estructura global de internet permite que un ciberdelincuente ubicado en un país ataque a víctimas situadas en otro, utilizando servidores alojados en un tercero, lo que genera serios problemas de jurisdicción y competencia judicial. Esta particularidad ha sido destacada por la Convención de Budapest sobre Ciberdelincuencia (2001), al señalar que la cooperación internacional constituye una herramienta imprescindible para enfrentar eficazmente estas conductas.

En paralelo, otra característica fundamental es la mutabilidad tecnológica. La ciberdelincuencia evoluciona al mismo ritmo que las innovaciones tecnológicas. Cada nuevo avance en materia de inteligencia artificial, sistemas de pago electrónico, redes sociales o internet de las cosas abre nuevas posibilidades para la comisión de ilícitos. Esto genera un desfase entre el desarrollo tecnológico y la capacidad legislativa para tipificar adecuadamente los delitos, lo que da lugar a vacíos normativos que los ciberdelinquentes aprovechan estratégicamente.

En síntesis, estas características complejizan la persecución penal y demandan cooperación internacional, actualización normativa constante y un enfoque interdisciplinario que combine derecho, informática y ciberseguridad.

2.1. Dependencia tecnológica de la víctima

Un rasgo distintivo de los delitos cibernéticos, en comparación con la criminalidad tradicional, es la dependencia tecnológica de la víctima, la cual incrementa de manera significativa su exposición a riesgos. En esa línea, Miró (2012) destaca la importancia que tiene el comportamiento del propio usuario en la materialización del cibercrimen. En numerosos casos, no es la complejidad técnica del atacante lo que posibilita la infracción, sino las acciones negligentes de la víctima, como emplear contraseñas poco seguras, realizar descargas sin verificación o proporcionar datos personales de manera imprudente. Así, la víctima deja de ocupar un rol pasivo y pasa a ser un agente activo, cuya forma de interactuar en el entorno digital influye directamente en la consumación del delito. Por ello, la prevención no debe limitarse a estrategias punitivas, sino incluir también la formación en competencias digitales y el fomento de una cultura de

ciberseguridad. A diferencia de los delitos convencionales, en los cuales la vulnerabilidad suele estar determinada por factores físicos o situacionales, en el ciberespacio la fragilidad se encuentra principalmente asociada al grado de confianza que los individuos depositan en los sistemas tecnológicos y, además, a los hábitos de autoprotección digital que decidan adoptar.

Como advierte Miró Llinares (2012) en numerosos casos, no es la pericia tecnológica del agresor la que permite la comisión del delito, sino más bien los fallos o conductas poco seguras del propio usuario. En ese sentido, el comportamiento de la víctima adquiere un papel determinante dentro del desarrollo del cibercrimen, ya que basta una acción mínima —como hacer clic en un enlace engañoso, descargar un programa infectado o compartir información personal en entornos poco confiables— para generar una vulnerabilidad. Este planteamiento, acorde con la victimología situacional, evidencia que la ocurrencia del hecho delictivo no depende únicamente de la habilidad del infractor, sino también de la interacción entre sus acciones y las rutinas digitales de la víctima.

En la práctica, esta dependencia tecnológica se traduce en que el nivel de riesgo de una persona o institución está estrechamente vinculado con su manera de interactuar con las tecnologías. Una víctima que emplea contraseñas débiles, que reutiliza claves en múltiples plataformas o que no actualiza sus sistemas operativos se convierte en un objetivo más atractivo y accesible para el delincuente. Numerosos ciberataques no se producen por fallos estructurales en sus sistemas de ciberseguridad, sino por la explotación de errores humanos, como el descuido de un empleado que abre un correo de phishing o que conecta un dispositivo externo infectado a la red corporativa.

Por otra parte, la confianza excesiva en dispositivos digitales como son los teléfonos móviles, aplicaciones financieras o servicios en la nube genera una percepción errónea de seguridad que contribuye a aumentar el riesgo. Muchos usuarios asumen que sus plataformas son intrínsecamente seguras, sin considerar que el desarrollo acelerado de nuevas tecnologías siempre trae consigo vulnerabilidades aún no detectadas. En consecuencia, cuanto más confían las personas en la tecnología, mayor es la exposición a ataques que explotan precisamente esa confianza.

En conclusión, la dependencia tecnológica de la víctima constituye una característica central de los delitos cibernéticos, ya que condiciona la forma en que los ataques se ejecutan y las posibilidades de éxito del infractor. A mayor grado de confianza ciega en plataformas y dispositivos, sin acompañarla de conductas preventivas, mayor será la vulnerabilidad de la víctima. De allí que la política criminal frente al cibercrimen deba incorporar estrategias de educación digital, concienciación ciudadana y cultura de la ciberseguridad, reconociendo que la víctima no es un agente pasivo, sino un actor cuya conducta influye directamente en la dinámica delictiva. La dependencia tecnológica, por tanto, vincula el perfil de la víctima con las posibilidades de ataque en cuanto a mayor confianza en plataformas o dispositivos sin precaución, mayor la vulnerabilidad.

2.2 Ejecución a distancia y deslocalización del delito

Una de las características más relevantes de los delitos cibernéticos es que pueden ejecutarse a distancia, sin necesidad de contacto físico con la víctima ni de presencia en el lugar donde se produce el daño. El infractor puede encontrarse en un país distinto al de la víctima, al del servidor que aloja la información comprometida o incluso al de la institución financiera afectada. Como destaca el Banco Interamericano de Desarrollo (BID, 2020), la naturaleza sin fronteras del ciberespacio demanda una cooperación regional sólida para responder eficazmente al crimen organizado informático antes de que sus ataques escalen fuera de control. Esta deslocalización genera enormes dificultades para la investigación, puesto que la obtención de pruebas digitales requiere en muchos casos de asistencia mutua entre Estados.

2.3 Anonimato y técnicas de ocultamiento

En el entorno digital, los infractores cuentan con múltiples herramientas para ocultar su identidad, desde el uso de direcciones IP falsas hasta la creación de perfiles ficticios y cuentas desechables. Estrada (2024) señala que todo dispositivo que accede a internet posee un identificador exclusivo, denominado dirección IP; no obstante, existen múltiples mecanismos que permiten ocultar o falsificar dicha dirección, generando la apariencia de una conexión desde una ubicación diferente. Esta posibilidad de enmascarar el origen real de la actividad digital favorece el anonimato de los ciberdelincuentes y representa un reto considerable para las autoridades encargadas de investigar y sancionar los

delitos cometidos en el entorno virtual. Esta invisibilidad del delincuente dificulta la imputación de responsabilidades penales, puesto que muchas veces los rastros digitales son efímeros o deliberadamente enmascarados, representando uno de los principales obstáculos para los operadores de justicia. Así como señala Cerezo (2020) Cabe destacar que la proporción de ciberdelitos esclarecidos ha disminuido con el paso del tiempo, pues mientras en el año 2011 se lograba resolver aproximadamente el 36% de los casos, para el 2018 dicha cifra se redujo a cerca del 22%. Asimismo, los delitos de naturaleza social, tales como amenazas, coacciones o vulneraciones al honor, presentan mayores niveles de resolución (entre el 50% y 80%), en contraste con los delitos de índole económica, como el fraude informático, cuya complejidad técnica y carácter transnacional dificultan significativamente su investigación y persecución penal.

2.4 Transnacionalidad y desafíos jurisdiccionales

Los delitos cibernéticos tienen un marcado carácter transnacional. Un ataque informático puede originarse en un país, afectar servidores en otro y perjudicar a víctimas en múltiples jurisdicciones de manera simultánea. La Convención de Budapest sobre Ciberdelincuencia (2001) ya advertía que “la naturaleza global de las redes hace indispensable una cooperación internacional rápida y eficaz, pues de otro modo los delitos quedarían impunes”. En ese sentido, la transnacionalidad plantea retos jurídicos considerables como son los conflictos de competencia entre tribunales, divergencias legislativas sobre la tipificación de ciertas conductas y lentitud en los mecanismos de asistencia judicial mutua. Sobre el presente, Miró Llinares (2012, pp. 200-210) subraya que una de las principales dificultades de la persecución penal en el ciberespacio es la falta de armonización normativa entre países. La naturaleza transnacional de los ataques obliga a fortalecer la cooperación internacional y a avanzar hacia reformas legislativas que garanticen la eficacia de la respuesta penal. Por tanto, sin coordinación global, gran parte de los delitos cometidos en línea queda en la impunidad.

2.5 Escalabilidad y automatización de los ataques

A diferencia del delito tradicional, donde el impacto está limitado por la capacidad del autor, en el cibercrimen un solo atacante puede comprometer miles de sistemas en simultáneo. Según un informe reciente de BASC (2025), se observa

una creciente automatización del delito cuando se utilizan herramientas como inteligencia artificial, bots o malware como servicio, para escalar estafas y fraudes con una velocidad sin precedentes. A diferencia de la criminalidad común, donde el daño suele ser proporcional al número de acciones realizadas, en el cibercrimen un solo atacante puede afectar simultáneamente a miles o millones de usuarios convirtiendo al cibercrimen en un fenómeno de alto impacto social y económico.

3. La extorsión digital como delito cibernético emergente

La extorsión ha sido históricamente entendida como un delito de carácter intimidatorio, en el cual el agresor constriñe la voluntad de la víctima para obtener un beneficio económico. Tradicionalmente, esta conducta se manifestaba en escenarios físicos como amenazas directas, cobro de cupos o presiones realizadas de manera personal. Sin embargo, el avance de las tecnologías de la información y comunicación ha permitido que este fenómeno migre hacia el ciberespacio, convirtiéndose en una de las formas más recientes y preocupantes de la ciberdelincuencia.

En este nuevo contexto, la extorsión digital se configura cuando el sujeto activo se vale de medios tecnológicos como correos electrónicos, redes sociales, aplicaciones móviles o programas maliciosos para intimidar a la víctima y exigirle una contraprestación económica. Tal como sostiene Miró, el ciberespacio se ha transformado en un “nuevo ámbito de oportunidad delictiva”, donde se reproducen las condiciones que facilitan la comisión de delitos como la extorsión (2012). Esta realidad marca la diferencia con la modalidad tradicional porque el delincuente ya no requiere presencia física, sino que puede actuar desde el anonimato, incluso desde otra jurisdicción, lo que dificulta su identificación y persecución. Es por ello que si antes, el objeto de la amenaza antes recaía sobre la integridad personal o los bienes materiales, hoy se dirige hacia los datos, archivos y sistemas digitales de la víctima. En esta línea, el Instituto Nacional de Ciberseguridad de España (INCIBE) advierte que modalidades como el ransomware o la sextorsión utilizan la retención de información y la amenaza de difusión de contenido íntimo como principales instrumentos de coacción (INCIBE, 2023) mostrando cómo la creciente dependencia tecnológica amplifica el poder del agresor.

Entonces, mientras la extorsión tradicional se dirigía a una víctima concreta en un lugar determinado, la extorsión digital puede afectar a cientos o miles de personas de manera simultánea mediante campañas automatizadas. Cerezo y García (2020) señalan que los ciberdelitos de carácter económico, entre los cuales se inserta la extorsión digital, han experimentado un crecimiento exponencial en los últimos años, en gran parte debido a la facilidad de su difusión y a la dificultad de esclarecimiento.

Un ejemplo claro de esta transformación es el fenómeno del “gota a gota digital”, donde prácticas extorsivas vinculadas al préstamo usurario tradicional se trasladan al espacio virtual a través de aplicaciones móviles. De este modo, lo que en un inicio requería contacto personal y presencia física se ha convertido en un hostigamiento permanente ejercido mediante la tecnología, lo cual confirma el carácter emergente de la extorsión digital como modalidad delictiva cibernética.

3.1 Evolución jurídica y tecnológica de la ciberextorsión

La extorsión digital no surge de la nada, sino que constituye la adaptación de una práctica criminal histórica a los cambios sociales y jurídicos provocados por la digitalización, con la expansión de Internet y la dependencia creciente de las personas y empresas respecto de sus datos, identidad digital y sistemas de comunicación, las formas de extorsión encontraron un nuevo espacio de desarrollo.

En el plano social, este cambio se explica porque la vida cotidiana se ha trasladado en gran parte al ciberespacio, las relaciones personales, laborales y financieras dependen cada vez más de dispositivos móviles, cuentas en línea y aplicaciones. Esto convierte a la información digital en un recurso especialmente valioso y, al mismo tiempo, en una fuente de vulnerabilidad. Como señala Miró (2012), el ciberespacio se ha constituido en un “ámbito de oportunidad delictiva”, donde se reproducen las condiciones que favorecen la aparición de nuevos delitos o la transformación de delitos tradicionales.

En este contexto, el derecho penal se ha visto obligado a responder con reformas normativas que reconozcan las nuevas modalidades de extorsión. A nivel internacional, el Convenio de Budapest sobre ciberdelincuencia (2001) marcó un

punto de partida al establecer estándares comunes para perseguir delitos cometidos mediante sistemas informáticos. Aunque no regula expresamente la ciberextorsión, sí sienta las bases para su persecución como ataque contra la confidencialidad e integridad de datos. En América Latina, algunos países han comenzado a incorporar de forma más clara estas modalidades digitales dentro de sus códigos penales. Perú, por ejemplo, aprobó en 2024 la Ley N.º 32183, que modificó el artículo 200 del Código Penal añadiendo a la ley 30096

para reconocer supuestos de “préstamos informáticos extorsivos”, vinculados al fenómeno del “gota a gota digital”, donde el medio tecnológico se convierte en la herramienta principal del delito.

La evolución tecnológica también ha aportado nuevas formas de coacción, inicialmente, la ciberextorsión se ejercía mediante amenazas directas por correo electrónico o mensajes, pero posteriormente se incorporaron herramientas como el ransomware, que bloquea archivos de la víctima hasta obtener un pago. El Instituto Nacional de Ciberseguridad de España (INCIBE) advierte que esta modalidad ha evolucionado hacia la doble extorsión, en la que además de cifrar la información, se amenaza con divulgarla públicamente, aumentando el poder intimidatorio (INCIBE, 2023).

3.2 Diferencias con la extorsión tradicional

Aunque la extorsión digital mantiene el mismo núcleo típico que la tradicional, que es la exigencia de una prestación bajo amenaza, presenta diferencias significativas derivadas del uso de medios tecnológicos. La primera de ellas está en el objeto de la amenaza porque mientras que en la extorsión clásica lo usual era amenazar con causar daño físico a la víctima o a sus bienes, en la digital la intimidación se dirige contra bienes intangibles como la información personal, las credenciales de acceso o la reputación en línea. El Instituto Nacional de Ciberseguridad de España (INCIBE) explica que modalidades como la sextorsión se apoyan en la posesión de imágenes privadas para presionar a la víctima, mientras que el ransomware se centra en el acceso a datos esenciales (INCIBE, 2023).

Además, en la extorsión tradicional, la cercanía territorial y el contacto directo eran características habituales, en cambio, la extorsión digital se realiza de

manera remota y anónima, lo que dificulta la identificación del agresor. Como señala Miró (2012), el ciberespacio ha generado un escenario donde los delincuentes pueden actuar desde cualquier lugar, reduciendo los riesgos de ser capturados gracias al anonimato y la transnacionalidad de Internet. En tercer lugar, la extorsión tradicional solía dirigirse a una persona o grupo reducido, mientras que la digital puede afectar a cientos o miles de víctimas simultáneamente mediante correos masivos, campañas automatizadas o aplicaciones fraudulentas. En este sentido, Cerezo y García (2020) destacan que el auge de los ciberdelitos económicos se debe en gran medida a la facilidad con que los delincuentes pueden replicar sus acciones en múltiples objetivos, lo que incrementa la incidencia y dificulta su persecución.

Otra diferencia importante es que, en la extorsión tradicional, la prueba suele basarse en testimonios, grabaciones o evidencias físicas. En cambio, en la digital la investigación requiere de evidencia electrónica (registros de conexión, direcciones IP, transacciones en criptomonedas), lo que exige conocimientos técnicos avanzados y cooperación internacional. El Convenio de Budapest sobre ciberdelincuencia (2001) y su Protocolo adicional sobre obtención de pruebas electrónicas son reflejo de esta necesidad de adaptación jurídica frente a los retos de la extorsión digital.

Finalmente, la extorsión digital no se limita a obtener dinero, sino que puede afectar la privacidad, la reputación e incluso la estabilidad de empresas o instituciones. La amenaza de difundir información personal o empresarial tiene efectos sociales y psicológicos que, en muchos casos, superan el alcance de la extorsión tradicional.

3.3 Impacto criminológico y social de la extorsión digital

La extorsión digital no puede analizarse únicamente desde su dimensión técnica o jurídica, pues también tiene un profundo impacto criminológico y social que la convierte en un fenómeno especialmente preocupante dentro de la ciberdelincuencia contemporánea. A diferencia de la extorsión tradicional, que se limitaba a contextos físicos y territoriales específicos, la modalidad digital afecta simultáneamente a individuos, familias, empresas e incluso a instituciones estatales, generando un daño que trasciende lo estrictamente patrimonial.

En el plano criminológico, Miró (2012) sostiene que el ciberespacio amplifica las oportunidades delictivas al ofrecer a los agresores un escenario global, anónimo y con barreras mínimas de acceso, lo que incrementa la frecuencia de delitos como la extorsión y reduce el riesgo de ser descubierto. Esta situación genera un desequilibrio estructural, mientras el delincuente actúa protegido por el anonimato, la víctima queda en una posición de indefensión, sometida a una amenaza que puede extenderse a escala mundial en cuestión de segundos. El resultado es un nuevo modelo de criminalidad, menos localizado y más difuso, que erosiona las fronteras clásicas del derecho penal.

En el plano individual, el impacto psicológico de la ciberextorsión es uno de sus rasgos más graves. Las víctimas de sextorsión, por ejemplo, no solo enfrentan la pérdida de dinero, sino también un profundo daño emocional derivado de la exposición de su intimidad. El Instituto Nacional de Ciberseguridad de España (INCIBE) advierte que este tipo de prácticas provoca sentimientos de culpa, ansiedad, miedo y estigmatización social, lo cual puede desembocar en cuadros de depresión e incluso en conductas suicidas (INCIBE, 2023).

En el plano familiar y comunitario, los efectos de la ciberextorsión también son notorios porque la amenaza digital, al no tener límites geográficos, puede extenderse a los contactos de la víctima, afectando la confianza en las relaciones sociales. Un caso paradigmático son las extorsiones mediante aplicaciones de préstamos informales “gota a gota digital”, en las que los delincuentes amenazan con difundir mensajes difamatorios o imágenes manipuladas a familiares, vecinos o compañeros de trabajo. Esto genera un clima de miedo colectivo y deteriora la cohesión social, al exponer no solo a la víctima directa sino también a su entorno cercano.

Los ataques de ransomware y las amenazas de filtración de datos pueden paralizar por completo las operaciones de una empresa, Cerezo y García (2020) destacan que este tipo de ciberdelitos ha alcanzado una de las tasas más altas de incidencia en España, llegando incluso a superar a los delitos tradicionales como el robo con violencia. Asimismo, advierten que los índices de esclarecimiento resultan particularmente bajos, principalmente debido a la complejidad técnica de las investigaciones y al carácter transnacional de las conductas. Estas circunstancias no solo generan pérdidas económicas directas

—como el pago de rescates—, sino también afectaciones colaterales, entre las que se incluyen sanciones por vulneración de normas de protección de datos, disminución de la clientela y deterioro de la imagen institucional o empresarial.

Desde un punto de vista social más amplio, la percepción de que cualquier dato personal o empresarial puede ser utilizado como herramienta de chantaje genera un efecto inhibitorio en la adopción de nuevas tecnologías. Ello repercute en el desarrollo económico y en la innovación, pues tanto ciudadanos como organizaciones pueden mostrarse reacios a digitalizar sus procesos por temor a convertirse en víctimas. En términos criminológicos, este fenómeno alimenta una sensación de inseguridad difusa, que no se limita a quienes sufren directamente el delito, sino que alcanza a toda la sociedad.

Finalmente, debe destacarse que el impacto de la extorsión digital es multidimensional abarcando lo psicológico, lo económico, lo social y lo cultural. Al amenazar la intimidad, la reputación y la estabilidad de las personas y organizaciones, la ciberextorsión se convierte en un delito que desborda los límites tradicionales de la criminalidad patrimonial. Esta amplitud de efectos explica por qué debe ser considerada no solo como una manifestación más de la extorsión clásica, sino como un delito cibernético emergente con consecuencias propias, que exige nuevas estrategias de prevención, asistencia a las víctimas y adaptación normativa constante.

4. Marco normativo nacional aplicable

La regulación de la ciberdelincuencia en el Perú se encuentra en proceso de constante adaptación, buscando responder a los cambios sociales y tecnológicos que generan nuevas modalidades de criminalidad. La extorsión digital y, en particular, el fenómeno del “gota a gota digital”, evidencian los vacíos normativos que aún persisten, así como los avances recientes que reflejan el esfuerzo del legislador por incorporar estas conductas en el Código Penal y en leyes especiales.

En líneas generales, el marco jurídico nacional se sostiene en las disposiciones del Código Penal peruano, en especial el artículo 200 sobre extorsión, el artículo 151 sobre coacción, el artículo 196 sobre estafa, los artículos incorporados mediante reformas para atender a los delitos informáticos; la Ley N.º 30096, Ley

de Delitos Informáticos (2013) y sus modificaciones posteriores, y las reformas recientes, entre ellas la Ley N.° 32183 de 2024, que introduce nuevas modalidades agravadas de extorsión vinculadas al uso de medios digitales.

Este conjunto de normas refleja una evolución progresiva, de una regulación pensada para delitos informáticos clásicos hacia una tipificación más específica de la extorsión digital, vinculada a contextos de criminalidad organizada y préstamos informales realizados mediante aplicaciones móviles.

4.1 El artículo 200 del Código Penal y la tipificación de la extorsión

El artículo 200 del Código Penal peruano define con claridad el delito de extorsión: “quien, mediante violencia o amenaza, somete a una persona o institución para obtener una ventaja indebida puede ser sancionado con una pena privativa de libertad que oscila entre diez y quince años.” Dicho tipo incluye una modalidad agravada que castiga con pena similar o mayor a quien comete el delito para perturbar el funcionamiento de servicios o infraestructuras públicas, consolidando así su capacidad para abordar situaciones convencionales de violencia o coacción indirecta.

Desde un enfoque doctrinal, Galván (2024) ofrece una visión crítica respecto a la evolución legislativa del artículo, señalando que entre los años 2001 y 2023 fue objeto de ocho modificaciones, orientadas principalmente a incrementar las sanciones, tipificar nuevas formas delictivas y establecer agravantes específicas. Sin embargo, Galván Ramos considera que dichas reformas no han producido un impacto real en la reducción de los casos de extorsión, ya que han operado más como una respuesta simbólica o “placebo punitivo”, antes que como un mecanismo efectivo de prevención o disuasión en el ámbito social.

Desde una perspectiva analítica, esto refleja una tensión persistente: por un lado, está la intención clara del legislador de ajustar el marco penal a realidades criminales en transformación; por otro lado, la persistencia del delito pese al endurecimiento refleja que la eficacia de una norma no depende únicamente de su severidad, sino también de su capacidad operativa en contextos reales de investigación y persecución penal. La aplicación del artículo 200 enfrenta, además, desafíos específicos relacionados con la sofisticación del mundo digital porque las amenazas ya no requieren presencia ni contacto físico, lo cual hace

que el tipo legal tradicional, pensado para contextos de coacción directa, resulte incompleto frente a la extorsión digital.

Asimismo, el enfoque legal tradicional presupone la existencia de una amenaza explícita o conducta violenta claramente reconocible, lo que dificulta tipificar adecuadamente formas más sutiles o indirectas de extorsión en línea, tales como campañas de hostigamiento sistemático, difusión masiva de datos privados, chantajes mediante redes sociales o amenazas mediadas por plataformas tecnológicas. Esta situación genera incertidumbre en operadores judiciales y fiscales, quienes deben recurrir a figuras generales de amenaza para encuadrar estas conductas, lo que puede resultar en una respuesta penal fragmentada o imprecisa.

De esta manera, aunque el artículo 200 sigue siendo la piedra angular de la represión delictiva por extorsión, su eficacia en contextos digitales está condicionada por su falta de adaptación conceptual al ciberespacio. Su efectividad futura dependerá de una adecuada interpretación doctrinal que contemple el medio tecnológico como parte del contexto delictivo y, eventualmente, de la formulación de un tipo específico de extorsión digital, que reconozca el uso de medios virtuales como elemento fundamental del delito.

4.2 La Ley N.º 30096, Ley de Delitos Informáticos

Promulgada el 22 de octubre de 2013, la Ley N.º 30096, conocida como Ley de Delitos Informáticos, marcó un antes y después en el derecho penal peruano, al convertirse en la primera norma integral destinada a sancionar delitos cometidos mediante el uso de tecnologías de la información. Su propósito fue prevenir y sancionar conductas ilícitas como el acceso no autorizado a sistemas, daño informático, interceptación de datos, fraude electrónico, suplantación de identidad y tráfico de contraseñas, conforme a los principios del Convenio de Budapest sobre Ciberdelincuencia (2001), al que el Perú se alineó legal y operativamente. (Defensoría del Pueblo, 2023, p. 24)

A pesar de su relevancia normativa, esta ley ha recibido observaciones críticas. El jurista Villavicencio (2014) señala que, aunque la norma construyó un marco penal alineado con estándares internacionales y estructuró una tipología clara de ciberdelitos, su alcance resultó limitado al ámbito de los delitos informáticos

“puros”, dejando sin abordar adecuadamente las modalidades “impuros”, aquellas en que la tecnología es un instrumento para cometer delitos clásicos, como la estafa o la extorsión digital.

Esta crítica resulta especialmente relevante, pues los delitos informáticos puros son aquellos que solo pueden cometerse dentro del entorno tecnológico, como el hacking, el sabotaje informático, la interceptación de comunicaciones digitales o la creación de programas maliciosos. La Ley 30096 tipificó con claridad estas conductas, reflejando una respuesta adecuada al entonces incipiente riesgo de intrusión y daño a los sistemas informáticos.

En cambio, los delitos informáticos impuros son aquellos que, aunque ya existían en la criminalidad tradicional (fraude, amenazas, extorsión), encuentran en la tecnología un medio facilitador y multiplicador. En este ámbito, la Ley 30096 mostró debilidades, pues no estableció figuras específicas para conductas en las que el núcleo delictivo es clásico, pero el medio digital cambia radicalmente su alcance y eficacia. Casos como la extorsión digital, el fraude electrónico masivo o el “gota a gota digital” quedaron fuera del foco de la ley, obligando a fiscales y jueces a encuadrar estos hechos en tipos penales tradicionales que no siempre captan la complejidad de las nuevas dinámicas criminales.

La consecuencia práctica de esta omisión ha sido la fragmentación en la persecución penal. Mientras que los delitos “puros” cuentan con artículos específicos en la Ley 30096, los “impuros” deben ser procesados recurriendo a normas generales del Código Penal, como el artículo 200 sobre extorsión o el artículo 196 sobre estafa, sin considerar que el uso de la tecnología añade un plus de lesividad y dificultad investigativa. De este modo, las modalidades más frecuentes en la vida cotidiana, las que afectan a ciudadanos a través de redes sociales, mensajería o aplicaciones móviles, no reciben un tratamiento legal diferenciado, a pesar de su fuerte impacto criminológico y social.

Por ello, la crítica de Villavicencio pone en evidencia que el problema central de la Ley 30096 no es lo que incluyó, sino lo que dejó fuera. La excesiva concentración en los delitos informáticos “puros” provocó que el legislador peruano no advirtiera la necesidad de tipificar con mayor precisión aquellos delitos híbridos, donde la tecnología no es el fin en sí misma, sino un instrumento decisivo para potenciar la coacción, el engaño o la intimidación. En este punto,

el vacío normativo es evidente frente a fenómenos contemporáneos como la sextorsión, la ciberextorsión financiera o las estafas mediante phishing, que constituyen la forma en que la mayoría de ciudadanos experimenta la ciberdelincuencia.

4.3 La Ley N.º 32183 (2024): reconocimiento expreso de la extorsión digital

La Ley N.º 32183, promulgada en diciembre de 2024, representa un avance crucial en la regulación penal peruana, ya que incorpora expresamente la modalidad de préstamos extorsivos digitales dentro del tipo penal de extorsión. Esta reforma adapta el artículo 200 del Código Penal, basado en el Decreto Legislativo 635, al considerar como delito habitualmente tipificado lo que se conoce en la práctica como “gota a gota digital”, una forma de presión económica ejercida mediante aplicaciones móviles u otros medios análogos.

La Ley incorpora el literal 200.2 al artículo 200, estableciendo que se sanciona igualmente a quien, "mediante amenaza, intimidación, engaño, ardid o violencia, induce u obliga a aceptar dinero o bienes que simulan un contrato de mutuo o cualquier otro", ampliando así la definición clásica del delito de extorsión para incluir conductas implícitas en préstamos fraudulentos digitales. Se establece una pena privativa de libertad no menor de diez ni mayor de quince años para estos casos, igualando el tratamiento sancionador con la extorsión tradicional.

Asimismo, se modifica la Ley de Delitos Informáticos (Ley N.º 30096) incorporando el artículo 8-A, que define el “préstamo informático extorsivo” como aquel realizado a través de plataformas digitales o Internet que induce o obliga mediante engaño o amenaza a aceptar un préstamo simulado con el propósito de obtener una ventaja indebida. La pena para este delito también se establece entre diez y quince años de prisión.

La norma contempla, además, circunstancias agravantes que elevan la pena hasta veinticinco años, en casos como el empleo de violencia, si la víctima es menor, adulto mayor, persona con discapacidad o en situación de vulnerabilidad que son agravantes que apuntan a proteger a los sectores sociales más expuestos a este tipo de delitos digitales.

Este reconocimiento explícito al fenómeno del gota a gota digital tiene un impacto político y social importante. Como señaló la congresista Norma Yarrow,

impulsora de la norma, el objetivo principal es "proporcionar protección legal especialmente a la población más vulnerable, que, por necesidad económica, es la que más recurre a este tipo de préstamos que están fuera del sistema financiero formal", reforzando así la seguridad económica de personas como amas de casa, estudiantes, adultos mayores y pequeños comerciantes (Comisión de Justicia del Congreso, 2024)

4.4 Vacíos y desafíos del marco normativo

A pesar de los avances normativos alcanzados con la Ley N.° 30096 y, más recientemente, con la Ley N.° 32183, el marco jurídico peruano aún presenta vacíos significativos y desafíos prácticos frente a la creciente complejidad de la extorsión digital. Estos vacíos se manifiestan en tres niveles: conceptual, operativo y de política pública.

En el plano conceptual, uno de los principales problemas es la ausencia de una definición unitaria y clara de lo que debe entenderse por extorsión digital. Si bien el artículo 200 del Código Penal ha sido ampliado para incorporar los préstamos informáticos extorsivos, ello no implica que todas las modalidades de coacción ejercidas mediante medios tecnológicos estén plenamente tipificadas. Conductas como la sextorsión, las amenazas de difundir información personal en redes sociales o los chantajes mediante correos electrónicos masivos quedan en una zona gris, obligando a los jueces y fiscales a recurrir a interpretaciones extensivas del tipo penal. Tal como advierte Villavicencio (2014), el legislador peruano se ha concentrado en los delitos informáticos “puros” —como el hacking o el sabotaje informático—, dejando sin un tratamiento específico a los delitos “impuros”, es decir, aquellos en los que la tecnología funciona como medio de comisión de figuras tradicionales, como la extorsión. Esta omisión revela que, pese a las reformas, la ley sigue sin captar la complejidad de los fenómenos híbridos.

En el plano operativo, la investigación y persecución de la extorsión digital enfrenta limitaciones técnicas y procedimentales. La obtención y preservación de la prueba electrónica continúa siendo un reto, ya que requiere pericia especializada y coordinación entre diversas instituciones. Además, los delitos digitales suelen tener un carácter transnacional, lo que dificulta la identificación de los responsables y hace necesaria la cooperación internacional. El Perú es

signatario del Convenio de Budapest sobre Ciberdelincuencia (2001), pero la implementación práctica de sus disposiciones aún es limitada, lo que retrasa la respuesta estatal frente a fenómenos como las redes internacionales de ransomware o el uso de criptomonedas en operaciones de ciberextorsión. La brecha entre las normas existentes y las capacidades institucionales en materia de ciberdelincuencia constituye uno de los principales obstáculos para garantizar una persecución penal efectiva (Defensoría del Pueblo, 2023, p. 25).

En el plano de política pública y victimología, el marco normativo actual se concentra principalmente en la sanción del agresor, pero ofrece pocas herramientas orientadas a la protección y asistencia de las víctimas. La ciberextorsión genera efectos psicológicos, económicos y sociales que requieren medidas de apoyo integral, desde asesoría legal y psicológica hasta mecanismos de reparación efectiva. Sin embargo, estas dimensiones están ausentes en la legislación, lo que obliga a las víctimas a enfrentar solas un proceso judicial que muchas veces resulta revictimizante. La victimización secundaria en delitos cometidos en entornos digitales es particularmente grave, pues las víctimas suelen experimentar estigmatización, desconfianza institucional y un fuerte impacto emocional derivado de la exposición pública (Miró, 2012)

Finalmente, es necesario advertir que el marco normativo enfrenta el desafío de mantenerse actualizado frente a la velocidad de la innovación tecnológica. Las aplicaciones móviles, las plataformas financieras alternativas y los sistemas de comunicación encriptada evolucionan con rapidez, generando continuamente nuevas oportunidades para los delincuentes. Frente a ello, el derecho penal corre el riesgo de quedar obsoleto si no adopta un enfoque flexible, dinámico y preventivo. La experiencia comparada en países como Colombia y México demuestra que las reformas legales deben ir acompañadas de campañas de educación digital, protocolos de cooperación con empresas tecnológicas y fortalecimiento de la ciberseguridad institucional para resultar realmente eficaces.

En conclusión, los vacíos y desafíos del marco normativo peruano se expresan en la falta de tipificación integral de la extorsión digital, las dificultades operativas en la obtención de pruebas y cooperación internacional, la escasa atención a las

víctimas y la falta de adaptación constante frente a la innovación tecnológica. Abordar estas carencias no solo requiere más reformas legales, sino también una visión estratégica que combine derecho penal, criminología, victimología y políticas públicas de prevención digital.

5.Marco normativo internacional

El carácter global y transnacional de la ciberdelincuencia ha impulsado la construcción de un marco normativo internacional que permita armonizar legislaciones, facilitar la cooperación judicial y garantizar la persecución de delitos cometidos en entornos digitales, entre ellos la extorsión digital. Dado que estas conductas suelen involucrar a agresores y víctimas ubicados en distintos países, así como a empresas proveedoras de servicios radicadas en múltiples jurisdicciones, la respuesta jurídica nacional resulta insuficiente si no se complementa con instrumentos internacionales de alcance vinculante y con compromisos de cooperación.

En este escenario, el Convenio de Budapest sobre ciberdelincuencia (2001) constituye el instrumento internacional más relevante y pionero en la materia. Adoptado por el Consejo de Europa y abierto a la adhesión de Estados no europeos, busca armonizar las legislaciones penales nacionales, establecer herramientas procesales eficaces y promover la cooperación internacional rápida y directa. Aunque el Convenio no tipifica expresamente la extorsión digital, sus disposiciones sobre acceso ilícito a sistemas, manipulación de datos, fraude informático e interceptación ilegal de comunicaciones ofrecen el sustento jurídico necesario para perseguir conductas que sirven como base a la ciberextorsión. De acuerdo con el propio Consejo de Europa, el tratado se ha convertido en el marco de referencia mundial frente a los delitos informáticos, por la claridad de sus definiciones y la obligatoriedad de la cooperación transfronteriza

A pesar de estos avances, el marco normativo internacional enfrenta desafíos importantes. En primer lugar, la falta de adhesión universal al Convenio de Budapest limita su eficacia, pues algunos Estados clave en el ecosistema digital aún no lo han ratificado. En segundo lugar, la asimetría tecnológica y legislativa entre países desarrollados y en desarrollo genera dificultades para aplicar de manera homogénea los estándares internacionales. Finalmente, la velocidad con que evoluciona la tecnología supera a menudo la capacidad de reacción

normativa, lo que permite que nuevas modalidades de ciberextorsión se expandan más rápido que las reformas legales.

En conclusión, el marco normativo internacional constituye un pilar indispensable para enfrentar la extorsión digital, al proporcionar un lenguaje común, mecanismos de cooperación judicial y estándares procesales mínimos. Sin embargo, su eficacia depende de la voluntad política de los Estados para adherirse e implementar sus disposiciones, así como de la capacidad de mantener una actualización normativa constante frente a los cambios tecnológicos. Solo mediante una respuesta internacional articulada será posible garantizar la protección efectiva de las víctimas y el fortalecimiento de la seguridad en el ciberespacio.

CAPITULO III: GOTA A GOTA DIGITAL

El denominado “gota a gota digital” constituye una de las expresiones más recientes de la criminalidad económica y tecnológica, esta se trata de la evolución de una práctica de crédito informal tradicional que, trasladada al entorno digital, reproduce sus características, pero amplificadas gracias al uso de plataformas móviles, redes sociales y aplicaciones financieras no reguladas.

En su forma clásica, el “gota a gota” hace referencia a préstamos de dinero que se conceden de manera rápida y sin mayores requisitos, pero sujetos a intereses desproporcionados que se cobran de manera periódica, bajo amenazas contra el deudor en caso de incumplimiento. Según Rodríguez (2015), en su investigación sobre microempresarios en Villavicencio (Colombia), este sistema se caracteriza por el círculo vicioso de deuda en el que los prestatarios pagan intereses exorbitantes, lo que los condena a trabajar únicamente para satisfacer las exigencias del prestamista y no para generar capital propio.

Con la digitalización, este mecanismo ha migrado hacia el ciberespacio, definiendo a esta figura como aquella práctica de crédito informal que utiliza aplicaciones móviles, redes sociales y plataformas tecnológicas para ofrecer préstamos rápidos, imponiendo intereses usurarios y ejerciendo coacción a través del uso indebido de datos personales, siendo la principal particularidad de esta modalidad que el control y la amenaza dejan de ser presenciales para convertirse en virtuales, materializándose en el hostigamiento por llamadas, mensajes y la difusión de información privada de las víctimas y sus contactos.

Menacho (2024) sostiene que el “gota a gota digital” debe entenderse como un delito complejo, que inicia con la atracción de víctimas mediante publicidad engañosa, continúa con la extracción de datos sensibles del dispositivo móvil, se consolida en la creación de una deuda creciente e impagable y culmina en la ciberextorsión. Este carácter progresivo involucra la comisión simultánea de delitos como extorsión, estafa y coacción, aprovechando la vulnerabilidad económica y tecnológica de los usuarios.

La doctrina penal también ha señalado que el “gota a gota digital” se enmarca dentro de los denominados delitos informáticos “impuros”, es decir, aquellos en los que la tecnología no constituye el fin en sí mismo, sino un medio para replicar

conductas clásicas como la extorsión o la estafa conforme lo señala Villavicencio (2014). En este sentido, la digitalización no cambia la esencia del delito, pero sí transforma radicalmente su alcance y la forma en que se ejecuta, multiplicando el número de víctimas y dificultando la persecución penal debido a su carácter deslocalizado. En ese sentido, su peligrosidad radica no solo en el daño patrimonial causado, sino en el impacto psicológico, social y comunitario que genera, al extender la intimidación de la víctima directa hacia su círculo cercano.

1. Modus operandi del préstamo 'gota a gota' digital

El “gota a gota” digital se estructura como un delito complejo, cuyo funcionamiento se articula en torno a la captación de la víctima, la obtención de información personal, la generación de una deuda impagable y, finalmente, la coacción o extorsión para el cobro. La primera fase corresponde a la captación de la víctima mediante publicidad engañosa mediante aplicaciones digitales y perfiles falsos en redes sociales que ofrecen créditos rápidos, inmediatos y sin requisitos, lo que resulta particularmente atractivo para personas excluidas del sistema bancario formal. Como advierte Rodríguez Ladino (2015), la falta de acceso al crédito convencional, unida a la desconfianza hacia la banca y a la necesidad urgente de liquidez, constituye la principal causa que lleva a los microempresarios y trabajadores informales a recurrir a estos esquemas. Además, se debe tener en cuenta que, en el ámbito digital, esta realidad se amplifica, pues la oferta llega de manera masiva y directa a través de las plataformas en línea.

En la segunda fase, los delincuentes aprovechan la instalación del aplicativo para solicitar permisos excesivos sobre el dispositivo móvil. De acuerdo con Menacho (2024), estas aplicaciones no se limitan a gestionar el préstamo, sino que exigen acceso a la agenda de contactos, fotografías, archivos multimedia, mensajes y hasta la ubicación del usuario. Esta práctica, aunque se presenta bajo la apariencia de un requisito técnico para el correcto funcionamiento del servicio, constituye en realidad un sofisticado mecanismo de control, pues coloca a la víctima en una situación de vulnerabilidad constante frente al prestamista, debido a que el acceso a esta información no solo permite verificar la identidad del usuario, sino también trazar un mapa de sus relaciones personales y familiares, lo que amplifica la capacidad de presión y amenaza.

Además, Miró (2012) explica que, en gran parte de los ciberdelitos, no es la pericia informática del delincuente lo que determina el éxito del ataque, sino la conducta del propio usuario, que muchas veces con descuidos o actos de confianza facilita la intrusión. Esta observación cobra relevancia en el caso del “gota a gota” digital, ya que es el propio deudor quien, movido por la necesidad económica, otorga voluntariamente permisos que resultan desproporcionados, sin reparar en las consecuencias, demostrando cómo la víctima, lejos de ser un actor pasivo, se convierte en un engranaje indispensable para el éxito del delito al minimizar los riesgos asociados a la entrega de datos sensibles, en un contexto de urgencia económica.

La tercera fase corresponde al desembolso del dinero y la creación de una deuda impagable. En este punto, el atractivo inicial reside cuando el monto prestado se deposita en la cuenta del solicitante en cuestión de minutos, e incluso en algunos casos sin que exista una solicitud expresa. Sin embargo, esta aparente facilidad oculta condiciones usurarias que hacen prácticamente imposible el cumplimiento del pago. Rodríguez Ladino (2015), en su estudio sobre los microempresarios de Villavicencio, documentó que en el esquema presencial del “gota a gota” los prestatarios destinaban sus ingresos casi exclusivamente al pago de intereses, sin lograr nunca reducir el capital ni mejorar su situación económica. Esta dinámica refleja que la deuda se concibe como un mecanismo diseñado para perpetuar la dependencia del deudor respecto al prestamista, de esta forma el usuario queda convertido en rehén financiero de la organización criminal, que utiliza la deuda como instrumento de dominación y control.

La cuarta fase consiste en la coacción y la extorsión digital, que se activa cuando la víctima no logra cubrir los pagos exigidos. En este momento, los delincuentes aprovechan la información personal previamente recopilada para amenazar con su divulgación pública, esta presión no se limita a la persona endeudada, sino que se extiende a su entorno, lo que multiplica el impacto del hostigamiento. El mecanismo suele desplegarse mediante llamadas intimidatorias, mensajes insistentes y, en algunos casos, publicaciones en redes sociales dirigidas tanto a la víctima como a familiares, amigos o compañeros de trabajo, con el fin de generar vergüenza, miedo y deterioro de su reputación.

Cerezo (2020) destaca que esta forma de ciberextorsión presenta particularidades que la distinguen de las modalidades tradicionales porque el daño no siempre se expresa en términos materiales inmediatos, sino que se centra en la inmaterialidad de la reputación digital y en la amenaza de exponer públicamente información íntima o comprometedor. De este modo, la víctima experimenta la carga económica imposible de asumir, y el temor constante a la destrucción de su imagen personal y social en los entornos digitales.

1.1. Atracción y reclutamiento de víctimas (publicidad en redes sociales y plataformas móviles)

El primer paso en el modus operandi del préstamo “gota a gota” digital es la captación de víctimas, lo cual se realiza mediante estrategias de publicidad dirigidas en redes sociales y a través de plataformas móviles. A diferencia de la modalidad tradicional, donde los prestamistas informales se acercaban personalmente a mercados, barrios o zonas de alta vulnerabilidad económica, la versión digital utiliza canales de difusión masiva que permiten llegar a un público mucho más amplio y heterogéneo.

Según Menacho (2024), los grupos criminales aprovechan la infraestructura de internet para anunciar créditos rápidos y sin requisitos en Facebook, Instagram, o mediante mensajes publicitarios en WhatsApp. Estas publicaciones suelen emplear frases llamativas como “dinero fácil y al instante”, “préstamos sin historial crediticio” o “recibe efectivo hoy mismo”, dirigidas principalmente a personas excluidas del sistema financiero formal, como trabajadores informales, pequeños comerciantes, amas de casa o estudiantes universitarios. El proceso de reclutamiento se consolida cuando los usuarios son inducidos a descargar aplicaciones móviles desde tiendas virtuales como Google Play Store o, en algunos casos, mediante enlaces directos enviados a través de correos electrónicos y mensajes de texto. Una vez descargada la aplicación, se solicita al usuario que brinde permisos amplios sobre su dispositivo, tales como acceso a contactos, galería de imágenes, archivos y ubicación geográfica. En apariencia, se trata de requisitos inocuos para habilitar el servicio, pero en realidad constituyen la base para el control y la posterior intimidación de la víctima.

Lo característico de esta fase es que mientras los delincuentes conocen de antemano las técnicas para manipular la voluntad de las víctimas, estas suelen confiar en la publicidad ofrecida, motivadas por la urgencia económica y la necesidad inmediata de liquidez. Tal como advierte Miró Llinares (2012), en el ámbito de la ciberdelincuencia, el éxito de las conductas ilícitas no depende necesariamente de la pericia técnica del agresor, sino más bien del comportamiento de la propia víctima, quien en numerosas ocasiones facilita información confidencial o acepta condiciones perjudiciales al dejarse llevar por ofertas engañosas o promesas de aparente beneficio.

En esta primera etapa se observa, además que los anuncios y aplicaciones están dirigidos a sectores vulnerables, que no tienen acceso a créditos bancarios y se ven obligados a recurrir a estas alternativas. Esta focalización convierte a las redes sociales y a los dispositivos móviles en espacios de reclutamiento masivo, donde la aparente facilidad del préstamo oculta una estructura de control que luego derivará en hostigamiento y extorsión.

1.2. Extracción de datos sensibles para ejercer presión

Una vez que la víctima ha descargado la aplicación y aceptado sus condiciones, el paso siguiente en el esquema del préstamo “gota a gota” digital consiste en la extracción masiva de datos sensibles. Esta fase es fundamental porque convierte el préstamo en un mecanismo de control permanente sobre la víctima, al otorgar a los delincuentes un poder de intimidación que trasciende el plano económico.

De acuerdo con Menacho (2024), los aplicativos utilizados para esta modalidad suelen solicitar permisos excesivos e innecesarios para su funcionamiento, tales como acceso a la lista de contactos, fotografías, archivos multimedia, mensajes de texto y, en algunos casos, la ubicación geográfica en tiempo real. Aunque estas solicitudes aparecen justificadas como parte de la configuración del servicio, en realidad constituyen la principal fuente de coacción, ya que permiten a los delincuentes manipular la información privada con fines extorsivos.

La relevancia de esta etapa radica en que, al recopilar información del entorno íntimo del usuario, el agresor no solo controla a la víctima directa, sino que también extiende su poder de presión a familiares, amigos y compañeros de trabajo. Este efecto multiplicador transforma una deuda personal en un problema

social más amplio, pues la amenaza de divulgar datos personales o imágenes comprometedoras genera un círculo de miedo que inmoviliza a la víctima y reduce su capacidad de denuncia.

Miró (2012) señala que, en los delitos cometidos en entornos digitales, la conducta de la víctima facilita el acceso del delincuente y condiciona la efectividad del ataque. Este planteamiento resulta plenamente aplicable al “gota a gota” digital, donde el consentimiento apresurado a los permisos del aplicativo abre la puerta a un control invasivo de la vida privada.

En la práctica, la extracción de datos sensibles se traduce en amenazas directas cuando los prestamistas informales advierten que divulgarán imágenes personales, difundirán mensajes privados o notificarán a contactos cercanos sobre la deuda si no se cumple con el pago. Este uso instrumental de la información refuerza la transición del préstamo usurario hacia la ciberextorsión, en la que la reputación y la privacidad de la víctima se convierten en rehenes del sistema criminal.

1.3. Creación de deuda creciente con intereses ocultos y amenazas constantes

Una vez captada la víctima y recopilada su información personal, el siguiente paso en el esquema del préstamo “gota a gota” digital es la generación de una deuda progresivamente impagable. Este proceso se sostiene en la aplicación de intereses usureros y en la incorporación de cargos ocultos que rara vez se explicitan en el contrato digital, lo cual coloca a la víctima en una situación de dependencia y sometimiento. De acuerdo con Menacho (2024), el atractivo inicial del préstamo se encuentra en la rapidez con la que se transfiere el dinero a la cuenta del usuario, en ocasiones sin que este lo haya solicitado expresamente. Sin embargo, el monto desembolsado suele estar sujeto a tasas que superan con creces los límites legales de interés, alcanzando incrementos semanales que duplican o triplican la deuda original en pocos días. Este mecanismo reproduce la lógica del “gota a gota” tradicional, pero con la ventaja para los delincuentes de que la gestión de cobros es más sistemática y automatizada gracias a la tecnología.

El problema se agudiza porque, en muchos casos, las aplicaciones imponen comisiones encubiertas o penalidades por retraso que no han sido previamente informadas. De esta manera, aun cuando la víctima intente cumplir con el pago inicial, siempre se encuentra con un saldo adicional pendiente que nunca logra saldar en su totalidad. La deuda, lejos de disminuir, se convierte en un ciclo permanente de pagos que jamás extinguen la obligación. Un estudio realizado en Villavicencio evidenció que los prestatarios de “gota a gota” llegaban a pagar intereses que alcanzaban hasta el veinte por ciento en periodos cortos, lo que constituye un claro ejercicio de usura. En la práctica, muchos microempresarios destinaban sus ingresos exclusivamente al pago de intereses, sin posibilidad de capitalizar ganancias ni mejorar sus condiciones de vida. Esta constatación permite comprender cómo el “gota a gota” digital reproduce y amplifica la misma lógica de sometimiento económico mediante el uso de aplicativos móviles y plataformas virtuales.

La presión psicológica se incrementa mediante el uso de mensajes intimidatorios, llamadas constantes o la difusión de amenazas hacia el círculo cercano de la víctima. Miró (2012) advierte que, en el cibercrimen, lo relevante no es únicamente el daño patrimonial directo, sino el impacto sobre la percepción de seguridad y confianza del individuo en el entorno digital. En este caso, la intimidación no se limita a la exigencia de pago, sino que explota el miedo a la exposición pública y a la afectación de la reputación personal y familiar.

El resultado es una forma de esclavitud financiera en la que la víctima se encuentra atrapada en un bucle de deuda creciente, incluso si logra abonar sumas superiores al monto original, la estructura de intereses y cargos adicionales asegura que nunca pueda liberarse completamente de la obligación.

2. Impacto criminológico y social del ‘gota a gota’ digital

El préstamo “gota a gota” digital no solo representa un problema de carácter económico, sino que constituye un fenómeno de profunda relevancia criminológica y social, pues altera las dinámicas de control, vulnerabilidad y victimización en la sociedad digital contemporánea. Su impacto se refleja tanto en el plano individual como en el colectivo, generando un entorno de inseguridad financiera, emocional y comunitaria.

Desde el punto de vista criminológico, este tipo de delito se inscribe dentro de las formas de criminalidad económica organizada, en la medida en que combina elementos de usura, estafa, coacción y extorsión. Menacho (2024) sostiene que el “gota a gota” digital opera bajo un esquema de delito complejo donde el crédito aparente es solo el inicio de una cadena que culmina en la ciberextorsión, mostrando cómo los delincuentes han adaptado prácticas tradicionales al entorno virtual, multiplicando el número de víctimas y perfeccionando los mecanismos de presión. En el caso de Villavicencio, se documenta que el cobro de estas deudas ha derivado en amenazas, cierres de negocios, destierros e incluso muertes, lo que confirma que la violencia constituye un elemento estructural de esta práctica (Rodríguez Ladino, 2015, p. 3). En el ámbito digital, esa misma violencia se manifiesta a través de hostigamiento por llamadas, mensajes y la divulgación de información personal, generando daños psicológicos y sociales que afectan tanto al deudor como a su círculo cercano.

El impacto social se observa, en primer lugar, en el endeudamiento progresivo de sectores vulnerables cuando trabajadores informales, amas de casa, estudiantes o pequeños comerciantes, al carecer de acceso al sistema financiero formal, se convierten en el principal blanco de estas organizaciones. La deuda creciente y la amenaza constante afectan la estabilidad económica de los hogares y, en muchos casos, provocan la pérdida de medios de subsistencia.

En segundo lugar, la presión ejercida a través de mensajes, llamadas o la amenaza de divulgar información privada desencadena cuadros de ansiedad, depresión y estigmatización social. Miró (2012) advierte que, en los delitos digitales, la afectación no se limita a lo patrimonial, sino que incide directamente en la confianza de las personas en el entorno tecnológico y en sus relaciones interpersonales. Este aspecto es crucial, pues la víctima no solo pierde recursos económicos, sino también parte de su autonomía y sentido de seguridad.

En tercer lugar, el “gota a gota” digital impacta en la confianza colectiva en el sistema financiero y en el ecosistema digital. Cuando la población percibe que el uso de aplicaciones o plataformas de crédito informal puede derivar en extorsión, se erosiona la credibilidad en las herramientas tecnológicas y en la economía digital en general. Este efecto colectivo limita la inclusión financiera, desalienta

la bancarización y refuerza la marginalidad de los sectores más pobres, reproduciendo así un círculo de exclusión y vulnerabilidad.

2.1. Impacto individual de la victimización

El impacto del “gota a gota” digital se aprecia con especial fuerza en el plano individual, pues la víctima no solo se enfrenta a una deuda impagable, sino que queda sometida a un régimen de control psicológico basado en la intimidación. Menacho (2024) explica que la extracción de datos sensibles a través de los aplicativos convierte al deudor en un sujeto permanentemente vigilado, lo que genera un estado de temor constante que reduce su capacidad de reacción o denuncia.

Este fenómeno produce, además del perjuicio económico, un daño psicológico que se traduce en ansiedad, estrés y sensación de indefensión. Según Miró (2012), en los delitos cometidos en entornos digitales la víctima no es un actor pasivo, sino que su interacción tecnológica condiciona la efectividad del delito. Así, la entrega de información o la aceptación de términos abusivos se convierte en la base para que los delincuentes ejerzan presión y manipulación emocional.

El impacto individual se manifiesta también en la pérdida de confianza en el entorno digital. Las víctimas suelen desarrollar miedo a utilizar aplicaciones financieras, redes sociales o servicios en línea, lo que profundiza su exclusión del ámbito tecnológico. Esta desconfianza limita sus oportunidades de inclusión financiera y, en muchos casos, afecta sus vínculos sociales, pues los familiares o contactos cercanos también pueden ser intimidados a partir de la información sustraída de los dispositivos.

2.2. Impacto colectivo o comunitario

El fenómeno del “gota a gota” digital no se limita a la relación entre prestamista y deudor, sino que produce consecuencias más amplias que afectan al conjunto de la comunidad. En este nivel, el impacto se manifiesta principalmente en tres dimensiones: la desconfianza colectiva en el sistema financiero, la erosión de la seguridad digital y la consolidación de redes de criminalidad organizada que operan de manera transnacional.

En primer lugar, la proliferación de préstamos extorsivos digitales debilita la confianza de la población en las tecnologías financieras y en los servicios

digitales en general. Como advierte Miró (2012), la victimización en el ciberespacio no solo tiene efectos patrimoniales, sino que socava la confianza social en las redes y plataformas virtuales, minando con ello la legitimidad de la economía digital. Esta desconfianza genera resistencia hacia procesos de bancarización e inclusión financiera, reproduciendo la exclusión de los sectores más vulnerables, que continúan dependiendo de alternativas informales de financiamiento.

En segundo lugar, el “gota a gota” digital afecta la percepción de seguridad comunitaria en el espacio digital. Al tratarse de un delito en el que las amenazas se extienden no solo a la víctima directa sino también a su entorno, el miedo se multiplica y alcanza a familiares, amigos y compañeros de trabajo, generando una sensación colectiva de inseguridad. Tal como señala Menacho (2024), el uso de datos sensibles no solo somete a la persona endeudada, sino que extiende el radio de intimidación a todo su círculo social, convirtiendo la deuda individual en un problema compartido que impacta en las dinámicas comunitarias.

A nivel estructural, la proliferación de este tipo de préstamos encuentra sustento en la exclusión financiera y en la excesiva tramitología de la banca formal. La investigación de Rodríguez Ladino (2015) evidencia que muchos prestatarios acudían al “gota a gota” porque los bancos exigían requisitos difíciles de cumplir, demandaban fiadores o generaban desconfianza en los sectores más vulnerables. Este hallazgo ayuda a entender por qué el “gota a gota” digital se difunde con tanta rapidez: responde a una necesidad real de acceso a crédito, aunque lo haga bajo condiciones abusivas y con consecuencias devastadoras para las víctimas.

En tercer lugar, la modalidad digital del “gota a gota” fortalece las estructuras de criminalidad organizada. A diferencia del esquema tradicional, donde la usura estaba ligada a contextos locales, el modelo digital permite a estas organizaciones ampliar su alcance más allá de las fronteras geográficas. Ello facilita la articulación con otros delitos como el lavado de activos, el fraude informático o la trata de datos personales, lo que incrementa la complejidad del fenómeno y convierte al “gota a gota” digital en una amenaza global.

En suma, el impacto colectivo de este delito radica en que trasciende la esfera individual para convertirse en un problema social y comunitario. Afecta la

cohesión social, erosiona la confianza en la economía digital e incrementa la percepción de vulnerabilidad frente a organizaciones criminales que utilizan la tecnología como herramienta de dominación.

3. Necesidad de un tipo penal específico para el 'gota a gota' digital

El fenómeno del “gota a gota” digital plantea un reto particular para el derecho penal contemporáneo, en la medida en que combina prácticas tradicionales de usura y extorsión con el uso intensivo de las tecnologías de la información. Aunque parte de su estructura encaja en figuras ya previstas en el Código Penal la complejidad de su *modus operandi* y su alcance social hacen evidente la necesidad de un tipo penal específico que capture la singularidad de esta modalidad delictiva.

En primer lugar, debe destacarse que el préstamo “gota a gota” digital no se limita a un delito de usura. Como explica Menacho (2024), se trata de un delito complejo, pues integra en su dinámica la captación de víctimas a través de medios digitales, la extracción abusiva de datos personales, la aplicación de intereses encubiertos y la posterior ciberextorsión mediante amenazas de difundir información sensible

En este sentido, subsumir todas estas conductas dentro del marco de la extorsión tradicional o del fraude informático genera un tratamiento parcial, que invisibiliza la dimensión psicológica y social del delito.

En segundo lugar, la aplicación de figuras ya existentes ha demostrado ser insuficiente por la falta de precisión normativa. Felipe Villavicencio Terreros (2014) advierte que el derecho penal peruano se ha centrado en los llamados “delitos informáticos puros” (como el acceso ilícito a sistemas o el sabotaje), dejando en segundo plano los “delitos informáticos impuros”, es decir, aquellos en los que la tecnología es un medio para cometer delitos clásicos como la extorsión o la estafa. El “gota a gota” digital pertenece a esta segunda categoría, lo que revela un vacío legislativo que dificulta una persecución eficaz y coherente.

En tercer lugar, la ausencia de un tipo penal específico genera problemas prácticos en la labor de jueces y fiscales. La tipificación fragmentada obliga a encajar la conducta en varias figuras penales al mismo tiempo, recurriendo al

concurso ideal entre extorsión, coacción y estafa. Esta dispersión no solo complica la labor probatoria, sino que también puede dar lugar a vacíos de punibilidad, ya que las penas y los elementos típicos no siempre reflejan la gravedad real del daño ocasionado a la víctima y a su entorno.

Asimismo, la necesidad de un tipo penal autónomo se justifica en función del impacto criminológico y social del delito. Como se ha señalado en los apartados anteriores, el “gota a gota” digital genera un círculo de victimización múltiple: por un lado, endeuda progresivamente a personas vulnerables; por otro, utiliza sus datos personales como mecanismo de presión; y finalmente, erosiona la confianza en el ecosistema digital y en el sistema financiero. Esta combinación de efectos hace que su peligrosidad trascienda la de los delitos tradicionales y demande un tratamiento jurídico particular.

En la experiencia comparada, países como Colombia y México ya han iniciado reformas normativas para tipificar de manera expresa los préstamos digitales extorsivos. En Colombia, la Superintendencia Financiera ha emitido alertas sobre el “gota a gota virtual”, reconociendo la necesidad de articular la legislación penal con mecanismos de control financiero. En México, por su parte, se han identificado aplicaciones conocidas como “montadeudas”, lo que ha impulsado investigaciones legislativas para sancionar penalmente la práctica y proteger a los usuarios frente al hostigamiento digital. Estas experiencias muestran que la creación de un tipo penal específico no solo es posible, sino también necesaria para enfrentar este fenómeno con mayor eficacia.

En conclusión, la necesidad de un tipo penal específico para el “gota a gota” digital responde a tres razones principales: la insuficiencia de los tipos penales actuales para abarcar la complejidad del delito, los problemas prácticos de fragmentación en la persecución judicial y el impacto criminológico y social diferenciado que esta modalidad produce. Reconocer esta figura en la legislación no implica sobredimensionar el poder punitivo, sino dotar al sistema de justicia de una herramienta precisa que permita sancionar de manera proporcional y efectiva a quienes, aprovechando las tecnologías digitales, reproducen y amplifican la violencia económica sobre los sectores más vulnerables de la sociedad.

3.1. Insuficiencia de los tipos penales existentes

El marco normativo vigente en el Perú no logra abarcar de manera integral la complejidad del “gota a gota” digital. Actualmente, las conductas que forman parte de esta modalidad suelen subsumirse en figuras como la extorsión, la estafa o la coacción. Sin embargo, este encuadre resulta parcial y fragmentado, porque no refleja la dinámica multietápica que caracteriza al fenómeno.

Menacho Ortega (2024) sostiene que el préstamo extorsivo digital constituye un delito complejo, en el que se entrelazan fases de captación, extracción de datos personales, aplicación de intereses abusivos y posterior ciberextorsión. Al obligar a los operadores jurídicos a descomponer estas conductas en varios tipos penales distintos, se pierde la visión de conjunto y, en muchos casos, se dificulta la labor probatoria. Villavicencio (2014) añade que la legislación peruana ha concentrado sus esfuerzos en los llamados delitos informáticos “puros” (acceso ilícito a sistemas, manipulación de datos, sabotaje digital), mientras que los delitos “impuros”, en los que la tecnología funciona como medio para reproducir figuras clásicas como la extorsión o la estafa, han quedado desatendidos. El “gota a gota” digital encaja precisamente en esta última categoría, lo que evidencia un vacío legislativo que reduce la capacidad de sanción efectiva.

La consecuencia práctica es que los fiscales y jueces se ven obligados a aplicar el concurso ideal entre extorsión, estafa y coacción, lo que genera inseguridad jurídica y, en algunos casos, deja lagunas en la determinación de la pena. Además, al no existir un reconocimiento expreso de la modalidad digital, no se valora de manera adecuada la particularidad de la coacción ejercida mediante el control de datos sensibles y la amenaza de divulgación pública en redes sociales.

En este sentido, la insuficiencia de los tipos penales actuales refuerza la necesidad de un tipo específico que capture la singularidad del préstamo “gota a gota” digital y reconozca su carácter autónomo como forma de criminalidad organizada en el entorno virtual.

4. Derecho comparado: respuestas legales frente a los préstamos extorsivos digitales

El fenómeno del préstamo “gota a gota” digital no es exclusivo del Perú, sino que forma parte de una tendencia regional y global en la que las organizaciones

criminales han encontrado en las tecnologías de la información un medio eficaz para reproducir y amplificar prácticas usurarias y extorsivas. Por ello, el análisis del derecho comparado permite identificar las diferentes respuestas normativas y políticas que se han desarrollado en países que enfrentan problemáticas similares, aportando lecciones útiles para la consolidación de un marco jurídico más sólido en el ámbito nacional.

En Colombia, la Superintendencia Financiera y la Policía Nacional han emitido múltiples alertas respecto al denominado “gota a gota virtual”. Esta modalidad se ha caracterizado por la difusión de aplicaciones móviles de crédito rápido, muchas de ellas ilegales, que imponen intereses excesivos y recurren a la intimidación digital para cobrar las deudas. Aunque la tipificación penal no incluye un delito autónomo de préstamo extorsivo digital, las autoridades han recurrido al delito de usura y a la extorsión como marcos de persecución. Sin embargo, diversos informes oficiales han advertido que la legislación aún resulta insuficiente y que es necesario crear normas específicas que regulen los créditos digitales informales, dado que las aplicaciones pueden operar desde el extranjero y escapar al control nacional.

En México, el fenómeno ha sido identificado bajo el nombre de “montadeudas”, y ha generado una fuerte reacción institucional debido al elevado número de denuncias. La Fiscalía General de Justicia de la Ciudad de México y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) han investigado aplicaciones que ofrecen préstamos exprés y luego hostigan a las víctimas mediante llamadas y mensajes amenazantes. Aunque la respuesta inicial ha sido de carácter administrativo, con la eliminación de aplicaciones fraudulentas de las tiendas virtuales, también se ha iniciado un proceso de reforma legal para incorporar esta modalidad dentro de los delitos de fraude y extorsión, así como para establecer sanciones más severas contra quienes desarrollen o difundan este tipo de plataformas.

En España, si bien el “gota a gota” digital no se presenta con la misma intensidad que en América Latina, existen antecedentes de alertas emitidas por organismos de protección al consumidor frente a aplicaciones financieras que operan de manera fraudulenta o abusiva. En este país, las prácticas usurarias digitales suelen abordarse a través de la legislación sobre usura y estafa, pero en los

últimos años se ha advertido la necesidad de ampliar el marco de protección frente a los denominados delitos económicos digitales, donde se combina la coacción con la manipulación tecnológica.

El derecho comparado revela, en consecuencia, dos tendencias principales. La primera consiste en el uso de figuras ya existentes, como la usura, la estafa o la extorsión, para perseguir judicialmente a los responsables, aunque con resultados limitados debido a la complejidad tecnológica de estas prácticas. La segunda es la emergencia de propuestas legislativas que buscan crear marcos normativos específicos, capaces de reconocer al préstamo digital extorsivo como una modalidad autónoma que combina elementos de criminalidad económica, ciberdelincuencia y victimización social.

En definitiva, la revisión de la experiencia internacional demuestra que el Perú no enfrenta este problema de manera aislada y que el reconocimiento legislativo del “gota a gota” digital, como se ha hecho con la Ley 32183, responde a una necesidad compartida en la región. Ello refuerza la importancia de diseñar un marco penal claro y especializado que no solo castigue, sino que también prevenga la expansión de este fenómeno delictivo en el entorno digital.

4.1 Colombia: alerta de la Superintendencia Financiera sobre el “gota a gota virtual”

En Colombia, el fenómeno del “gota a gota” tiene una larga tradición en su forma presencial, asociada históricamente a redes de usura y criminalidad organizada que operaban en barrios populares y zonas de comercio informal. Con la irrupción de las tecnologías de la información, esta práctica se trasladó al entorno digital, dando lugar al denominado “gota a gota virtual”, que ha generado gran preocupación entre las autoridades por su alcance masivo y su capacidad de afectar a poblaciones vulnerables.

La Superintendencia Financiera de Colombia, junto con la Policía Nacional y el Ministerio de Tecnologías de la Información, ha emitido en los últimos años diversas alertas públicas sobre el uso de aplicaciones móviles que ofrecen créditos fáciles e inmediatos, pero que imponen intereses desproporcionados y recurren a la intimidación para el cobro de deudas. Estas entidades han advertido que tales aplicaciones, en su mayoría no registradas ni supervisadas por el

sistema financiero formal, constituyen un grave riesgo para los usuarios, quienes terminan sometidos a amenazas y hostigamiento digital al no poder cumplir con las condiciones impuestas.

La particularidad del “gota a gota virtual” en Colombia radica en que se presenta como un servicio legítimo de microcrédito, aprovechando la desconfianza histórica hacia la banca tradicional y la exclusión financiera de amplios sectores de la población. De esta manera, los prestamistas digitales han logrado expandirse con rapidez en comunidades que carecen de acceso a préstamos bancarios y que, en muchos casos, desconocen los mecanismos legales de protección frente al endeudamiento abusivo.

Aunque la legislación colombiana sanciona la usura y la extorsión, las autoridades han reconocido que estas figuras resultan insuficientes para enfrentar la nueva modalidad digital. Los informes de la Superintendencia Financiera señalan que el “gota a gota virtual” no solo constituye un problema económico, sino también un asunto de seguridad ciudadana y ciberseguridad, dado que las aplicaciones fraudulentas suelen operar desde el extranjero, lo que dificulta la persecución penal y la sanción de los responsables.

En respuesta, se han impulsado campañas de educación financiera y de prevención digital, orientadas a advertir a los ciudadanos sobre los riesgos de descargar aplicaciones no autorizadas y a fomentar el uso de canales financieros formales. Sin embargo, la ausencia de un tipo penal específico sigue siendo un vacío relevante, lo que ha llevado a distintos sectores académicos y judiciales a proponer reformas que tipifiquen expresamente el préstamo extorsivo digital como delito autónomo.

La experiencia colombiana demuestra, por tanto, que el “gota a gota virtual” es un fenómeno que desborda las categorías jurídicas tradicionales y que requiere un marco normativo claro y especializado. El reconocimiento temprano de este problema por parte de la Superintendencia Financiera constituye un paso importante, pero la falta de reformas legales concretas mantiene en estado de vulnerabilidad a los sectores más expuestos al endeudamiento informal digital.

En esta línea, la propia Superintendencia Financiera ha impulsado la campaña “No caiga en el gota a gota virtual”, alertando a los ciudadanos sobre las

aplicaciones que exigen permisos excesivos en los dispositivos móviles y luego usan esa información para acosar y amenazar a las víctimas. La entidad advirtió que estas plataformas, al no estar reguladas, generan un riesgo que trasciende lo económico y compromete la seguridad digital y personal de los usuarios (Superintendencia Financiera de Colombia, 2025).

4.2 México: aplicaciones “montadeudas”

En México, el fenómeno equivalente al “gota a gota” digital ha sido identificado bajo la denominación de “montadeudas”, término con el que se alude a las aplicaciones móviles que ofrecen créditos exprés y que posteriormente someten a los usuarios a prácticas de hostigamiento y extorsión. Este problema se ha expandido en los últimos años, generando preocupación en las autoridades financieras y judiciales debido al número creciente de denuncias y al fuerte impacto social que produce en los sectores más vulnerables.

La modalidad de funcionamiento es similar a la observada en otros países de la región: las aplicaciones prometen préstamos inmediatos, sin requisitos formales ni revisión de historial crediticio, pero imponen intereses usureros y plazos de pago imposibles de cumplir. Cuando la víctima no logra cubrir el monto en el tiempo señalado, los prestamistas digitales recurren a la intimidación, enviando mensajes amenazantes tanto al deudor como a sus contactos, obtenidos a través de los permisos concedidos al momento de instalar la aplicación.

La Fiscalía General de Justicia de la Ciudad de México, junto con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), ha liderado investigaciones sobre estas plataformas, logrando en algunos casos la detención de responsables y la eliminación de cientos de aplicaciones fraudulentas de las principales tiendas virtuales. Sin embargo, las propias autoridades han reconocido que se trata de un fenómeno difícil de erradicar, ya que las aplicaciones se reactivan bajo nuevos nombres o migran a servidores en el extranjero, lo que dificulta su rastreo y sanción.

La respuesta del Estado mexicano ha sido doble. Por un lado, se ha trabajado en medidas administrativas y preventivas, consistentes en la identificación y denuncia pública de aplicaciones ilegales, así como en campañas de educación digital para advertir a los usuarios sobre los riesgos de recurrir a estos servicios.

Por otro lado, se han iniciado debates legislativos orientados a tipificar de manera expresa el préstamo digital extorsivo, de modo que no quede subsumido únicamente en las figuras de fraude o extorsión tradicionales. Este esfuerzo busca reconocer la especificidad de la modalidad y brindar a fiscales y jueces una herramienta más clara para su persecución.

El caso mexicano resulta ilustrativo porque muestra cómo las “montadeudas” han pasado de ser un fenómeno marginal a convertirse en un problema nacional de seguridad digital y económica. El aumento de denuncias, así como la evidencia del daño psicológico y social ocasionado, ha puesto en evidencia la urgencia de reformas normativas y de una estrategia integral que combine derecho penal, control administrativo y políticas de prevención digital.

La Fiscalía General de Justicia de la Ciudad de México, junto con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), ha liderado investigaciones sobre estas plataformas, logrando en algunos casos la eliminación de aplicaciones fraudulentas de las principales tiendas virtuales. La Policía Cibernética de la SSC CDMX también ha advertido sobre los riesgos de descargar este tipo de aplicaciones, señalando que suelen operar desde el extranjero y que utilizan permisos excesivos para acceder a contactos y datos personales, lo que facilita el hostigamiento posterior. Estas instituciones han lanzado campañas de información y prevención para educar a los usuarios sobre cómo identificar prestamistas falsos y denunciar aplicaciones ilegales (SSC CDMX, 2024; CONDUSEF, 2024).

4.3. España: regulación y alertas del SERNAC sobre apps financieras con comportamiento extorsivo digital – MULAS DIGITALES

En España, si bien el fenómeno del préstamo “gota a gota” digital no presenta la misma magnitud que en América Latina, también se han identificado riesgos asociados a aplicaciones financieras que operan con prácticas abusivas o fraudulentas. Estos riesgos han motivado tanto a las autoridades judiciales como a organismos de protección al consumidor a reforzar los mecanismos de control y a advertir públicamente sobre la peligrosidad de estas plataformas.

El marco normativo español cuenta con la Ley de Represión de la Usura de 1908, aún vigente, que declara nulos los contratos de préstamo en los que se imponen

intereses desproporcionados o usurarios. A esta norma se suma la tipificación penal de la estafa y la coacción, que se aplican en casos donde el cobro abusivo se acompaña de engaños o amenazas. No obstante, estos instrumentos resultan limitados frente a las modalidades digitales actuales, que combinan usura, extorsión y el uso indebido de datos personales para hostigar a las víctimas.

En los últimos años, organismos de protección al consumidor han emitido alertas frente a aplicaciones móviles que ofrecen créditos rápidos con condiciones poco claras, intereses elevados y mecanismos de presión digital contra los deudores. Entre ellos, destaca el papel del Servicio Nacional del Consumidor (SERNAC), que aunque pertenece al sistema de protección al consumidor en Chile, ha servido como referencia regional al advertir sobre el riesgo de las plataformas digitales que emplean prácticas extorsivas y que también tienen incidencia en el mercado español a través de aplicaciones transnacionales. Estas advertencias han contribuido a visibilizar un fenómeno que no se limita a un país, sino que se expande por la interconexión digital y la ausencia de fronteras en el ciberespacio.

En el ámbito regional, destaca la experiencia del Servicio Nacional del Consumidor (SERNAC) de Chile, que ha investigado aplicaciones móviles de préstamos que pedían permisos excesivos sobre los dispositivos, como acceso a contactos, cámara, localización y archivos personales. Estas aplicaciones fueron denunciadas por incurrir en hostigamiento y amenazas contra los usuarios. El SERNAC ofició a Google y Apple solicitando la remoción de estas plataformas y remitió los antecedentes a la policía para eventuales acciones penales. La advertencia subraya que estas prácticas no son aisladas, sino que forman parte de un patrón internacional de criminalidad digital asociado a los préstamos abusivos (SERNAC, 2024).

España ha optado, además, por reforzar la supervisión administrativa a través del Banco de España y de la Agencia Española de Protección de Datos, que investigan a aquellas entidades o aplicaciones que vulneran los derechos de los consumidores mediante la explotación de información personal. Aunque no se ha creado un tipo penal autónomo, la experiencia española muestra un esfuerzo por articular el derecho penal, la normativa civil y el derecho de consumo en un marco integral que permita ofrecer mayores garantías a los usuarios.

En conclusión, la experiencia española evidencia que la regulación de los préstamos digitales con carácter extorsivo requiere no solo del derecho penal, sino también de un enfoque preventivo y de protección al consumidor. Las alertas institucionales, junto con el control administrativo, han resultado herramientas útiles para anticipar los riesgos de estas plataformas, aunque todavía queda pendiente una adecuación legislativa más clara frente a las nuevas formas de criminalidad digital.

CAPITULO IV: PRÉSTAMOS MEDIANTE APLICATIVOS (8-A)

1. La evolución del préstamo informal hacia la digitalización

El préstamo informal ha sido, históricamente, una alternativa de financiamiento para aquellas personas que, debido a la falta de historial crediticio, la ausencia de garantías o la exclusión social, no podían acceder al sistema bancario tradicional, esta modalidad adoptó expresiones como el “gota a gota”, caracterizándose por tasas usurarias, cobros diarios y la utilización de la intimidación física como método de presión. Tal como documenta Rodríguez Ladino, en contextos como el de Villavicencio (Colombia), los prestatarios destinaban gran parte de sus ingresos únicamente a cubrir los intereses exigidos por los prestamistas, sin posibilidad de mejorar sus condiciones económicas (2015).

El préstamo informal se configura como un sistema paralelo al financiero formal, caracterizado por la ausencia de regulación, la inexistencia de contratos escritos y la total dependencia del prestatario frente al prestamista; esta ausencia de garantías legales coloca al deudor en un escenario de indefensión, pues no existen mecanismos estatales que limiten la imposición de intereses desproporcionados ni que aseguren el cumplimiento de condiciones equitativas. Como advierte Menacho, estas prácticas no buscan promover la inclusión crediticia ni mejorar las condiciones de vida de quienes recurren a ellas, sino mantener un modelo de dependencia económica que asegura beneficios continuos para el prestamista a costa de la precariedad del prestatario (2024). En paralelo, el préstamo informal ha incidido en la vida comunitaria al generar climas de tensión y miedo colectivo. Los prestamistas suelen ejercer control territorial, utilizando la intimidación y la violencia como instrumentos de cobro, lo

que convierte al crédito en un mecanismo de dominación social. Este fenómeno se vincula, además, con el crecimiento de redes delictivas que instrumentalizan el préstamo para consolidar su poder en barrios y comunidades. Como señala Rodríguez Ladino, en estas dinámicas los prestatarios no solo quedan atrapados en ciclos de deuda perpetua, sino que también son víctimas de un entorno de hostigamiento que repercute en sus familias y en el tejido social de la comunidad (2015).

Con la digitalización, este esquema ha experimentado una transformación sustancial, debido a que lo que antes dependía de prestamistas locales y de relaciones de proximidad, ahora se ha trasladado a un entorno virtual que permite ampliar exponencialmente la escala de víctimas y reducir los costos de operación para los delincuentes. Menacho Ortega explica que este cambio responde a la capacidad de las aplicaciones móviles de reproducir la lógica del préstamo informal en el ciberespacio, combinando la usura con la extorsión digital y el acceso indebido a datos personales (2024).

Este tránsito hacia lo digital no ha sido fortuito, sino que responde a la creciente exclusión financiera de amplios sectores de la población y a la masificación del acceso a teléfonos inteligentes e Internet. Mientras que en el esquema tradicional los prestamistas debían establecer contacto directo con los prestatarios en espacios físicos, en la actualidad las aplicaciones móviles permiten llegar a un público mucho más amplio mediante anuncios en redes sociales, mensajes masivos y plataformas de descarga en línea. De esta manera, el crédito informal ha encontrado en la digitalización un canal eficaz para captar a miles de usuarios en situación de necesidad, eliminando la limitación geográfica que caracterizaba a la práctica presencial. Este fenómeno debe entenderse, además, como una consecuencia directa de la exclusión financiera que caracteriza a gran parte de la población latinoamericana. En sociedades donde el acceso al crédito formal exige garantías, historial bancario y condiciones que muchas personas no pueden cumplir, la oferta de préstamos rápidos y sin requisitos aparece como una alternativa tentadora. Sin embargo, esa misma necesidad se convierte en un factor de vulnerabilidad que los prestamistas digitales explotan para asegurar su control. Como advierte Villavicencio, los delitos informáticos impuros se nutren

precisamente de esa vulnerabilidad social, pues la tecnología funciona como un instrumento que amplifica la capacidad de sometimiento económico (2014).

Además, el paso a lo digital ha permitido a estas organizaciones diversificar sus mecanismos de operación y blanqueo de capitales. Mientras que el préstamo informal tradicional dependía de circuitos locales de circulación del dinero, en el ámbito digital los recursos obtenidos se canalizan a través de transferencias electrónicas, criptomonedas, casas de apuestas en línea y otras plataformas financieras virtuales, lo que dificulta su rastreo por parte de las autoridades. Esta evolución no solo incrementa la rentabilidad del delito, sino que lo conecta con formas más complejas de criminalidad organizada, generando un fenómeno que trasciende lo económico y que requiere respuestas coordinadas tanto en el plano penal como en el regulatorio. Otro aspecto relevante de la digitalización es la creciente sofisticación de las aplicaciones en cuanto a su capacidad para evadir controles y dificultar la persecución penal. Muchas de estas plataformas no cuentan con un domicilio legal, cambian de nombre constantemente o migran sus servidores a jurisdicciones extranjeras, lo que impide rastrear con facilidad a los responsables. Este carácter transnacional obliga a repensar la eficacia de los marcos normativos nacionales, que suelen ser insuficientes frente a delitos que se desarrollan en un espacio digital sin fronteras. Como señala Cerezo y García, la transnacionalidad del cibercrimen plantea problemas jurisdiccionales que complican la investigación y el enjuiciamiento, pues los prestamistas pueden operar desde cualquier parte del mundo contra víctimas localizadas en diferentes países (2020).

La transición del ámbito físico a la digital supone, además, un cambio en la forma de captación. A diferencia del “gota a gota” tradicional, donde los prestamistas se publicitaban en mercados o barrios, el “gota a gota” digital utiliza anuncios en redes sociales, mensajes masivos en línea y aplicaciones disponibles en tiendas oficiales. Investigaciones recientes han identificado más de mil aplicaciones fraudulentas de préstamos en América Latina, muchas de ellas descargables desde Google Play, que operaban con características idénticas de hostigamiento digital y usura, independientemente del país en el que se instalaran (ESET, 2024).

La tecnología no solo amplió el alcance, sino que se convirtió en un mecanismo de control más sofisticado, estas aplicaciones exigen permisos excesivos sobre los dispositivos móviles de las víctimas, obteniendo acceso a sus contactos, fotografías, mensajes y ubicación. Ello permite que la intimidación trascienda lo económico y se convierta en un hostigamiento psicológico y social. Como advierte Miró, en muchos ciberdelitos no es la sofisticación técnica del delincuente lo que garantiza el éxito, sino la conducta de los usuarios, que, por necesidad o desconocimiento, facilitan voluntariamente el acceso a su información personal (2012). El impacto de este modelo entonces no se limita a lo económico, sino que se proyecta sobre el tejido social al erosionar la confianza en los entornos digitales. La amenaza de difundir fotografías, conversaciones o datos personales convierte al préstamo digital en un fenómeno de victimización múltiple, donde la víctima no solo sufre la pérdida patrimonial, sino también el daño psicológico y social derivado del hostigamiento público. Miró Llinares ha señalado que el cibercrimen afecta bienes jurídicos intangibles como la privacidad y la reputación, cuya afectación puede ser incluso más lesiva que el perjuicio patrimonial (2012), es así que, este rasgo diferencia al “gota a gota” digital del modelo tradicional, pues lo convierte en un delito con repercusiones colectivas que trascienden el ámbito individual.

Este proceso digital también intensifica los riesgos para las víctimas, pues ya no se trata únicamente de la imposibilidad de pagar una deuda con intereses abusivos, sino de la amenaza de exponer información íntima y la consecuente destrucción de la reputación personal. Autoridades como la Superintendencia Financiera de Colombia han advertido públicamente sobre estos peligros mediante campañas como “No caiga en el gota a gota virtual”, destacando que las apps de crédito fácil suelen operar sin supervisión, exigen permisos invasivos y derivan en prácticas extorsivas cuando la víctima incumple (Superintendencia Financiera de Colombia, 2025).

Por último, la expansión del “gota a gota” digital revela la necesidad de respuestas coordinadas a nivel internacional y de políticas públicas de educación digital, la experiencia comparada muestra que los países no han logrado enfrentar eficazmente este problema únicamente con reformas penales, sino que requieren campañas de concientización sobre los riesgos de descargar

aplicaciones fraudulentas y de compartir información personal. En ese sentido, la advertencia de organismos como la Superintendencia Financiera de Colombia y la CONDUSEF en México es ilustrativa, pues subraya que la prevención no depende solo de la sanción penal, sino también de la capacidad de los usuarios para reconocer y evitar prácticas fraudulentas. En el caso peruano, la promulgación de la Ley N.º 32183 y la incorporación del artículo 8-A a la Ley N.º 30096 de Delitos Informáticos reconocen expresamente el riesgo que supone esta evolución digital del préstamo informal. La norma sanciona a quienes, mediante plataformas tecnológicas, inducen u obligan a aceptar préstamos simulados con fines extorsivos, estableciendo penas privativas de libertad entre diez y quince años; sin embargo, se advierte que la persecución de estos delitos enfrenta limitaciones debido a la naturaleza transnacional y anónima de las aplicaciones, lo que reduce la eficacia de los marcos normativos convencionales.

2. Naturaleza jurídica del préstamo mediante aplicativos móviles

El préstamo mediante aplicativos móviles constituye un fenómeno en el que confluyen aspectos del derecho civil, del derecho del consumidor y del derecho penal; en términos civiles, el contrato de mutuo sigue siendo la figura jurídica de referencia, pues se trata de un acuerdo en virtud del cual una de las partes entrega dinero a otra con la obligación de devolverlo en un plazo determinado. Sin embargo, cuando este esquema se traslada a plataformas tecnológicas no reguladas, surgen elementos que distorsionan la esencia del mutuo y que, en determinados supuestos, pueden convertir la operación en ilícita. La diferencia principal radica en que, en los préstamos digitales informales, el consentimiento del usuario se obtiene mediante cláusulas redactadas en términos abusivos. Menacho señala que estas aplicaciones no buscan establecer una relación contractual equilibrada, sino que se valen del aparente consentimiento del usuario para acceder a información personal y para imponer condiciones usurarias (2024). Esto las coloca en un espacio jurídico ambiguo, pues se presentan como contratos de préstamo, pero en realidad encubren un mecanismo de sometimiento económico.

Desde el derecho del consumidor, la problemática se intensifica. Según el Servicio Nacional del Consumidor de Chile, varias aplicaciones de crédito rápido han sido investigadas porque solicitaban permisos invasivos y operaban sin

domicilio conocido ni inscripción en registros oficiales, lo que vulnera el principio de transparencia y las normas básicas de protección a los usuarios (SERNAC, 2024). En consecuencia, aunque formalmente el usuario “acepta” el contrato, en la práctica no existe información clara ni un marco de protección efectivo, lo que desnaturaliza la figura contractual y abre la puerta a prácticas abusivas.

En el ámbito penal, la naturaleza de estos préstamos se vincula con la extorsión, la coacción y la estafa. Rodríguez mostró que, en el “gota a gota” tradicional, los prestatarios terminaban atrapados en un ciclo de pagos sin posibilidad de liberación, lo que en la práctica constituía una forma de sometimiento financiero (2015), demostrando que los prestatarios quedaban atrapados en un ciclo de pagos continuos destinados casi exclusivamente a cubrir intereses, sin posibilidad de liberarse de la deuda. Este esquema, en la práctica, no se configura como un préstamo legítimo sino como un mecanismo de sometimiento financiero, donde la aparente relación contractual encubre en realidad una forma de explotación permanente del deudor. De esta manera, lo que en apariencia es un contrato civil de mutuo se transforma en un dispositivo de intimidación digital, donde el incumplimiento de pago ya no genera un conflicto patrimonial, sino una situación de hostigamiento y coacción que afecta la libertad y la dignidad de la víctima.

Como advierte Miró, este tipo de prácticas se inscriben dentro de lo que denomina “ciberdelitos impuros”, es decir, aquellos en los que la tecnología no es el fin del delito, sino el medio que potencia la comisión de ilícitos clásicos como la estafa o la extorsión. La importancia de esta categoría radica en que obliga a un análisis jurídico más allá de la simple apariencia contractual indicando que lo relevante no es que exista un acuerdo formalizado, sino cómo la tecnología amplifica la capacidad de control del delincuente sobre la víctima (2012). En ese sentido, el préstamo “gota a gota” digital ilustra claramente la transformación de un delito económico tradicional en una forma sofisticada de ciberextorsión, cuya peligrosidad se multiplica por la rapidez, el anonimato y la capacidad de alcance que ofrece el entorno digital.

El legislador peruano ha reconocido esta tensión con la incorporación del artículo 8-A a la Ley 30096, que tipifica el “préstamo informático extorsivo”. Este precepto refleja que, cuando el supuesto contrato se acompaña de amenazas, engaños o

coacciones, deja de ser un negocio jurídico válido y pasa a configurarse como delito. Como señala Villavicencio, en el ámbito penal lo determinante no es la denominación contractual utilizada, sino la afectación de bienes jurídicos como la libertad de decisión y el patrimonio (2014).

3. Análisis jurídico del artículo 8-A de la Ley N.º 30096

La Ley N.º 32183, promulgada en diciembre de 2024, incorporó al ordenamiento peruano el artículo 8-A de la Ley N.º 30096 de Delitos Informáticos, con el propósito de sancionar específicamente los préstamos informáticos extorsivos, también denominados “gota a gota digitales”. Esta norma adapta la figura de la extorsión tradicional a los desafíos derivados de las nuevas tecnologías, reconociendo que las aplicaciones móviles y plataformas digitales se han convertido en vehículos para la comisión de prácticas usurarias y extorsivas.

El texto del artículo establece que se impondrá pena privativa de libertad no menor de diez ni mayor de quince años a quien, “mediante amenaza, intimidación, engaño, ardid o violencia, induzca u obligue a aceptar dinero o bienes que simulan un contrato de mutuo o cualquier otro”. Asimismo, incorpora agravantes que elevan la pena hasta veinticinco años en supuestos donde se emplee violencia física o cuando las víctimas pertenezcan a grupos vulnerables, como menores de edad, adultos mayores o personas con discapacidad.

Desde el punto de vista dogmático, el artículo 8-A presenta varias características relevantes. En primer lugar, tipifica un delito pluriofensivo, en la medida en que protege simultáneamente la libertad de decisión del individuo, su patrimonio y la seguridad de sus datos personales. Como explica Villavicencio, los delitos informáticos impuros son aquellos en los que la tecnología sirve como medio para potenciar la comisión de ilícitos tradicionales, lo que exige que el derecho penal adapte sus categorías a este nuevo contexto (2014), estando el artículo 8-A claramente en esta categoría, ya que no sanciona un ataque directo al sistema informático, sino el uso de este para generar un mecanismo extorsivo.

En segundo lugar, debe destacarse que el artículo 8-A, si bien representa un avance al sancionar el uso de mecanismos digitales de amenaza, engaño o simulación contractual, no logra abarcar plenamente la realidad del fenómeno. En la mayoría de los casos, los usuarios no son obligados a aceptar el préstamo,

sino que acceden voluntariamente debido a su necesidad urgente de dinero y a la exclusión del sistema financiero formal, esta decisión inicial, aunque tomada en condiciones de vulnerabilidad, no encaja en la lógica de la coacción prevista por el tipo penal, ya que, el problema radica en que la norma parte de la premisa de un consentimiento viciado desde el inicio, cuando en la práctica lo que ocurre es que el consentimiento es otorgado libremente y recién se transforma en un escenario extorsivo en la etapa de cobro, cuando el prestamista recurre a la intimidación digital; además, como advierte Miró, los delitos informáticos impuros se caracterizan precisamente por esa ambigüedad, en la que la tecnología no crea la coacción desde el inicio, sino que potencia y agrava conductas tradicionales como la extorsión en fases posteriores (2012).

Finalmente, aunque el artículo 8-A constituye un esfuerzo legislativo por visibilizar y sancionar el préstamo informático extorsivo, su alcance resulta todavía limitado frente a la realidad del fenómeno, pues en la mayoría de los casos, los usuarios no son obligados desde el inicio, sino que acceden voluntariamente al préstamo motivados por la necesidad económica y la exclusión del sistema financiero formal. La coacción aparece recién en la etapa de cobro, cuando el prestamista utiliza la información personal obtenida para intimidar a la víctima; en este sentido, la norma no logra abarcar del todo la dinámica real del “gota a gota” digital, pues parte de la idea de un consentimiento viciado desde el inicio, cuando en realidad se trata de un consentimiento aparente en el origen que se convierte posteriormente en un escenario de extorsión, ello muestra que, si bien la tipificación representa un avance, aún persisten desafíos normativos y dogmáticos a modificar.

3.1 Elementos del tipo penal: inducción, amenaza, engaño, simulación legal

El artículo 8-A de la Ley N.º 30096 tipifica el “préstamo informático extorsivo” sobre la base de cuatro elementos principales: la inducción, la amenaza, el engaño y la simulación legal. Estos componentes permiten delimitar el alcance del tipo penal y distinguirlo de otras figuras delictivas vinculadas al fraude o a la coacción.

En primer lugar, la inducción se refiere a la acción de convencer o persuadir a la víctima para que acepte el préstamo en condiciones abusivas, a diferencia de un

contrato civil de mutuo en el que el consentimiento es informado y libre, en el préstamo digital la inducción opera mediante la explotación de la necesidad económica y la promesa de inmediatez, Menacho señala que, el atractivo inicial de estas aplicaciones radica en la rapidez del desembolso, lo que genera en la víctima una confianza irreflexiva que facilita la aceptación de condiciones desventajosas (2024) y este elemento evidencia que la voluntad del prestatario está condicionada desde el inicio, lo que convierte a la inducción en un instrumento esencial para la consumación del delito.

En segundo lugar, la amenaza constituye el núcleo coactivo del tipo penal, pues en el “gota a gota digital”, la amenaza se despliega de manera virtual, a través de mensajes, llamadas o publicaciones en redes sociales, dirigidas no solo a la víctima, sino también a sus familiares o contactos, Cerezo advierte que esta forma de ciberextorsión tiene como particularidad el uso de la reputación digital como herramienta de presión, lo que incrementa la sensación de indefensión de la víctima y refuerza el carácter inmaterial del daño (2020), por tanto, la amenaza, no se limita a exigir el pago de la deuda, sino que compromete bienes jurídicos como la privacidad y la dignidad.

El tercer elemento es el engaño, entendido como la utilización de artificios o ardidés para inducir a la víctima a aceptar un préstamo que no corresponde a una relación contractual legítima. En este contexto, el engaño suele manifestarse en la creación de aplicaciones que simulan ser entidades financieras formales, el ofrecimiento de tasas falsas o la omisión de cláusulas relativas a comisiones y penalidades, buscando generar una apariencia de legitimidad que encubre el verdadero propósito extorsivo.

Finalmente, la simulación legal se refiere al uso de contratos o figuras jurídicas aparentes que, en realidad, no constituyen verdaderos negocios válidos, ya que, el artículo 8-A sanciona a quienes obligan a aceptar dinero o bienes bajo la apariencia de un contrato de mutuo u otro semejante. En la práctica, estos contratos simulados sirven como fachada para legitimar prácticas usurarias y coercitivas, presentando al usuario un acuerdo formal que, en esencia, nunca busca el cumplimiento de obligaciones bilaterales justas, sino el sometimiento del deudor a un ciclo de deuda creciente y a mecanismos de presión. Como advierte Miró, en el análisis de los delitos digitales no basta con atender a la

forma contractual, sino que debe valorarse el contexto tecnológico y social en el que la conducta se desarrolla (2012).

Esta apariencia de legalidad introduce un problema dogmático importante, pues si se observa desde una perspectiva estrictamente civil, el prestatario da su consentimiento al préstamo, lo que le otorga cierta validez formal al contrato; sin embargo, ese consentimiento no responde a una negociación libre e informada, sino a una aceptación condicionada por la necesidad económica y la estructura prediseñada del aplicativo, que oculta comisiones, penalidades y el uso indebido de datos personales. Así, lo que en principio parece un acto jurídico válido se transforma, en su desarrollo, en un mecanismo de intimidación y sometimiento, donde la supuesta legalidad funciona únicamente como una pantalla que encubre la actividad delictiva.

De esta manera, la simulación contractual se convierte en una herramienta estratégica para los prestamistas digitales, quienes logran ocultar la verdadera naturaleza del delito bajo la forma de un mutuo civil, ello genera una dificultad adicional para la aplicación del artículo 8-A, ya que la norma se construye sobre la base de que la coacción o el engaño operan desde el inicio, cuando en realidad la mayoría de usuarios accede voluntariamente al préstamo y es recién en la fase de incumplimiento cuando la intimidación digital convierte la relación en una extorsión. En consecuencia, la figura de la simulación legal pone en evidencia la sofisticación de los ciberdelincuentes y al mismo tiempo muestra los límites de la respuesta penal, que debe avanzar hacia un entendimiento más realista de estas prácticas híbridas entre lo contractual y lo delictivo.

En conjunto, estos cuatro elementos demuestran que el artículo 8-A no se limita a sancionar una simple práctica usuraria, sino que configura un delito complejo en el que la inducción, la amenaza, el engaño y la simulación se integran como partes de un proceso destinado a someter económica, psicológica y socialmente a la víctima. La identificación de cada uno de estos elementos resulta crucial para la adecuada aplicación del tipo penal, evitando confusiones con otras figuras como la estafa o la coacción, y asegurando la eficacia de la respuesta jurídica frente a un fenómeno en constante evolución.

4. Extorsión digital como consecuencia del incumplimiento del pago.

Una de las características más graves del préstamo “gota a gota digital” es que, en caso de incumplimiento de los pagos, la relación contractual simulada se transforma en un escenario de extorsión, el acreedor ilegal ya no actúa como prestamista, sino como un agente de coacción que utiliza la información personal recopilada durante la instalación de la aplicación como medio de presión. En este punto, el problema deja de ser meramente patrimonial y se convierte en un fenómeno de victimización múltiple, en el que confluyen el hostigamiento psicológico, la destrucción de la reputación digital y la amenaza constante de exposición social.

Menacho explica que esta fase delictiva constituye el verdadero núcleo del préstamo informático extorsivo, pues es aquí donde se evidencia la finalidad última de los prestamistas que es someter al deudor no por medios legales de cobro, sino mediante intimidaciones digitales persistentes (2024). La deuda se convierte, de este modo, en una excusa para desencadenar un proceso de hostigamiento que genera en la víctima una sensación de indefensión prolongada.

Según Cerezo, la extorsión digital presenta particularidades que la diferencian de la extorsión clásica debido a que el daño no es necesariamente material inmediato, sino que se centra en la amenaza de divulgar información privada que afecta la reputación y la vida social de la persona (2020). En el contexto del “gota a gota” digital, esta amenaza se materializa en llamadas telefónicas, mensajes intimidatorios y, en muchos casos, en la publicación de fotografías o conversaciones en redes sociales dirigidas no solo contra la víctima, sino también contra sus familiares y contactos, convirtiendo la extorsión en un proceso expansivo, que multiplica los efectos negativos más allá del deudor directo. La Superintendencia Financiera de Colombia ha advertido que este tipo de prácticas configuran un “círculo de violencia digital”, en el que las víctimas son acosadas sistemáticamente hasta que realizan pagos forzados, sin que exista la intención de extinguir la deuda (Superintendencia Financiera de Colombia, 2025). De manera similar, la Policía Cibernética de la Ciudad de México ha reportado múltiples casos en los que las aplicaciones de préstamo ilegal enviaban mensajes de difamación masiva a los contactos de las víctimas como represalia por la falta de pago (SSC México, 2023).

Desde el plano jurídico, la extorsión digital como consecuencia del incumplimiento del pago pone de manifiesto que el contrato nunca fue genuino, sino que sirvió como fachada para establecer un mecanismo de coacción. Como advierte Villavicencio, lo relevante en estos casos no es la formalidad del mutuo, sino la afectación de bienes jurídicos como la libertad individual y el patrimonio, que son vulnerados mediante la intimidación ilegítima (2014). En consecuencia, el incumplimiento del pago no debería analizarse bajo la óptica civil del deudor moroso, sino bajo la perspectiva penal de la víctima sometida a un proceso extorsivo.

TERCERA PARTE: CONTRASTACIÓN DE HIPÓTESIS, TOMA DE POSTURA Y CONSECUENCIAS

1. Contrastación de las hipótesis

En el caso de la presente tesis, el proceso de contrastación se orienta a examinar la correspondencia entre el fenómeno empírico del “gota a gota” digital y el marco jurídico establecido por el artículo 8-A de la Ley N.º 30096, así como a evaluar si la actual regulación penal es suficiente para sancionar las conductas delictivas que surgen de los préstamos extorsivos realizados mediante aplicativos móviles.

Para tal efecto, se contrastó los fundamentos doctrinarios con los hechos observables y las manifestaciones actuales del fenómeno partiendo del reconocimiento de que el “gota a gota” digital no constituye un hecho aislado, sino una evolución tecnológica de prácticas usureras y coercitivas preexistentes. En ese sentido, se buscó establecer si el marco normativo vigente, particularmente el artículo 8-A de la Ley de Delitos Informáticos, responde adecuadamente a esta nueva modalidad delictiva o si, por el contrario, deja espacios de impunidad debido a su formulación restrictiva centrada en la inducción o coacción inicial.

La contrastación también permite verificar si las conductas asociadas al préstamo digital informal pueden subsumirse dentro de los tipos penales tradicionales de extorsión (artículo 200 del Código Penal) o de estafa (artículo 196), o si requieren un tratamiento penal autónomo. En este punto, el estudio de autores como Miró (2012), Rodríguez (2015) y Menacho (2024) resulta determinante, pues sus análisis evidencian cómo la digitalización no crea nuevos

bienes jurídicos; sino que transforma los medios de agresión y amplifica la capacidad de control de los delincuentes sobre las víctimas.

Asimismo, el proceso de contrastación permitió identificar que la mayoría de las víctimas acceden voluntariamente al préstamo, pero terminan siendo objeto de extorsión posterior mediante el uso indebido de sus datos personales; también permitió entender que el artículo 8-A no logra abarcar estos supuestos, dado que su estructura típica exige la existencia de inducción o amenaza previa, y, finalmente, que esta limitación genera vacíos normativos que obstaculizan la persecución penal efectiva.

1.1. Análisis e interpretación del problema planteado

El problema central de esta investigación se orienta a determinar si el fenómeno denominado “gota a gota” digital puede ser subsumido en el tipo penal previsto en el artículo 8-A de la Ley N.º 30096, conforme a los principios del sistema penal peruano, esta interrogante surge de la necesidad de examinar la adecuación típica del préstamo extorsivo digital dentro del presente marco normativo.

El artículo 8-A, incorporado por la Ley N.º 32183, establece la sanción para quien, mediante amenaza, intimidación, engaño o ardid, induce u obliga a aceptar dinero o bienes que simulan un contrato de mutuo o cualquier otro; sin embargo, su redacción genera dudas sobre su capacidad para abarcar situaciones en las que la víctima accede voluntariamente al préstamo y el acto extorsivo ocurre de manera posterior, esta problemática radica en la disparidad entre el texto legal y la realidad delictiva, ya que, en la práctica, los usuarios que recurren a préstamos digitales lo hacen de forma voluntaria, motivados por la urgencia económica y la exclusión del sistema financiero formal; no obstante, esta decisión inicial desemboca en un proceso de hostigamiento cuando las aplicaciones utilizan la información personal del prestatario para ejercer presión psicológica o extorsión digital, poniendo en cuestión si la tipicidad penal debe ampliarse para abarcar la coacción posterior.

Desde una perspectiva doctrinal, Villavicencio sostiene que la interpretación de los tipos penales debe considerar la afectación real de los bienes jurídicos protegidos, en este caso la libertad individual, la intimidad y el patrimonio (2014); conforme a ello, si el daño se produce después del consentimiento inicial, el

derecho penal no puede permanecer inactivo bajo el pretexto de la voluntariedad del acto. De igual manera, Miró distingue los llamados ciberdelitos impuros, en los cuales la tecnología no constituye el fin, sino el medio que potencia la comisión de delitos clásicos como la estafa o la extorsión (2012), siendo que, el fenómeno del “gota a gota digital” se ubica precisamente en esta categoría de delitos impuros, en tanto combina un componente económico, que es el préstamo usurario, con un componente tecnológico, como el acceso y uso indebido de datos personales, para generar una situación de coerción; por tanto, se debe determinar si el tipo penal actual logra abarcar esta complejidad o si resulta insuficiente frente a la realidad criminológica y tecnológica del delito.

1.1.1 Hipótesis principal

La contrastación de la hipótesis principal permite afirmar que el fenómeno denominado "gota a gota digital" no puede subsumirse dentro del tipo penal previsto en el artículo 8-A de la Ley N.º 30096, confirmándose la validez de la hipótesis planteada en el marco teórico. La presente investigación demostró que este tipo penal fue diseñado para sancionar conductas en las cuales el consentimiento de la víctima se encuentra viciado desde el inicio por medios como la inducción, la amenaza, la intimidación, el engaño o el ardid; en cambio, en el caso del “gota a gota digital”, el prestatario, en la mayoría de casos, acepta voluntariamente el préstamo desde un inicio, lo que genera un problema de atipicidad penal, dado que el verbo rector del tipo “inducir u obligar” no se configura en esta modalidad.

La doctrinal y normativa realizado permite constatar que la estructura del artículo 8-A responde a un modelo de engaño inicial, propio de los fraudes informáticos o de los contratos simulados; no obstante, el fenómeno del préstamo digital extorsivo se desarrolla en dos fases distintas: una primera, donde el usuario solicita voluntariamente el préstamo a través de una aplicación o red social; y una segunda, en la que, ante el incumplimiento del pago, el prestamista utiliza los datos personales obtenidos del dispositivo móvil para intimidar, coaccionar o humillar públicamente al prestatario, siendo esta segunda fase donde se materializa la verdadera lesividad penal, ya que el acto de hostigamiento se convierte en un mecanismo de extorsión.

En consecuencia, el “gota a gota digital” no puede ser comprendido dentro de la figura penal actual porque la extorsión no antecede al consentimiento, sino que

aparece con posterioridad, este rasgo temporal modifica la estructura del tipo penal y deja fuera de sanción especializada a una práctica que resulta atípica desde la perspectiva jurídica. Como sostiene Villavicencio, la tipicidad penal no puede construirse sobre supuestos que no estén expresamente contemplados en la norma, pues ello vulneraría el principio de legalidad (2014); por tanto, la falta de adecuación típica del “gota a gota digital” al artículo 8-A confirma que el legislador no ha captado la naturaleza evolutiva del delito, la cual se transforma en una conducta extorsiva.

En este contexto, la hipótesis principal se confirma plenamente al contrastar que el artículo 8-A de la Ley N.º 30096 no puede aplicarse al fenómeno del “gota a gota digital”, debido a que el tipo penal requiere una coacción o engaño previo a la aceptación del préstamo, mientras que en esta modalidad el consentimiento inicial suele ser voluntario y la coacción surge posteriormente, evidenciando la necesidad de reformular el tipo penal para incorporar la fase extorsiva posterior al contrato, adecuando la norma a la realidad del fenómeno criminal.

1.1.2 Primera hipótesis secundaria

La primera hipótesis secundaria plantea que el fenómeno denominado “gota a gota” digital constituye una práctica extorsiva, en la medida en que, los métodos de cobro empleados por los prestamistas implican amenazas, coacción y hostigamiento digital destinados a obtener el pago mediante la intimidación, tras la contrastación teórica y empírica, se confirma que esta afirmación resulta válida, dado que el elemento determinante no es el modo en que se origina la obligación, sino la manera en que se exige su cumplimiento a través de medios ilícitos y vulnerando la libertad personal.

En efecto, los aplicativos móviles que ofrecen préstamos inmediatos sin garantías aparentes recurren a mecanismos de presión que exceden el ámbito contractual y se insertan en la lógica penal de la extorsión, tal como señala Menacho, estas plataformas obtienen acceso a información sensible del usuario como contactos, fotografías, mensajes y ubicación con el pretexto de evaluar su capacidad crediticia(2024); sin embargo, una vez otorgado el préstamo, dicha información es utilizada como instrumento de coerción, transformando la dinámica en sometimiento digital por la amenaza de difundir información privada

o de exponer públicamente la deuda buscando de esta forma, quebrar la voluntad de la víctima y asegurar el beneficio económico del prestamista.

Asimismo, Cerezo destaca que en las ciberextorsiones, el daño no radica únicamente en la pérdida patrimonial, sino en el impacto emocional y reputacional que sufren las víctimas (2024), en este caso, el “gota a gota digital” reproduce este patrón, ya que el miedo a la humillación pública o al perjuicio social obliga a las personas a cumplir con los pagos exigidos, incluso en condiciones de abuso.

Por otro lado, la práctica extorsiva se evidencia en la intención del prestamista, cuyo propósito no es recuperar el dinero legítimamente prestado, sino obtener un provecho económico indebido mediante la intimidación, según Rodríguez, en el esquema tradicional del “gota a gota” los cobradores recurrían a la intimidación física o verbal para mantener un flujo constante de intereses (2015); la digitalización no ha eliminado esa violencia, sino que la ha trasladado al ciberespacio, donde el control se ejerce mediante la vigilancia y la amenaza de exposición social, por tanto, el elemento coercitivo permanece intacto, aunque haya cambiado el medio de ejecución. En este sentido, puede afirmarse que el “gota a gota” digital representa una mutación tecnológica del delito de extorsión previsto en el artículo 200 del Código Penal al representar un sujeto activo que, mediante amenazas o intimidación, obliga a otro a entregar dinero o a realizar un acto contra su voluntad diferenciándose únicamente en el soporte digital y en el uso instrumental de los datos personales como medio de presión.

1.1.3 Segunda hipótesis secundaria

La segunda hipótesis secundaria parte de la premisa de que la tipicidad del delito previsto en el artículo 8-A de la Ley N.º 30096 se construye exclusivamente sobre las acciones de inducción u obligación inicial mediante amenaza, intimidación, engaño o ardid, dejando fuera de su ámbito de aplicación los casos en que la víctima accede voluntariamente al préstamo, pero luego es sometida a mecanismos de coacción o extorsión digital, demostrando que el tipo penal vigente no alcanza la complejidad del fenómeno del “gota a gota digital” en su configuración actual, ya que, esta redacción evidencia que el foco del tipo penal se sitúa en el momento de la aceptación del préstamo, entendiendo la coacción o el engaño como condición necesaria para que la conducta sea punible; sin

embargo, como se ha demostrado en el desarrollo de esta investigación, la gran mayoría de los casos de préstamos digitales no inician con una amenaza, sino con una decisión voluntaria de la víctima, motivada por su necesidad económica.

En ese sentido, como se ha señalado, el delito no se configura al inicio de la relación, sino durante la fase de cobro, cuando el prestamista emplea la información personal recopilada a través del aplicativo para intimidar o extorsionar al deudor. Este desfase entre la conducta típica y la realidad práctica genera un problema de atipicidad material, pues la norma no alcanza a sancionar los actos más frecuentes del fenómeno, como sostiene Villavicencio, en el derecho penal debe atenderse no solo a la forma del contrato, sino a la afectación efectiva de bienes jurídicos como la libertad de decisión, la intimidad y el patrimonio(2014), siendo que, en el caso del “gota a gota digital”, el consentimiento inicial no elimina el carácter delictivo del comportamiento posterior, ya que la intimidación transforma un negocio aparentemente lícito en un acto de extorsión.

Por otro lado, la doctrina sobre los ciberdelitos impuros, desarrollada por Miró, resulta especialmente útil para entender este vacío, el autor explica que los delitos impuros son aquellos en los que la tecnología no constituye el fin, sino el medio que potencia y amplifica conductas tradicionales como la estafa o la extorsión (2012). Bajo esta lógica, el préstamo digital informal no puede analizarse únicamente desde el consentimiento contractual, sino desde el uso abusivo de los medios tecnológicos que facilitan la coacción posterior; la ley peruana, al ceñirse únicamente a la fase inicial del préstamo, pierde la perspectiva integral del delito y deja sin sanción los actos de hostigamiento que, en la práctica, representan el núcleo del daño. Asimismo, se advierte que el problema de esta redacción radica en la falsa presunción de coacción previa, Menacho explica que, en la mayoría de los casos, los usuarios descargan las aplicaciones de manera consciente, aceptan los términos y autorizan el acceso a sus datos sin comprender las consecuencias de esa cesión (2024); sin embargo, al no existir una “inducción” ni una “obligación” en el momento del consentimiento, el artículo 8-A no puede aplicarse de manera directa, lo que genera impunidad frente a los hechos más comunes en la práctica.

De este modo, la regulación actual responde a una concepción centrada en la voluntad inicial del prestatario, sin advertir que el verdadero bien jurídico lesionado surge en la etapa de cobro, la digitalización del crédito informal ha modificado radicalmente las condiciones de riesgo, y el marco penal no ha evolucionado al mismo ritmo; por ello, esta hipótesis reafirma la necesidad de una reforma legislativa que amplíe la tipicidad del artículo 8-A, incorporando los supuestos en los que el consentimiento inicial se convierte, a través del abuso digital, en un mecanismo de extorsión encubierta.

2. Presentación de la postura personal

Desde una perspectiva jurídica y práctica, resulta innegable que la incorporación del artículo 8-A a la Ley N.º 30096 de Delitos Informáticos representó un paso adelante en la política criminal peruana, pues permitió visibilizar y sancionar una modalidad delictiva emergente asociada al uso de las tecnologías de la información con fines extorsivos; no obstante, la configuración típica del “préstamo informático extorsivo” evidencia una limitación estructural al asumir que la víctima es inducida u obligada desde el inicio a aceptar un préstamo mediante coacción, engaño o amenaza cuando en la realidad del fenómeno del “gota a gota digital”, esta presunción no se cumple en la mayoría de los casos.

La evidencia recogida por estudios sobre estas prácticas en entornos digitales, tanto en el Perú como en otros países de América Latina, demuestra que los usuarios suelen acceder voluntariamente a los préstamos ofrecidos a través de aplicaciones móviles o redes sociales, impulsados por la necesidad económica inmediata, el desempleo, la informalidad o la exclusión del sistema bancario formal. Como señala Rodríguez, en el préstamo informal tradicional los prestatarios ya partían de una posición de vulnerabilidad estructural, pues el acceso al crédito formal les era negado por carecer de historial crediticio o de garantías; esta misma lógica de exclusión se replica ahora en el entorno digital, donde la aparente libertad del usuario para aceptar el préstamo encubre una situación de necesidad económica que distorsiona la verdadera autonomía de su voluntad (2015).

En este sentido, el problema central del artículo 8-A radica en que su verbo rector “inducir u obligar” no refleja con precisión el mecanismo de acción del delito en su etapa inicial, en la mayoría de los casos, el usuario no es víctima de una

inducción ilícita previa, sino que se somete voluntariamente a condiciones contractuales abusivas a cambio de una solución financiera urgente. Por ello, la redacción del tipo penal deja fuera una gran cantidad de supuestos en los que la conducta delictiva se perfecciona con posterioridad, cuando el prestamista utiliza la información personal de la víctima para ejercer presión o intimidación digital, configurando una verdadera ciberextorsión derivada del préstamo.

Desde este punto de vista, el artículo 8-A incurre en un error de enfoque temporal debido a que centra su atención en el acto inicial de aceptación del préstamo, pero no considera que el núcleo lesivo del delito se produce con posterioridad, cuando el acreedor transforma el acuerdo en un instrumento de amenaza. Es importante añadir que, como advierte Miró, muchos delitos digitales “impuros” no pueden analizarse desde las categorías tradicionales del derecho penal, ya que el entorno tecnológico amplifica la capacidad de control del agente y modifica la forma en que se concreta el daño (2012), siendo que en el presente caso, la afectación penalmente relevante surge en el momento en que el prestamista, valiéndose de los datos obtenidos por medios legítimos, los convierte en herramientas de coacción donde la amenaza se materializa a través del acceso a contactos, fotografías o archivos que luego son utilizados para amenazar al deudor. De esta manera, el fenómeno no encaja plenamente en el marco del artículo 8-A, pues la coacción no precede al contrato, sino que lo sucede y lo distorsiona.

Por tanto, sostengo que el artículo 8-A, aunque constituye un avance, no comprende la esencia del fenómeno delictivo, ya que tipifica el acto inicial y no la dinámica extorsiva posterior, lo cual genera una brecha entre la realidad criminal y la respuesta jurídica, por ende, se requiere una redefinición integral que incorpore esta evolución criminológica. No basta con castigar al prestamista que induce o engaña para otorgar un préstamo; debe sancionarse también al que, habiendo celebrado un contrato, utiliza la información personal obtenida de manera digital para presionar, amenazar o extorsionar a la víctima, ya que, solo de este modo se logrará una protección penal efectiva frente a un delito que se perfecciona en el ámbito digital.

3. Propuesta de solución del problema.

La regulación actual del artículo 8-A de la Ley N.º 30096 adolece de una limitación dogmática y práctica, pues su redacción se concentra en el momento inicial y no en el proceso delictivo posterior que caracteriza al préstamo extorsivo digital; en efecto, el tipo penal sanciona a quien “mediante amenaza, intimidación, engaño, ardid o violencia induce u obliga a aceptar dinero o bienes que simulan un contrato de mutuo o cualquier otro”, lo que presupone una coacción o engaño en el instante de la aceptación del préstamo; no obstante, como se ha demostrado, la mayoría de víctimas accede al crédito digital de forma aparentemente voluntaria, impulsada por su necesidad económica y la falta de acceso al sistema financiero formal.

De ahí que resulte imprescindible una reformulación del tipo penal, orientada a reflejar la verdadera dinámica del delito, en este sentido, la norma debería ampliar su alcance para sancionar también las conductas que surgen después de la aceptación del préstamo, cuando el acreedor, amparado en la autorización de acceso a datos, amenaza con divulgar información privada o ejerce presión mediante amenazas para obtener un beneficio indebido; por tanto, se propone modificar el artículo 8-A de la Ley N.º 30096, añadiendo un segundo párrafo que precise el carácter progresivo del delito y su conexión con las tecnologías de la información, siendo posible la siguiente redacción:

“Asimismo, será reprimido con la misma pena quien, habiendo obtenido el consentimiento del usuario para otorgarle un préstamo o crédito mediante plataformas digitales, utilice la información personal, contactos, archivos o datos de su dispositivo con el propósito de coaccionar, intimidar o extorsionar al prestatario, buscando obtener un beneficio económico indebido o la ejecución forzada del pago.”

Esta adición permitiría sancionar adecuadamente los supuestos más frecuentes en la práctica del “gota a gota” digital, donde el usuario no es víctima de coacción inicial, pero sí de hostigamiento posterior; además, la propuesta refuerza la protección de bienes jurídicos como la libertad individual, la privacidad y la seguridad digital, los cuales hoy quedan insuficientemente tutelados. Concluyendo que, al incorporar esta conducta como una forma autónoma de extorsión digital derivada del préstamo, el marco penal se adecuaría mejor a la realidad de las víctimas y reduciría los márgenes de impunidad.

Asimismo, la propuesta encuentra respaldo en la experiencia comparada; en Colombia, la Superintendencia Financiera ha advertido sobre la necesidad de fortalecer los mecanismos penales para sancionar los “préstamos gota a gota virtuales”, donde el consentimiento inicial se desvirtúa posteriormente por las amenazas y difusiones de datos personales. De igual modo, en México, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) ha impulsado reformas para sancionar a las aplicaciones de préstamo rápido que “emplean tácticas de intimidación digital, con acceso a la información privada del usuario”, reconociendo que el delito se configura con posterioridad al contrato, estas experiencias reflejan que el derecho comparado ya ha identificado el mismo vacío que enfrenta la legislación peruana.

En consecuencia, la propuesta de modificación del artículo 8-A busca alinear el derecho penal nacional con la realidad criminológica contemporánea al incluir la fase de amenaza y uso indebido de datos personales, el tipo penal lograría una mayor correspondencia con la práctica delictiva y permitiría sancionar de manera efectiva las conductas más frecuentes en el fenómeno del “gota a gota” digital. De igual forma, la propuesta refuerza la protección de bienes jurídicos como la libertad individual, la privacidad, la seguridad informática y la dignidad humana, que hoy se ven gravemente comprometidos por el empleo de medios tecnológicos para la presión económica.

Finalmente, es necesario precisar que esta reforma no busca criminalizar la necesidad económica ni la decisión voluntaria de acceder a un préstamo informal, sino sancionar el uso posterior y abusivo de los medios digitales como herramientas de intimidación y control. En suma, la modificación propuesta no sustituye el contenido del artículo 8-A, sino que lo complementa, extendiendo su aplicación a las fases más comunes del delito y asegurando que el Derecho Penal peruano mantenga la coherencia con el principio de intervención mínima del Derecho Penal, garantizando que la respuesta jurídica se dirija únicamente contra las conductas que, bajo apariencia contractual, transforman la relación económica en un mecanismo de extorsión tecnológica.

4. Impacto de la implementación de la propuesta.

La implementación de la modificación propuesta al artículo 8-A de la Ley N.º 30096 tendría un impacto trascendental en diversos niveles del orden jurídico, social e institucional, al adecuar la respuesta penal a la realidad actual del fenómeno del “gota a gota” digital. En primer lugar, a nivel penal, la reforma permitiría superar la rigidez dogmática del tipo vigente, que limita la punibilidad a los supuestos en los que la víctima fue inducida u obligada a aceptar el préstamo mediante amenaza o engaño, ya que, al incorporar la posibilidad de sancionar también el hostigamiento posterior al consentimiento inicial, se cubriría el vacío normativo que hoy deja impunes los casos más frecuentes, en los que el delito se perfecciona cuando el prestamista utiliza los medios digitales para presionar o extorsionar al deudor.

Desde una perspectiva dogmática, esta ampliación fortalecería la coherencia interna del sistema penal, al reconocer la naturaleza progresiva y dinámica de este tipo de criminalidad, debido a que el préstamo digital no constituye un hecho aislado, sino un proceso que inicia con una apariencia contractual y culmina con la instrumentalización de los datos personales como herramienta de coacción; en este sentido, la reforma permitiría al operador de justicia reconstruir el delito en su totalidad, entendiendo que la afectación de bienes jurídicos como la libertad, la autodeterminación y la seguridad digital se produce en la fase de cobro, no en el momento del consentimiento en adición, como señala Villavicencio, el derecho penal no puede limitarse a las formas externas de la conducta, sino que debe proteger efectivamente los valores esenciales de la persona frente a nuevas modalidades de coerción, sean físicas, económicas o tecnológicas (2014).

La modificación, además, no supone una expansión punitiva arbitraria, sino una adecuación racional del tipo penal a las condiciones contemporáneas del delito, como sostiene Miró, los ciberdelitos impuros que son aquellos en los que la tecnología potencia las formas tradicionales de agresión exigen respuestas jurídicas flexibles que contemplen la función instrumental de los medios digitales (2012) y, aplicado al caso del préstamo informal digital, esto implica reconocer que el riesgo no se origina en el contrato mismo, sino en la manipulación tecnológica posterior; por tanto, la reforma ampliaría la eficacia del artículo 8-A

sin contradecir el principio de legalidad penal, sino precisando el alcance del verbo rector frente a la evolución del fenómeno.

En segundo lugar, la propuesta tendría un impacto significativo en la eficacia de la persecución penal pues el Ministerio Público y la policía nacional contarían con una base normativa más clara para tipificar las denuncias relacionadas con los préstamos extorsivos digitales, eliminando la actual incertidumbre en la cual muchas investigaciones son archivadas por considerarse “conflictos contractuales”, pese a que los hechos posteriores en los que se encuentran las amenazas, difusión de datos personales o el hostigamiento psicológico, configuran una extorsión encubierta. Con la modificación, se unificarían los criterios interpretativos, fortaleciendo la persecución penal para poder identificar a los responsables.

En el plano social, la reforma representaría un avance en la protección de los sectores económicamente vulnerables, que constituyen el blanco principal de estas redes delictivas, Rodríguez señala que, el préstamo informal genera un círculo vicioso de dependencia y hostigamiento que deteriora la estabilidad económica y emocional de las víctimas (2015), y, en su versión digital, este patrón se agrava por el uso de información íntima como mecanismo de presión, entonces, reconocer penalmente este abuso posterior al contrato significaría un acto de justicia social, pues el Estado dejaría de asumir que la necesidad económica implica consentimiento real, enfocando esta modificación en sancionar la explotación digital de la vulnerabilidad, reafirmando la función protectora del derecho penal.

Asimismo, la implementación de esta modificación contribuiría al fortalecimiento de la educación digital y la cultura de ciberseguridad, como advierte Miró, la prevención del cibercrimen no puede basarse únicamente en la sanción, sino también en la concienciación ciudadana (2012) y, visibilizando penalmente la práctica del “gota a gota digital” se incentivaría la creación de campañas educativas sobre el manejo responsable de la información personal, los permisos de las aplicaciones móviles y los riesgos de los préstamos informales en línea, reforzando la prevención primaria del delito y promoviendo una mayor alfabetización tecnológica, especialmente en los sectores más expuestos.

Finalmente, el impacto político-criminal de la reforma se proyectaría en la consolidación de un derecho penal más humano y realista, como afirma Menacho, el Estado debe adaptar sus herramientas normativas a los nuevos escenarios tecnológicos, sin perder de vista la dignidad humana como límite al poder punitivo (2024), se debe tener en cuenta que la modificación del artículo 8-A no busca castigar la necesidad económica ni la decisión voluntaria de quien acude a un préstamo informal, sino sancionar el uso abusivo de los medios digitales para controlar, amenazar o extorsionar a las víctimas; además, este matiz garantista asegura que la intervención penal se mantenga dentro de los principios de proporcionalidad y subsidiariedad, reafirmando la confianza de la sociedad en un sistema de justicia capaz de proteger sin criminalizar la vulnerabilidad.

5. Consecuencias

La implementación de una reforma penal como la propuesta en el artículo 8-A de la Ley N.º 30096 generaría una serie de consecuencias relevantes que deben analizarse desde distintas dimensiones: jurídica, social, institucional y político-criminal, estas repercusiones no se limitan únicamente a la ampliación del marco punitivo, sino que abarcan transformaciones profundas en la forma en que el Estado, el Derecho Penal y la sociedad comprenden y enfrentan las nuevas manifestaciones del delito en entornos digitales.

Desde el punto de vista jurídico, la consecuencia más inmediata sería la reconfiguración del ámbito de punibilidad del delito informático extorsivo, al reconocer que el consentimiento inicial de la víctima no excluye necesariamente la tipicidad penal. Con esta modificación, el Derecho Penal peruano asumiría una visión más realista de las relaciones económicas digitales, comprendiendo que el poder coercitivo no siempre se manifiesta de manera abierta, sino que puede expresarse mediante mecanismos tecnológicos de control y manipulación de información Villavicencio sostiene que el Derecho Penal debe evolucionar hacia una protección material de los bienes jurídicos, superando las barreras formales de los contratos o de los actos de consentimiento (2014) y esta nueva configuración del tipo penal fortalecería la tutela de bienes como la libertad de autodeterminación, la integridad psicológica y la privacidad digital, consolidando un modelo de protección más acorde con los desafíos de la era tecnológica.

Asimismo, una consecuencia positiva sería la reducción de la impunidad estructural que hoy caracteriza a los préstamos digitales extorsivos, ya que, muchos de estos casos quedan archivados en el sistema judicial bajo el argumento de que no existe inducción o amenaza inicial; con la reforma propuesta, las autoridades tendrían un marco más amplio para la persecución penal, evitando la desnaturalización del fenómeno, ello permitiría mayor uniformidad en la calificación jurídica de los hechos y en los criterios de imputación fiscal, garantizando un tratamiento más homogéneo y justo para las víctimas. Además, esta ampliación del tipo penal fortalecería el principio de legalidad material, al ofrecer una norma clara, precisa y previsible frente a las conductas que se pretenden sancionar.

En el plano social, las consecuencias serían igualmente significativas. La tipificación explícita del uso indebido de datos personales con fines extorsivos contribuiría a reconstruir la confianza ciudadana en el sistema de justicia, al demostrar que el Estado es capaz de adaptarse a las nuevas formas de criminalidad y proteger efectivamente a los sectores más vulnerables, Rodríguez recuerda que, el “gota a gota” tradicional constituye un fenómeno que perpetúa la desigualdad social, la exclusión económica y el miedo colectivo(2015), siendo de manera similar su versión digital; en este sentido, la intervención penal no solo tendría un carácter represivo, sino también restaurador y preventivo, al frenar la expansión de prácticas que degradan la dignidad de las personas y reproducen relaciones de sometimiento económico. Además, la reforma podría brindar medidas orientadas a la prevención, detección y denuncia temprana de estos delitos, como advierte Miró, el combate al cibercrimen requiere estrategias integrales que combinen la sanción penal con la reducción de oportunidades delictivas mediante educación, diseño tecnológico seguro y responsabilidad social digital (2012) y esta visibilización legal del fenómeno serviría también como un disuasivo simbólico, al establecer un mensaje claro el cual sería que la explotación de la vulnerabilidad económica a través de medios tecnológicos no quedará impune.

Desde la perspectiva institucional, la reforma implicaría la necesidad de fortalecer las capacidades técnicas y humanas de las unidades de investigación en delitos informáticos del Ministerio Público y la Policía Nacional, debido a que

la persecución eficaz de los préstamos extorsivos digitales exige conocimientos en trazabilidad de datos, análisis de redes y cooperación internacional. De este modo, el impacto institucional de la reforma no se reduciría a la modificación del texto legal, sino que implicaría una modernización del sistema penal para afrontar las nuevas manifestaciones del crimen organizado digital; ello podría incluso generar efectos positivos en la articulación con organismos internacionales y plataformas tecnológicas, permitiendo el rastreo de aplicaciones fraudulentas y la localización de redes transnacionales de extorsión económica.

Por otro lado, las consecuencias político-criminales de la reforma serían de gran trascendencia; en primer lugar, la ampliación del artículo 8-A contribuiría a consolidar una política criminal coherente con la realidad social y tecnológica del país, dejando atrás el enfoque meramente reactivo frente a la criminalidad digital; en segundo lugar, otorgaría mayor legitimidad al Derecho Penal como instrumento de protección ciudadana, no solo frente a la violencia física, sino también frente a las nuevas formas de agresión psicológica y económica que surgen en el ciberespacio, Menacho afirma que, el desafío del legislador contemporáneo es “reconocer que el daño digital no solo destruye sistemas informáticos, sino también proyectos de vida”(2024), de ahí que la consecuencia más profunda de esta reforma sería la reafirmación del Derecho Penal como garante de la dignidad humana en entornos digitales.

Finalmente, las consecuencias de la implementación de esta propuesta se proyectan hacia una transformación cultural del sistema de justicia y de la percepción social del delito digital, ya que, la tipificación más completa del préstamo informático extorsivo no solo fortalecería la respuesta punitiva, sino que fomentaría una conciencia colectiva sobre la necesidad de responsabilidad digital, tanto en los usuarios como en las empresas tecnológicas; en suma, esta reforma no solo corregiría un vacío normativo, sino que impulsaría un cambio estructural hacia un Derecho Penal más adaptativo, inclusivo y garantista, capaz de responder con efectividad a los desafíos tecnológicos vigentes.

6. Conclusiones

El análisis integral del fenómeno del “gota a gota digital” ha permitido constatar que este constituye una evolución criminológica del préstamo informal

tradicional, caracterizada por la utilización de herramientas tecnológicas como medio de captación, control y coacción, a través del estudio doctrinal, normativo y comparado, se ha evidenciado que esta modalidad delictiva no solo reproduce las lógicas de la usura y la intimidación propias del “gota a gota” físico, sino que las amplifica exponencialmente gracias al acceso a información personal y a la capacidad de ejercer presión psicológica a distancia, ya que, el tránsito del ámbito físico al digital ha permitido que este delito adquiriera nuevas dimensiones de alcance y sofisticación, lo que exige un replanteamiento profundo de las categorías jurídicas tradicionales.

En el plano jurídico, se concluye que la actual redacción del artículo 8-A de la Ley N.º 30096, si bien representa un avance en la tipificación de conductas extorsivas cometidas mediante medios digitales, resulta insuficiente para abarcar la totalidad del fenómeno. El tipo penal parte del supuesto de que la víctima es inducida o coaccionada desde el inicio a aceptar un préstamo, sin considerar que, en la práctica, la mayoría de usuarios acceden a estos créditos por necesidad económica o exclusión financiera, este consentimiento inicial, aunque aparentemente libre, deriva en una relación desigual que culmina en una forma de coacción digital posterior, mediante el uso indebido de los datos personales de la víctima; en tal sentido, la limitación del tipo a la inducción o amenaza inicial genera un vacío de punibilidad frente a las fases más lesivas del delito.

A partir de esta constatación, se concluye que el fenómeno del préstamo digital extorsivo debe entenderse como un delito de desarrollo progresivo, cuya fase inicial puede presentarse como una relación civil lícita, pero que se transforma en ilícita al emplearse medios tecnológicos para ejercer control, hostigamiento o extorsión. Por tanto, el Derecho Penal debe adecuarse a esta naturaleza evolutiva, incorporando en su regulación los elementos propios de la criminalidad digital, como la manipulación de datos personales, la intimidación virtual y la difusión de información privada, pues solo así podrá garantizarse la tutela efectiva de bienes jurídicos como la libertad individual, la privacidad y la seguridad informática.

Asimismo, el estudio ha permitido identificar que la digitalización del préstamo informal no solo plantea un problema jurídico, sino también social y estructural, vinculado a la exclusión financiera, la precariedad económica y la vulnerabilidad

tecnológica, ya que, las víctimas del “gota a gota” digital no son sujetos pasivos de coacción inmediata, sino personas atrapadas en un entorno de necesidad que limita su capacidad de decisión; por ello, se concluye que la respuesta penal debe ir acompañada de políticas públicas de inclusión crediticia, educación financiera y alfabetización digital, a fin de reducir los factores estructurales que propician la expansión de este delito.

En consecuencia, la propuesta de reforma del artículo 8-A formulada en esta investigación busca complementar el tipo penal existente, incorporando expresamente la punición de las conductas extorsivas que se producen con posterioridad al consentimiento inicial, permitiendo esta modificación sancionar a quienes, habiendo obtenido la información del usuario, utilizan dicha información para coaccionarlo, intimidarlo o amenazarlo con el fin de obtener un beneficio económico indebido; por tanto, se trata de una propuesta que no amplía injustificadamente el poder punitivo del Estado, sino que corrige una omisión legislativa y restituye la coherencia del sistema penal frente a la realidad delictiva contemporánea.

Entre los principales beneficios de esta propuesta, se destacan la reducción de la impunidad, el fortalecimiento de la tutela de los bienes jurídicos afectados, la mejora de la seguridad jurídica y la confianza en el entorno digital; además, en el plano social, permitiría una respuesta más empática y protectora frente a las víctimas, reafirmando el compromiso del Estado con la defensa de la dignidad humana frente a las nuevas formas de violencia digital.

Finalmente, se concluye que el Derecho Penal peruano se encuentra en un punto de inflexión frente al desafío que representan los delitos digitales, en este caso, el “gota a gota digital” ha evidenciado que la tecnología no solo amplifica la capacidad de los delincuentes, sino que también revela las limitaciones de los marcos normativos tradicionales, de ahí que la modernización legislativa no deba concebirse como una expansión punitiva, sino como una adaptación inteligente del derecho penal a la realidad tecnológica, capaz de equilibrar la protección de los derechos fundamentales con las exigencias de eficacia en la persecución del delito.

7. Recomendaciones

- **Modificar el artículo 8-A de la Ley N.º 30096**, a fin de que no solo sancione la inducción o coacción en la etapa de contratación del préstamo, sino también los actos de amenaza, intimidación o extorsión que se produzcan durante la fase de cobro, permitiendo así una protección integral frente al fenómeno del “gota a gota digital”.
- **Fortalecer la supervisión y control de aplicativos de préstamo digital**, mediante la implementación de mecanismos tecnológicos y regulatorios que permitan identificar, bloquear y sancionar plataformas no autorizadas que operan en el país, en coordinación con entidades como la SBS y organismos de ciberseguridad.
- **Promover programas de educación financiera y digital**, dirigidos especialmente a sectores vulnerables, con el objetivo de prevenir el acceso a créditos informales digitales y reducir la exposición de los usuarios a prácticas extorsivas vinculadas al uso indebido de datos personales.

REFERENCIAS BIBLIOGRÁFICAS

1. Superintendencia de Banca, Seguros y AFP del Perú (SBS). (2023). *SBS advierte sobre aplicaciones de préstamos que acceden a información privada para extorsionar a usuarios*.
<https://www.sbs.gob.pe/Portals/0/jer/PRENSA/2023/NOTA%20DE%20PRENSA%20-%20SBS%20-%20Apps%20de%20prestamos.pdf>
2. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF). (2022). *Montadeudas: te extorsionan a través de un préstamo por app*. Gobierno de México.
<https://www.gob.mx/condusef/articulos/montadeudas-te-extorsionan-a-traves-de-un-prestamo-por-app>
3. Superintendencia Financiera de Colombia. (2023). *Alerta sobre aplicaciones de préstamos no autorizadas*.
<https://www.superfinanciera.gov.co/publicacion/alerta-sobre-aplicaciones-de-prestamos-no-autorizadas>
4. Quizhpe, J. (2025). *Delito de ciberextorsión: un análisis jurídico*. Universidad Nacional de Loja. Dialnet.
5. Organización de los Estados Americanos (OEA). (2020). *Ciberdelito en América Latina y el Caribe: análisis, retos y recomendaciones*.
6. Guerrero Alarcón, J. C. (2024). *INFLUENCIA DEL DELITO DE EXTORSION EN LOS PRESTAMOS GOTA A GOTA, DISTRITO DE VILLA EL SALVADOR, 2023*. [Tesis de maestría, Universidad Nacional Federico Villarreal]. Repositorio UNFV.
7. Rodríguez Ladino, J. J. Impacto financiero causado por los cuentagotas en microempresarios de Villavicencio. [Tesis de maestría, Universidad Nacional de Colombia sede Manizales]. Repositorio UNAL.
<https://repositorio.unal.edu.co/bitstream/handle/unal/55146/17330041.2015.pdf?sequence=1&isAllowed=y>

8. Eslava-Zapata, R., Rojas-Hermida, C. J., & García-Peñaloza, J. E. (2024). Variables asociadas a los delitos informáticos en Latinoamérica. *Revista Academia & Derecho*, 15(28), 1-21.
9. Menacho Ortega, B. A. (2024). Aplicativos gota a gota como instrumento de encubrimiento para la comisión de ciberdelitos económicos en entornos digitales en el Perú [Tesis de maestría, Universidad Internacional de La Rioja]. <https://reunir.unir.net/bitstream/handle/123456789/16590/Menacho%20Ortega%20C%20Bertho%20Arturo.pdf?isAllowed=y&sequence=1&utm>
10. Quezada-Quizhpe, A., & Gende-Ruperti, C., (2025). Delito de Ciberextorsión: Un Análisis Jurídico, y Comparativo en País de Latinoamérica, Perú, Colombia y Ecuador. *593 Digital Publisher CEIT*, 10(1), 546-556, <https://doi.org/10.33386/593dp.2025.1.2893>
11. Ramírez, C. T. E. (Ed.). (2024). *La impunidad en los delitos informáticos. Una problemática de poco interés para legisladores, jueces y fiscales* (Vol. 7, Número 9). *Revista de Investigación de la Corte Superior de Justicia de Huánuco*.