Capítulo 18

Derecho digital y tecnologías de la información contra la extorsión y el crimen organizado en Ancash – Perú

Richard Fermín Contreras Horna, Edith Patricia Barrionuevo Blas, Juan Walther Ramírez Choque, Ysis Katherine Montoya Vereau, Giselle Milagros Floriano Mija

Contreras Horna, R. F., Barrionuevo Blas, E. P., Ramírez Choque, J. W., Montoya Vereau, Y. K., & Floriano Mija, G. M. (2026). Derecho digital y tecnologías de la información contra la extorsión y el crimen organizado en Ancash – Perú. En A. B. Benalcázar (Coord). Ciencias sociales y humanidades en América Latina. Investigaciones disciplinares e interdisciplinarias desde la región (Volumen II). (pp. 421-444). Religación Press. http://doi.org/10.46652/religacionpress.430.c910

18

Derecho digital y tecnologías de la información contra la extorsión y el crimen organizado en Ancash – Perú

Resumen

La presente investigación tiene como objetivo analizar la relación entre el derecho digital y las tecnologías de la información con la eficacia frente a la extorsión y el crimen organizado en la región Áncash, Perú. El estudio adoptó un enfoque cuantitativo correlacional de corte transversal con diseño no experimental. La población estuvo conformada por todos los abogados colegiados activos de la región Áncash, seleccionándose mediante muestreo no probabilístico intencional por conveniencia una muestra de 200 abogados: 100 del Ilustre Colegio de Abogados de Áncash (ICAA) y 100 del Colegio de Abogados del Santa (CAS), bajo criterios de inclusión y exclusión definidos. Se aplicó una encuesta de 40 ítems en escala Likert, validada por tres expertos, con coeficiente alfa de Cronbach de $\alpha = 0.971$. La prueba de normalidad Kolmogorov-Smirnov confirmó distribución no normal, empleándose el coeficiente Rho de Spearman para determinar correlación y significancia entre variables. Los resultados evidencian una relación positiva y significativa entre el desarrollo del derecho digital con sus dimensiones de marco normativo digital, uso de TIC en investigación e interoperabilidad institucional y la eficacia frente a la extorsión y el crimen organizado en Áncash. Se concluye que fortalecer la interoperabilidad tecnológico-institucional, respaldada por un marco robusto de derecho digital, habilitación legal, control judicial y protección de datos, incrementa significativamente la eficacia operativa e investigativa frente a la extorsión y el crimen organizado en Áncash.

Palabras clave: Derecho digital; tecnologías de la información; extorsión; crimen organizado; interoperabilidad; Áncash.

Introducción

La transformación digital ha reconfigurado profundamente las estructuras sociales, económicas y criminales a escala global, donde la conectividad masiva, la proliferación de dispositivos inteligentes y la economía basada en datos han generado nuevas oportunidades para el desarrollo humano, pero simultáneamente han ampliado el espacio operativo del crimen organizado. En este escenario, la extorsión, el sicariato por encargo, las estafas digitales y el financiamiento ilícito han encontrado en la infraestructura tecnológica un ecosistema propicio para su expansión, desafiando la capacidad de respuesta de los Estados y sus sistemas de justicia. Zuboff (2019), advierte que el capitalismo de vigilancia incentiva la extracción masiva de datos, generando asimetrías de poder informacional que benefician tanto a corporaciones como a actores criminales que explotan las mismas infraestructuras digitales para sus operaciones ilícitas. La comprensión de este fenómeno exige un abordaje interdisciplinario que articule el derecho, la tecnología y las políticas públicas de seguridad de manera coherente y sostenible.

La gobernanza de las infraestructuras digitales no es neutral: distribuye poder entre actores estatales, corporativos y criminales de maneras que el derecho debe regular con precisión y eficacia. Esta distribución asimétrica del poder informacional ha favorecido que organizaciones criminales adopten herramientas digitales sofisticadas para coordinar operaciones, anonimizar identidades y dispersar activos ilícitos con una velocidad que supera los tiempos de respuesta institucional tradicional. Adeyeri y Abroshan (2024), señalan que las amenazas de ciberseguridad tienen ramificaciones geopolíticas significativas, exigiendo respuestas estatales coordinadas y cooperación internacional efectiva. La telefonía móvil, la mensajería cifrada y las cuentas receptoras de fondos extorsivos constituyen hoy la columna vertebral operativa del crimen organizado, planteando desafíos que los marcos jurídicos tradicionales no fueron diseñados para enfrentar con la celeridad y precisión que la realidad criminal contemporánea exige.

En el plano internacional, la expansión de la ciberdelincuencia ha motivado respuestas normativas de diversa naturaleza y alcance. Mejía-Lobo et al. (2023), destacan que la ausencia de marcos normativos armonizados entre países facilita que organizaciones criminales aprovechen las brechas jurisdiccionales para operar con relativa impunidad, señalando que el Convenio de Budapest y sus protocolos adicionales representan el esfuerzo más sistemático de armonización normativa internacional en materia de ciberdelincuencia. Paralelamente, legislaciones como la Investigatory Powers Act del Reino Unido (2016) y la Communications Assistance for Law Enforcement Act de Estados Unidos (1994), han establecido arquitecturas legales que combinan ampliación de capacidades investigativas con mecanismos de supervisión, doble control y rendición de cuentas. Estas experiencias demuestran que la eficacia tecnológica en la lucha contra el crimen organizado es alcanzable sin sacrificar garantías constitucionales, siempre que el diseño normativo sea preciso, proporcional y auditable.

La Unión Europea ha desarrollado una jurisprudencia particularmente relevante en materia de límites al acceso estatal a datos digitales y protección de derechos fundamentales en entornos tecnológicos. Phang y Kaabi (2025), en una revisión sistemática de 35 años de evolución legal en materia de privacidad, concluyen que la efectividad de los marcos normativos depende no solo de su robustez formal sino de los mecanismos de supervisión independiente y los estándares de proporcionalidad aplicados al acceso estatal a datos personales. De Hert y Papakonstantinou (2016), analizan el Reglamento General de Protección de Datos europeo, señalando que su arquitectura de derechos y obligaciones constituye un referente global para diseñar sistemas de tratamiento de información que equilibren seguridad y libertad. La protección de datos personales emerge así no como obstáculo a la investigación criminal, sino como condición de legitimidad del Estado y de sostenibilidad del valor probatorio de la evidencia digital obtenida en investigaciones penales.

En América Latina, la problemática adquiere características particulares vinculadas a la debilidad institucional, la corrupción y la

expansión territorial del crimen organizado. Trujillo et al. (2022), documentan que la transformación digital en la región ha avanzado de manera desigual, generando brechas tanto en las capacidades criminales como en las respuestas estatales, con organizaciones delictivas que adoptan tecnologías más rápidamente que las instituciones encargadas de combatirlas. Corcino et al. (2025), señalan que la transformación digital impacta directamente en la rentabilidad de actividades económicas formales e informales, creando condiciones que el crimen organizado aprovecha para expandir sus operaciones de extorsión hacia sectores productivos que dependen de infraestructura digital para sus transacciones. La extorsión telefónica, el "gota a gota" y el sicariato coordinado digitalmente representan manifestaciones concretas de esta hibridación criminal que afecta especialmente a poblaciones vulnerables en contextos de institucionalidad débil.

La protección de datos personales en América Latina ha seguido un proceso de consolidación normativa posterior al europeo, con avances significativos, pero también con persistentes brechas de implementación efectiva. Ramírez (2023), documenta que en México el reconocimiento formal del derecho a la protección de datos personales requirió un proceso gradual de desarrollo normativo, evidenciando que la consolidación de derechos digitales exige acompañamiento institucional sostenido. Judijanto et al. (2024), muestran que en Indonesia persiste una brecha significativa entre el marco normativo de protección de datos y su aplicación efectiva, con definiciones legales ambiguas y mecanismos de supervisión limitados, problemática que se replica en distintos grados en países latinoamericanos. Esta brecha adquiere especial relevancia cuando el Estado utiliza datos personales con fines de investigación criminal, pues la ausencia de controles efectivos puede generar tanto vulneraciones de derechos como contaminación probatoria que invalide las actuaciones investigativas y erosione la confianza ciudadana en las instituciones.

En el Perú, la expansión del crimen organizado y de la delincuencia común se explica, en parte, por su adaptación acelerada a la infraestructura digital: teléfonos inteligentes como centros de coordinación,

mensajería cifrada, cuentas "mulas" para cobros de extorsión y mercados ilícitos sostenidos por plataformas digitales. El Estado peruano enfrenta una brecha operativa significativa: los tiempos de obtención de datos, el fraccionamiento institucional y la falta de canales técnicos estandarizados permiten que el dinero se disperse y los actores se oculten antes de que la respuesta institucional se active. Floriano et al. (2024), señalan que la efectividad de las políticas públicas en el sistema penal peruano depende en gran medida de la existencia de mecanismos de supervisión y evaluación que aseguren su cumplimiento por parte de las instituciones responsables, diagnóstico directamente aplicable al diseño de sistemas de respuesta digital frente al crimen organizado en el país.

El marco normativo peruano ha experimentado desarrollos relevantes orientados a fortalecer las capacidades tecnológicas del Estado frente al crimen organizado. El Decreto Legislativo N.º 1412 consolidó principios como privacidad desde el diseño en el ámbito del gobierno digital (Presidencia del Consejo de Ministros, 2018), mientras que la Política Nacional de Transformación Digital al 2030 amplía este marco hacia entidades públicas, empresas y ciudadanía (Presidencia del Consejo de Ministros, 2023). Torres (2025), señala que el gobierno digital y la protección de datos personales en la administración pública peruana requieren fortalecer capacidades institucionales específicas, particularmente en materia de gobernanza de datos y respuesta ante incidentes de seguridad. El Decreto de Urgencia N.º 007-2020 aprobó el Marco de Confianza Digital, estableciendo condiciones para que las interacciones digitales entre ciudadanos e instituciones se desarrollen con garantías de seguridad y protección de derechos fundamentales (Presidencia de la República del Perú, 2020).

La protección de datos personales como derecho fundamental constituye el marco de legitimidad dentro del cual deben operar las capacidades tecnológicas del Estado en materia de investigación criminal. La Constitución Política del Perú reconoce en su artículo 2.6 el derecho fundamental a la protección de datos personales, tutelado mediante el hábeas data (Constitución Política del Perú, 1993). Quiroz

(2016), analiza el hábeas data como garantía para el acceso a información y la autodeterminación informativa, evidenciando tendencias jurisprudenciales que refuerzan la exigencia de control judicial sobre el tratamiento de datos personales por parte del Estado. Alvarado (2016), desarrolla los estándares de gestión de seguridad de la información en el régimen peruano de protección de datos personales, señalando que las entidades públicas deben implementar medidas técnicas y organizativas proporcionales al riesgo que representan sus tratamientos de información, estándares directamente aplicables al diseño de sistemas interoperables de investigación criminal.

El desarrollo del derecho digital en el Perú enfrenta desafíos de implementación que trascienden la producción normativa. ComexPerú (2022), señala que, pese a iniciativas legislativas como el Proyecto de Ley N.º 878/2021-CR sobre una Ley General de Internet, persisten vacíos normativos y desafíos en la implementación efectiva de derechos digitales, especialmente en materia de acceso equitativo y neutralidad en la red. Rudas y Cajahuanca (2025), identifican, mediante revisión sistemática, que las ciencias jurídicas en la era digital enfrentan innovaciones y desafíos legales que exigen especialización creciente, particularmente en la intersección entre tecnología, privacidad y seguridad pública. Barrio (2023), destaca que el cumplimiento basado en el riesgo constituye la pieza cardinal del nuevo derecho digital europeo, modelo que el Perú debería adoptar para orientar sus políticas de implementación normativa en materia de tecnologías de la información aplicadas a la seguridad pública y al combate del crimen organizado.

La interoperabilidad tecnológico-institucional emerge como condición necesaria para la eficacia del combate al crimen organizado en el Perú. Casanovas et al. (2022), señalan que la gobernanza socio-legal en la era del internet de las cosas e industria 4.0 requiere enfoques que articulen normas jurídicas con arquitecturas técnicas, superando la dicotomía entre regulación formal y diseño tecnológico. Guillén et al. (2025), documentan que el big data y la toma de decisiones en el sector público peruano presentan oportunidades significativas para mejorar la eficacia institucional, pero requieren marcos de gobernanza

que garanticen el uso ético y legal de la información, condición indispensable para que los datos obtenidos en investigaciones criminales mantengan su valor probatorio. En el Perú, la Plataforma de Interoperabilidad del Estado (PIDE) constituye la infraestructura base sobre la cual pueden construirse flujos estandarizados de información entre la PNP, el Ministerio Público, la UIF y los operadores de telecomunicaciones, evitando demoras que permiten al crimen organizado adaptarse y evadir la acción estatal.

La región Áncash no es ajena a la problemática del crimen organizado y la extorsión. Su geografía diversa, que combina zonas costeras, andinas y amazónicas, junto con la presencia de importantes actividades económicas como la minería, la pesca y el comercio, ha generado condiciones propicias para la expansión de organizaciones criminales que utilizan infraestructura digital para coordinar sus operaciones. De La Torre y Quiroz (2023), documentan que los ciberdelitos se asocian significativamente con fraudes financieros, señalando que la digitalización acelerada ha creado nuevas modalidades de victimización que afectan tanto a personas naturales como a empresas y organizaciones. En Áncash, la extorsión a empresas mineras, comerciantes, transportistas y profesionales genera flujos económicos significativos que financian la expansión del crimen organizado regional, con modalidades que combinan amenazas físicas con coordinación digital mediante telefonía móvil, mensajería cifrada y cuentas bancarias intermediarias (Rey, 2025).

La respuesta institucional en la región Áncash frente al crimen organizado digital enfrenta limitaciones estructurales que reflejan los problemas sistémicos del sistema de justicia peruano. León et al. (2025), señalan que los delitos informáticos requieren actualizaciones normativas constantes frente a nuevas formas de ciberdelitos, destacando que la brecha entre la legislación vigente y las modalidades criminales emergentes genera espacios de impunidad que el crimen organizado aprovecha sistemáticamente. Haro et al. (2025), complementan este diagnóstico al señalar que los delitos digitales requieren respuestas jurídicas que combinen capacidades tecnológicas con

mecanismos de protección de derechos, destacando la necesidad de especialización jurídica y técnica en las instituciones encargadas de la persecución del crimen organizado. En Áncash, la fragmentación entre la PNP, el Ministerio Público y el Poder Judicial, la ausencia de protocolos estandarizados para el manejo de evidencia digital y la limitada capacidad pericial especializada disponible en la región constituyen obstáculos que reducen significativamente la eficacia investigativa.

La presente investigación se justifica en la necesidad de generar evidencia empírica sobre la relación entre el derecho digital con sus dimensiones de marco normativo digital, uso de TIC en investigación e interoperabilidad institucional y la eficacia frente a la extorsión y el crimen organizado en Áncash. Nosratabadi et al. (2023), evidencian empíricamente que la sostenibilidad social de la transformación digital depende de la capacidad de los marcos normativos e institucionales para gestionar los riesgos asociados al uso de tecnologías digitales, hallazgo aplicable al diseño de sistemas de seguridad pública basados en TIC. La investigación aporta datos cuantitativos obtenidos de operadores jurídicos directamente involucrados en la persecución del crimen organizado en Áncash, contribuyendo al debate académico y a la formulación de propuestas concretas de mejora normativa e institucional para la región, en un contexto donde el Perú ocupa el quinto lugar en América Latina en el Índice Global de Ciberseguridad 2024 pero aún enfrenta vulnerabilidades significativas en su infraestructura digital (Presidencia del Consejo de Ministros, 2024).

La innovación tecnológica en la lucha contra el crimen organizado solo es sostenible si se diseña como política de derecho digital: eficacia basada en datos, pero con garantías constitucionales verificables. Lessig (2006), señala que el código tecnológico funciona como regulador, advirtiendo que sin límites claros la intervención tecnológica puede erosionar derechos fundamentales y habilitar abusos institucionales. Quach et al. (2022), documentan las tensiones entre tecnologías digitales, privacidad y datos, señalando que estas tensiones requieren marcos regulatorios que equilibren innovación y protección de derechos. En ese contexto el estudio tiene como objetivo analizar

la relación entre el derecho digital, las tecnologías de la información y su impacto en la eficacia de la lucha contra la extorsión y el crimen organizado en la región de Áncash, Perú.

Derecho digital y tecnologías de la información

El marco normativo digital constituye el conjunto de principios, normas y reglas jurídicas que ordenan la producción, circulación y protección de datos, la investigación penal en entornos tecnológicos, la responsabilidad de intermediarios y la gobernanza de sistemas automatizados. Matos et al. (2025), sostienen que el derecho digital comprende el conjunto de normas y principios jurídicos orientados a regular las actividades y relaciones que se desarrollan en entornos tecnológicos, con el propósito de proteger derechos fundamentales como la privacidad, la protección de datos personales y la libertad de expresión frente a los desafíos derivados de las tecnologías emergentes. En el Perú, este marco se articula sobre la base constitucional del artículo 2.6 de la Constitución Política (1993), que reconoce el derecho fundamental a la protección de datos personales, desarrollado legislativamente a través de la Ley N.º 29733 y su reglamento aprobado mediante el Decreto Supremo N.º 016-2024-JUS (Ministerio de Justicia y Derechos Humanos, 2024), que incorpora obligaciones de notificación y registro de incidentes de seguridad aplicables a entidades públicas y privadas en toda la región.

El marco normativo digital peruano se complementa con instrumentos de gobierno digital que establecen principios rectores para el tratamiento de información en entornos tecnológicos. El Decreto Legislativo N.º 1412 consolidó principios como privacidad desde el diseño y nivel de protección adecuado para los datos personales en el ámbito del gobierno digital (Presidencia del Consejo de Ministros, 2018), mientras que el Decreto de Urgencia N.º 007-2020 aprobó el Marco de Confianza Digital orientado a garantizar la confianza de las personas en su interacción con servicios digitales (Presidencia de la República del Perú, 2020; Hernández, 2022).

Extorsión y crimen organizado

La extorsión es un delito que tiene un impacto significativo en la seguridad ciudadana, la actividad económica y la confianza en las instituciones. Este crimen ha evolucionado, adoptando nuevas formas tecnológicas, como el uso de líneas telefónicas prepago, mensajes cifrados y transferencias a cuentas de terceros. Según Zuboff (2019), la digitalización reconfigura las relaciones de poder, permitiendo que el crimen organizado opere con menor riesgo de ser identificado. La percepción de extorsión es un indicador de la magnitud del problema y de la eficacia de las respuestas institucionales ante el fenómeno.

La extorsión está estrechamente vinculada con el uso de infraestructura tecnológica, que facilita la operación criminal de bajo costo y alto anonimato. De La Torre y Quiroz (2023), indican que los ciberdelitos, como fraudes financieros, se han intensificado con la digitalización, afectando tanto a personas como a empresas. La extorsión a sectores como la minería y el comercio genera flujos económicos que financian al crimen organizado. La medición de la frecuencia y percepción de la extorsión es esencial para diseñar políticas públicas adecuadas que contrarresten este fenómeno (Floriano et al., 2024).

La cooperación interinstitucional y la confianza ciudadana son fundamentales para combatir la extorsión. Nosratabadi et al. (2023), sostienen que la sostenibilidad social de la transformación digital depende de marcos normativos eficaces, mientras que Trujillo et al. (2022), señalan que las brechas en los sistemas de respuesta permiten que el crimen organizado se aproveche de la debilidad estatal. La falta de capacidades tecnológicas en las instituciones del sistema de justicia limita la efectividad de la respuesta frente a la extorsión, lo que revela la insuficiencia de las respuestas institucionales actuales ante el problema.

La respuesta estatal frente a la extorsión debe ser tanto reactiva como preventiva. Según Lessig (2006), el diseño de infraestructuras di-

gitales puede regular los comportamientos en el entorno digital, como se refleja en medidas como la limitación de líneas móviles y el bloqueo de terminales asociados a actividades delictivas. La efectividad de estas medidas depende de una implementación coordinada entre las autoridades competentes. El fortalecimiento de las capacidades tecnológicas y la cooperación interinstitucional son clave para enfrentar el crimen organizado digital, como lo demuestra la necesidad de fortalecer los marcos normativos y las capacidades de inteligencia criminal (Mittelstadt et al., 2016).

Metodología

Este estudio se clasificó como básico, empleando un diseño no experimental y un enfoque cuantitativo correlacional transversal. Un diseño de investigación no experimental transversal recoge datos en un punto específico en el tiempo, observando las variables sin manipularlas (Hernández & Mendoza, 2018). El propósito central fue determinar la relación entre la variable derecho digital y tecnologías de la información, con sus dimensiones: marco normativo digital, uso de TIC en investigación e interoperabilidad institucional y la variable extorsión y crimen organizado, con sus dimensiones: frecuencia y percepción de extorsión, presencia de crimen organizado y eficacia de la respuesta estatal en la región Áncash, sin intervenir sobre ninguna de las variables de estudio. Este enfoque resulta apropiado cuando el objetivo es describir y correlacionar fenómenos tal como se presentan en la realidad institucional, generando evidencia empírica que sirva de base para la formulación de políticas públicas y propuestas normativas aplicables al contexto regional (Arias et al., 2022).

La población del estudio estuvo conformada por todos los abogados colegiados activos de la región Áncash, registrados en los colegios de abogados con sede en la región: el Ilustre Colegio de Abogados de Áncash (ICAA) y el Colegio de Abogados del Santa (CAS). Esta población fue seleccionada por constituir operadores jurídicos con conocimiento directo del marco normativo aplicable al combate del crimen organizado, experiencia en litigación penal y capacidad para

evaluar las capacidades y limitaciones del sistema institucional frente a la extorsión y el crimen organizado digital en el contexto de la región Áncash (Hernández & Mendoza, 2018). La totalidad de abogados colegiados activos en ambas instituciones al momento de la aplicación del instrumento constituyó el universo poblacional del estudio, abarcando profesionales que ejercen en las distintas provincias y zonas geográficas que conforman la región.

Dado el tamaño de la población y las características del fenómeno estudiado, se optó por un muestreo no probabilístico intencional por conveniencia, seleccionándose una muestra de 200 abogados: 100 pertenecientes al Ilustre Colegio de Abogados de Áncash (ICAA) y 100 al Colegio de Abogados del Santa (CAS). Los criterios de inclusión considerados fueron: (a) abogado colegiado activo en el ICAA o el CAS al momento del estudio; (b) experiencia mínima de dos años en ejercicio profesional; (c) desempeño en áreas vinculadas a derecho penal, derecho digital, derecho procesal, asesoría a entidades públicas o litigación en materia de crimen organizado o extorsión en la región Áncash; y (d) disposición voluntaria e informada a participar en el estudio. Los criterios de exclusión fueron: (a) abogados con habilitación suspendida o inhabilitados al momento del estudio; (b) profesionales sin experiencia en materias vinculadas a las variables de investigación; y (c) participantes que no completaran el instrumento de manera íntegra (Arias et al., 2022).

El recojo de información se obtuvo mediante una encuesta de 40 preguntas distribuidas en escala Likert de cinco niveles desde "totalmente en desacuerdo" hasta "totalmente de acuerdo" que fueron validadas mediante juicio de tres expertos en derecho digital, tecnologías de la información y derecho penal. Los ítems se distribuyeron proporcionalmente entre las seis dimensiones de las dos variables, cubriendo los aspectos centrales del marco normativo digital, el uso de TIC en investigación, la interoperabilidad institucional, la frecuencia y percepción de extorsión, la presencia de crimen organizado y la eficacia de la respuesta estatal en la región Áncash. Previo a la aplicación definitiva, se realizó una prueba piloto con 10 participantes para evaluar

la comprensión de los ítems y la consistencia interna del instrumento, obteniéndose un coeficiente alfa de Cronbach de $\alpha = 0.971$, valor que evidencia alta confiabilidad del instrumento (Supo & Zacarías, 2024).

Con el apoyo de la prueba de normalidad Kolmogorov-Smirnov, los datos demostraron que no correspondían a una distribución normal, por lo que se utilizó la prueba Rho de Spearman para hallar el nivel de correlación y el grado de significancia entre las variables y sus dimensiones. El procesamiento estadístico se realizó con el software SPSS versión 27, siguiendo los procedimientos establecidos por Supo y Zacarías (2024), para investigaciones correlacionales con variables ordinales. Los resultados fueron interpretados considerando tanto la magnitud del coeficiente de correlación donde valores entre 0.10 y 0.39 indican correlación baja, entre 0.40 y 0.69 correlación moderada, y entre 0.70 y 1.00 correlación alta como el nivel de significancia estadística, estableciendo como umbral $p < 0.05$ para la aceptación de las hipótesis de investigación. Además, este proceso fue complementado con una revisión documental exhaustiva que incluyó artículos científicos, tesis y documentos nacionales e internacionales relevantes para el objeto de estudio (Creswell & Creswell, 2018).

Resultados

Tabla 1.
Prueba de normalidad de las puntuaciones de derecho digital y tecnologías de la información con la extorsión y crimen organizado

Variables	Kolmogorov-Smirnov		
	Estadístico	gl	Sig.
Derecho digital y tecnologías de la información	,087	200	,000
Extorsión y crimen organizado	,226	200	,000

Nota: elaboración propia. SPSS V. 27

Ha = Los datos no tienen un patrón de distribución normal.

Ho = Los datos tienen un patrón de distribución normal.

En la tabla 1, se muestra la prueba de normalidad Kolmogorov Smirnov, donde el resultado en ambas variables arrojo un p-valor inferior a 0.05; por ello, descartándose así la hipótesis nula y por ende los datos se ajustan a una distribución no paramétrica, por lo que se recurre a la estadística de Rho de Spearman.

Tabla 2.
Grado de correlación entre derecho digital y tecnologías de la información con sus dimensiones y la extorsión y crimen organizado

Criterio a evaluar	Extorsión y crimen organizado		
	Coeficiente Rho de Spearman	gl	Sig.
Derecho digital y tecnologías de la información	0.703	200	0.000
Marco normativo digital	0.719	200	0.000
Uso de TIC en investigación	0.650	200	0.000
Interoperabilidad institucional	0.657	200	0.000

Nota: elaboración propia. SPSS V. 27

La tabla 2 muestra que el coeficiente de Rho de Spearman para derecho digital y tecnologías de la información con la extorsión y crimen organizado es de 0.703, lo que indica una correlación alta. Además, el marco normativo digital tiene un coeficiente de 0.719, mientras que el uso de TIC en investigación y la interoperabilidad institucional muestran correlaciones moderadas (0.650 y 0.657, respectivamente). Todos los coeficientes son estadísticamente significativos ($p < 0.05$).

Conclusiones

La investigación evidenció que el fortalecimiento del derecho digital y sus dimensiones, como el marco normativo, el uso de TIC en investigación y la interoperabilidad institucional, resulta esencial para incrementar la eficacia en la lucha contra la extorsión y el crimen

organizado en Áncash. Los resultados demuestran una correlación significativa entre el desarrollo de estas dimensiones tecnológicas y la mejora en la respuesta estatal frente a estos fenómenos. Este hallazgo subraya la necesidad de políticas públicas que promuevan la integración de tecnologías en el ámbito judicial y de seguridad, asegurando el cumplimiento de los derechos fundamentales.

Además, se concluyó que la interoperabilidad tecnológica, sustentada en un marco normativo robusto, es clave para la eficiencia operativa de las instituciones encargadas de combatir el crimen organizado. La investigación también destaca que la falta de capacitación y recursos en las instituciones judiciales y de seguridad limita la efectividad de las respuestas institucionales. Por lo tanto, es fundamental invertir en la formación de los operadores jurídicos y en la infraestructura tecnológica del Estado para garantizar una respuesta más ágil y efectiva frente a los delitos digitales y las nuevas formas de extorsión en la región.

Referencias

Adeyeri, A., & Abroshan, H. (2024). Geopolitical ramifications of cybersecurity threats: State responses and international cooperations in the digital warfare era. *Information*, 15(11), 682. https://doi.org/10.3390/info15110682

Alvarado, F. J. (2016). La gestión de la seguridad de la información en el régimen peruano de protección de datos personales. *Revista Foro Jurídico*, (15), 26–41.

Arellano, C. A. (2020). El derecho de protección de datos personales. *Biolex*, 12(23), 163–174. https://doi.org/10.36796/biolex.v0i23.194

Arias, J., Holgado, J., Tafur, T., & Vásquez, M. (2022). *Metodología de la investigación: El método ARIAS para realizar un proyecto de tesis*. Editorial Inudi Perú.

Barrio, M. (2023). El cumplimiento basado en el riesgo o risk-based compliance, pieza cardinal del nuevo derecho digital europeo. *Análisis del Real Instituto Elcano (ARI)*, (34).

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press.

Casanovas, P., de Koker, L., & Hashmi, M. (2022). Law, socio-legal governance, the Internet of Things, and Industry 4.0: A middle-out/inside-out approach. *J*, 5(1), 64–91. https://doi.org/10.3390/j5010005

Chereja, I., Erdei, R., Delinschi, D., Pasca, E., Avram, A., & Matei, O. (2025). Privacy-conducive data ecosystem architecture: By-design vulnerability assessment using privacy risk expansion factor and privacy exposure index. *Sensors*, 25(11). https://doi.org/10.3390/s25113554

Chhetri, T. R., Kurteva, A., DeLong, R. J., Hilscher, R., Korte, K., & Fensel, A. (2022). Data protection by design tool for automated GDPR compliance verification based on semantically modeled informed consent. *Sensors*, 22(7). https://doi.org/10.3390/s22072763

ComexPerú. (2022). Comentarios ComexPerú al Proyecto de Ley N.º 878/2021-CR – Ley General de Internet. https://n9.cl/udq29

Congreso de la República. (2011, 3 de julio). *Ley N.º 29733, Ley de Protección de Datos Personales*. https://n9.cl/6dopz

Corcino, H. D., Espejo, L. F., & Montano, J. (2025). Transformación digital y rentabilidad financiera en MYPES del comercio peruano. *Revista Venezolana de Gerencia*, 30(14), 1225–1239. https://doi.org/10.52080/rvgluz.30.especial14.22

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE Publications.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, 32(2), 179–194. https://doi.org/10.1016/j.clsr.2016.02.006

De La Torre, C. M., & Quiroz, J. I. (2023). Ciberdelito y su asociación en el cometimiento de fraudes financieros en la pandemia de la COVID-19. *Revista Venezolana de Gerencia*, 28(102), 609–628. https://doi.org/10.52080/rvgluz.28.102.11

Drozd, O., & Kirrane, S. (2023). A conceptual consent request framework for mobile devices. *Information*, 14(9). https://doi.org/10.3390/info14090515

Floriano, R., Contreras, R. F., Contreras, A. M., & Floriano, G. M. (2024). Políticas públicas inclusivas en el sistema penal peruano como alternativa a la prisión preventiva en mujeres. *Revista Venezolana de Gerencia*, 29(11), 293–308. https://doi.org/10.52080/rvgluz.29.e11.17

Floridi, L. (2014). *The fourth revolution*. Oxford University Press.

García, A. (2007). La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado. *Boletín Mexicano de Derecho Comparado*, 40(120), 743–778.

Grünewald, E., Halkenhäußer, J. M., Leschke, N., & Pallas, F. (2023). *Towards cross-provider analysis of transparency information for data protection*. arXiv. https://doi.org/10.48550/arXiv.2309.00382

Guillén, E. N., Martínez, J. A., Massa, L. A., & Cabel, D. J. (2025). Big data y toma de decisiones en el sector público peruano. *Revista Venezolana de Gerencia*, 30(111), 1322–1336. https://doi.org/10.52080/rvgluz.30.111.5

Haro, K. A., Santillán-Lima, J. C., Alcívar, M. J., & Rangel, H. E. (2025). Delitos digitales y protección jurídica en Ecuador: una revisión crítica del derecho informático como garante de los derechos digitales. *Tesla Revista Científica*, 5(1). https://doi.org/10.55204/trc.v5i1.e488

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernández, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4. https://doi.org/10.1186/1869-0238-4-5

Hernández, O. I. (2022). Pluralismo jurídico del siglo XXI y los derechos digitales: reflexiones en torno a la sentencia SU-420 de 2019 de la Corte Constitucional colombiana. *Justicia*, 27(41), 137–149. https://doi.org/10.17081/just.27.41.5702

Hernández-Sampieri, R., & Mendoza, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Education. https://doi.org/10.22201/fesc.20072236e.2019.10.18.6

Judijanto, L., Solapari, N., & Putra, I. (2024). An analysis of the gap between data protection regulations and privacy rights implementation in Indonesia. *The Easta Journal Law and Human Rights*, 3(1), 20–29. https://doi.org/10.58812/eslhr.v3i01.351

Karagiannis, C., & Vergidis, K. (2021). Digital evidence and cloud forensics: Contemporary legal challenges and the power of disposal. *Information*, 12(5). https://doi.org/10.3390/info12050181

Kuner, C. (2007). *European data protection law*. Oxford University Press.

León, L. S., Olmedo, A. N., & Durán, A. R. (2025). Los delitos informáticos en el COIP y su actualización frente a nuevas formas de ciberdelitos. *Revista Ciencias Holguín*, 31(4).

Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

Loblich, M., & Musiani, F. (2014). Net neutrality and communication research: The implications of Internet infrastructure for the public sphere. *Communication Yearbook*, 38(1), 339–367. https://doi.org/10.1080/23808985.2014.11679167

Machuca, S. A., Vinueza, N. V., Sampedro, C. R., & Santillán, L. (2022). Habeas data y protección de datos personales en la gestión de las bases de datos. *Revista Universidad y Sociedad*, 14(2), 244–251.

Matos, M. R., Espinoza, J. C., Musse, R. S., Apaza, J. P., Patiño, G. C., & Chamoli, A. W. (2025). Armonización de derechos digitales. *Revista InveCom*, 5(3). https://doi.org/10.5281/zenodo.14635310

Mejía-Lobo, M., Hurtado-Gil, S. V., & Grisales-Aguirre, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista de Ciencias Sociales*, 29(2), 356–372. https://doi.org/10.31876/rcs.v29i2.39981

Ministerio de Justicia y Derechos Humanos. (2024, 30 de noviembre). Decreto Supremo N.º 016-2024-JUS, que aprueba el Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales. https://n9.cl/avx4li

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2). https://doi.org/10.1177/2053951716679679

Nosratabadi, S., Atobishi, T., & Hegedűs, S. (2023). Social sustainability of digital transformation: Empirical evidence from EU-27 countries. *Administrative Sciences*, 13(5). https://doi.org/10.3390/admsci13050126

OECD. (2019). *Digital government in Peru: Working closely with citizens*. OECD Publishing. https://doi.org/10.1787/0c1eb85b-en

Pasquale, F. (2015). *The black box society*. Harvard University Press.

Phang, K., & Kaabi, J. (2025). Privacy in flux: A 35-year systematic review of legal evolution, effectiveness, and global challenges. *Journal of Cybersecurity and Privacy*, 5(4). https://doi.org/10.3390/jcp5040103

Presidencia de la República del Perú. (2020, 9 de enero). Decreto de Urgencia N.º 007-2020 que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento. Diario Oficial El Peruano. https://n9.cl/9c3ket

Presidencia del Consejo de Ministros. (2018, 13 de setiembre). *Decreto Legislativo N.º 1412, que aprueba la Ley de Gobierno Digital*. https://n9.cl/wvhuj

Presidencia del Consejo de Ministros. (2023). Decreto Supremo N.º 085-2023-PCM que aprueba la Política Nacional de Transformación Digital al 2030. https://n9.cl/k39xf

Presidencia del Consejo de Ministros. (2024, 12 de diciembre). *Perú en el Índice Global de Ciberseguridad 2024: Retos y oportunidades*. https://n9.cl/310g53

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Quiroz, R. (2016). El hábeas data, protección al derecho a la información y a la autodeterminación informativa. *Letras*, 87(126), 23–49. https://doi.org/10.30920/letras.87.126.2

Ramírez, M. A. (2023). El derecho a la protección de datos personales en México. Nuevos retos para la administración pública. *Revista Enfoques: Ciencia Política y Administración Pública*, 21(39), 1–30. https://doi.org/10.60728/ta9q0908

Rey, A. (2025, 03 de octubre). Extorsión a mineras, transportistas y emprendedores, entonces paguemos menos impuestos. *Perú21*. https://n9.cl/md493

Rudas, C. R., & Cajahuanca, G. W. (2025). Ciencias jurídicas en la era digital: revisión sistemática sobre innovaciones y desafíos legales actuales. *Revista Tribunal*, 5(12), 43–58. https://doi.org/10.59659/revistatribunal.v5i12.192

Ryng, J., Guicherd, G., Saman, J. A., Choudhury, P., & Kellett, A. (2022). Internet shutdowns: A human rights issue. *The RUSI Journal*, 167(4–5), 50–63. https://doi.org/10.1080/03071847.2022.2156234

Supo, J., & Zacarías, H. (2024). *Metodología de la investigación científica: Niveles de investigación*. Independently Published.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Torres, R. E. (2025). Gobierno digital y protección de datos personales en la administración pública peruana. *Revista SAPERE*, 1(28).

Trujillo, G., Rodríguez, L., Mejía, D., & López, R. del P. (2022). Transformación digital en América Latina: una revisión sistemática. *Revista Venezolana de Gerencia*, 27(100), 1519–1536. https://doi.org/10.52080/rvgluz.27.100.15

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Richard Fermín Contreras Horna
Universidad Nacional del Santa | Ancash | Perú
https://orcid.org/0000-0003-3340-715X
richardfcontreras48@gmail.com
Abogado. Doctor en derecho. Docente universitario.
Edith Patricia Barrionuevo Blas
Universidad San Pedro | Ancash | Perú
https://orcid.org/0000-0001-9181-8489
barrionuevoedithpatricia@gmail.com
Abogada. Doctora en derecho. Docente universitario.
Juan Walther Ramírez Choque
Universidad Nacional de San Agustín de Arequipa | Arequipa | Perú
https://orcid.org/0000-0002-7970-8268
juanwaltherrc@gmail.com
Abogado. Con estudios concluidos en maestría en derecho penal y procesal penal, Maestro en docencia universitaria. Doctorando en educación.
Ysis Katherine Montoya Vereau
Universidad Tecnológica del Perú | Ancash | Perú
https://orcid.org/0000-0003-2327-3784
ymontoyav27@gmail.com
Abogada. Maestra con mención en derecho penal y procesal penal. Docente universitario.
Giselle Milagros Floriano Mija
Universidad Nacional del Santa| Ancash | Perú
https://orcid.org/0009-0001-6625-6207
giselleflomi@gmail.com
Estudiante de derecho, estudios de inglés a nivel básico y especializaciones en diversos estudios relacionados a la investigación científica.

Digital Law and Information Technologies Against Extortion and Organized Crime in Ancash, Peru

Abstract

This research aims to analyze the relationship between digital law and information technologies and their effectiveness against extortion and organized crime in the Ancash region, Peru. The study adopted a quantitative, correlational, cross-sectional approach with a non-experimental design. The population consisted of all active licensed lawyers in the Ancash region, from which a sample of 200 lawyers was selected using non-probabilistic intentional convenience sampling: 100 from the Illustrious Bar Association of Ancash (ICAA) and 100 from the Bar Association of Santa (CAS), under defined inclusion and exclusion criteria. A 40-item Likert scale survey was applied, validated by three experts, with a Cronbach's alpha coefficient of $\alpha = 0.971$. The Kolmogorov-Smirnov normality test confirmed a non-normal distribution, and Spearman's Rho coefficient was used to determine the correlation and significance between variables. The results show a positive and significant relationship between the development of digital law —with its dimensions of digital regulatory framework, use of ICT in investigation, and institutional interoperability— and effectiveness against extortion and organized crime in Ancash. It

is concluded that strengthening technological-institutional interoperability, supported by a robust digital law framework, legal enabling, judicial control, and data protection, significantly increases operational and investigative effectiveness against extortion and organized crime in Ancash.

Keywords: Digital law; information technologies; extortion; organized crime; interoperability; Ancash.

Direito Digital e Tecnologias da Informação Contra Extorsão e Crime Organizado em Ancash, Peru

Resumo

Esta pesquisa tem como objetivo analisar a relação entre o direito digital e as tecnologias da informação e sua eficácia contra a extorsão e o crime organizado na região de Ancash, Peru. O estudo adotou uma abordagem quantitativa correlacional de corte transversal com delineamento não experimental. A população foi composta por todos os advogados licenciados ativos da região de Ancash, dos quais foi selecionada uma amostra de 200 advogados por meio de amostragem não probabilística intencional por conveniência: 100 da Ordem dos Advogados Ilustre de Ancash (ICAA) e 100 da Ordem dos Advogados de Santa (CAS), sob critérios de inclusão e exclusão definidos. Aplicou-se um questionário de 40 itens em escala Likert, validado por três especialistas, com coeficiente alfa de Cronbach de $\alpha = 0{,}971$. O teste de normalidade de Kolmogorov-Smirnov confirmou distribuição não normal, empregando-se o coeficiente Rho de Spearman para determinar a correlação e significância entre as variáveis. Os resultados evidenciam uma relação positiva e significativa entre o desenvolvimento do direito digital — com suas dimensões de marco normativo digital, uso de TIC na investigação e interoperabilidade institucional — e a eficácia contra a extorsão e o crime organizado em Ancash. Conclui-se que fortalecer a interoperabilidade tecnológico-institucional, apoiada por um marco robusto de direito digital, habilitação legal, controle judicial e proteção de dados, aumenta significativamente a eficácia operacional e investigativa contra a extorsão e o crime organizado em Ancash.

Palavras-chave: Direito digital; tecnologias da informação; extorsão; crime organizado; interoperabilidade; Ancash.