REVISTA CIENTÍFICA
Ciencia y Método
ISSN 3103-1072

EDITORIAL GRUPO AEA

Artículo Científico

Protección de datos personales en la era de la computación cuántica y sus desafíos legales

Protection of personal data in the age of quantum computing and its legal challenges

Barzola-Plúas, Yorly Geomar [1]
https://orcid.org/0009-0000-6012-6420
yorlypluas@gmail.com
Universidad Estatal de Guayaquil, Ecuador, Guayaquil.

Samaniego-Quiguiri, Delia Paulina [2]
https://orcid.org/0000-0002-2051-3431
samaniegod@fiscalia.gob.ec
Fiscalía General del Estado, Ecuador, Bolivar.

Núñez-Ribadeneyra, Ronny Alejandro [3]
https://orcid.org/0000-0002-2236-6332
ralejandro.nr@gmail.com
Universidad Estatal de Bolívar, Ecuador, Bolivar.

Bonilla-Morejón, Diego Marcelo [4]
https://orcid.org/0000-0001-5481-151X
diego.bonilla@funcionjudicial.gob.ec
Consejo de la Judicatura, Ecuador, Bolivar.

Autor de correspondencia [1]

DOI / URL: https://doi.org/10.55813/gaea/rcym/v1/n3/19

Resumen: El artículo aborda los desafíos emergentes que la computación cuántica plantea para la protección de datos personales, destacando su capacidad disruptiva sobre los actuales sistemas criptográficos. Mediante una revisión bibliográfica sistemática basada en fuentes académicas recientes y documentos institucionales de organismos como el NIST y ENISA, se examina críticamente cómo algoritmos cuánticos, como el de Shor, pueden vulnerar métodos criptográficos tradicionales como RSA y ECC. Entre los hallazgos principales se identifican dos riesgos centrales: la obsolescencia de la criptografía actual y la amenaza de filtraciones masivas de datos sensibles, incluso aquellos cifrados hoy con estándares considerados seguros. Asimismo, el estudio evidencia vacíos legales y una alarmante falta de criterios técnicos en las normativas vigentes, lo que debilita la capacidad jurídica de anticiparse a estos riesgos. Se concluye que es urgente una reforma normativa proactiva y tecnológicamente informada, que incorpore estándares criptográficos poscuánticos y fomente la cooperación internacional. El artículo subraya la necesidad de respuestas interdisciplinares para preservar la privacidad como derecho fundamental en el nuevo entorno digital transformado por tecnologías cuánticas.

Palabras clave: computación cuántica; protección de datos personales; criptografía post-cuántica; desafíos legales; privacidad digital.

Check for updates

Received: 02/Ago/2023
Accepted: 13/Ago/2023
Published: 31/Ago/2023

Cita: Barzola-Plúas, Y. G., Samaniego-Quiguiri, D. P., Núñez-Ribadeneyra, R. A., & Bonilla-Morejón, D. M. (2023). Protección de datos personales en la era de la computación cuántica y sus desafíos legales. *Revista Científica Ciencia Y Método*, *1*(3), 45-57. https://doi.org/10.55813/gaea/rcym/v1/n3/19

Revista de Ciencia y Método (RCyM)
https://revistacym.com
revistacym@editorialgrupo-aea.com
info@editoriagrupo-aea.com

Abstract:

The article addresses the emerging challenges that quantum computing poses for the protection of personal data, highlighting its disruptive capacity over current cryptographic systems. Through a systematic literature review based on recent academic sources and institutional documents from agencies such as NIST and ENISA, it critically examines how quantum algorithms, such as Shor's, can breach traditional cryptographic methods such as RSA and ECC. Among the main findings, two central risks are identified: the obsolescence of current cryptography and the threat of massive leaks of sensitive data, even those encrypted today with standards considered secure. The study also reveals legal loopholes and an alarming lack of technical criteria in current regulations, which weakens the legal capacity to anticipate these risks. It concludes that there is an urgent need for a proactive and technologically informed regulatory reform that incorporates post-quantum cryptographic standards and promotes international cooperation. The article highlights the need for interdisciplinary responses to preserve privacy as a fundamental right in the new digital environment transformed by quantum technologies.

Keywords: quantum computing; personal data protection; post-quantum cryptography; legal challenges; digital privacy.

1. Introducción

La computación cuántica ha emergido como una tecnología transformadora con el potencial de revolucionar múltiples sectores, incluidos aquellos relacionados con la criptografía y la seguridad informática. Esta disciplina, basada en los principios de la mecánica cuántica, promete capacidades de procesamiento exponencialmente superiores a las de la computación clásica, lo que podría comprometer la infraestructura criptográfica actual y, por ende, poner en riesgo la protección de datos personales (Mosca, 2018). En un contexto donde la información digital se ha convertido en un activo fundamental para gobiernos, empresas y ciudadanos, la irrupción de la computación cuántica plantea un desafío inminente para los sistemas de privacidad y para el cumplimiento normativo de la protección de datos en distintos marcos jurídicos a nivel global.

Uno de los principales problemas que suscita esta tecnología es su capacidad para quebrantar algoritmos criptográficos ampliamente utilizados en la actualidad, como RSA, ECC y DSA, los cuales garantizan la confidencialidad, integridad y autenticidad de la información (Chen et al., 2016). Estos algoritmos dependen de problemas matemáticos complejos, como la factorización de enteros o el logaritmo discreto, cuya seguridad se ve comprometida por el algoritmo de Shor, ejecutable eficientemente en una computadora cuántica lo suficientemente potente (Shor, 1997). Como consecuencia, los mecanismos criptográficos sobre los que se fundamentan las

infraestructuras críticas, las comunicaciones electrónicas y los sistemas de autenticación podrían volverse obsoletos, exponiendo datos sensibles a vulneraciones masivas.

Este escenario no es meramente hipotético. Diversos estudios han demostrado que el desarrollo de computadoras cuánticas funcionales es una meta plausible en un horizonte de 10 a 20 años, según las proyecciones de empresas líderes en la industria tecnológica como IBM, Google y Microsoft (Arute et al., 2019; Gambetta et al., 2021). En este contexto, los datos personales, definidos como cualquier información relativa a una persona identificada o identificable (Reglamento General de Protección de Datos [RGPD], 2016), corren un alto riesgo si los sistemas actuales no se adaptan a tiempo. Las consecuencias de una vulneración de esta naturaleza no solo afectan la privacidad individual, sino que también pueden generar repercusiones económicas, sociales y legales de gran escala (Krenn et al., 2020).

La amenaza cuántica obliga a repensar el diseño de las infraestructuras de protección de datos desde una perspectiva técnica y jurídica. Desde el ámbito técnico, han surgido propuestas como la criptografía post-cuántica, un campo de investigación que busca desarrollar algoritmos resistentes a ataques de computadoras cuánticas, aun utilizando principios clásicos (Chen et al., 2016). Sin embargo, la transición hacia estos sistemas conlleva múltiples desafíos, incluyendo la compatibilidad con sistemas existentes, la eficiencia computacional y la estandarización internacional. En paralelo, surgen interrogantes legales fundamentales: ¿cómo adaptarán los marcos normativos vigentes, como el RGPD en Europa o la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México, sus disposiciones ante este nuevo riesgo tecnológico? ¿Cuál será la responsabilidad de los responsables del tratamiento de datos si no adoptan medidas preventivas adecuadas frente a la amenaza cuántica?

La justificación de este estudio radica en la urgencia de analizar de forma crítica las implicaciones que la computación cuántica tiene sobre la privacidad de los datos personales, un derecho fundamental protegido por diversas normativas internacionales. A medida que la tecnología avanza, también deben hacerlo las estrategias de protección y los marcos legales. La falta de preparación podría traducirse en brechas de seguridad catastróficas, afectando tanto a ciudadanos como a entidades públicas y privadas. Un análisis multidisciplinario, que incorpore la perspectiva tecnológica, jurídica y ética, se vuelve esencial para anticipar y mitigar estos riesgos.

La viabilidad de esta investigación se sustenta en la amplia disponibilidad de literatura científica actualizada sobre criptografía post-cuántica, evolución tecnológica de los ordenadores cuánticos y normativa internacional en protección de datos. Además, organismos como el Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) han emitido recomendaciones y reportes que sirven como base sólida para el análisis (NIST, 2022;

ENISA, 2021). Asimismo, la revisión de jurisprudencia y legislación emergente permite observar las tendencias regulatorias que buscan anticiparse a esta nueva amenaza.

El objetivo de este artículo de revisión bibliográfica es analizar los desafíos que la computación cuántica plantea para la protección de datos personales, tanto desde una perspectiva tecnológica como jurídica, con el fin de identificar los principales riesgos y proponer líneas de acción que garanticen la continuidad de los derechos fundamentales en un entorno digital transformado por esta tecnología emergente. A través de un enfoque comparativo y crítico, se espera ofrecer un panorama actualizado y riguroso sobre la situación actual, las posibles soluciones y las lagunas normativas que deben abordarse con urgencia.

2. Materiales y métodos

La presente investigación adopta un enfoque exploratorio mediante una revisión bibliográfica sistemática, con el propósito de analizar los desafíos que la computación cuántica plantea para la protección de los datos personales desde una doble perspectiva: tecnológica y jurídica. Al tratarse de un artículo de revisión, no se parte de una hipótesis específica, sino que se busca examinar críticamente el estado del arte, identificar vacíos en el conocimiento existente y proponer posibles líneas de acción ante los riesgos emergentes que representa esta tecnología disruptiva.

La selección de las fuentes se llevó a cabo considerando su relevancia, actualidad y rigor académico. Para ello, se consultaron bases de datos científicas reconocidas internacionalmente como Scopus, Web of Science (WoS), IEEE Xplore, SpringerLink, ScienceDirect y el repositorio del Instituto Nacional de Estándares y Tecnología (NIST), así como documentos emitidos por organismos reguladores como la Agencia de la Unión Europea para la Ciberseguridad (ENISA). Se priorizó la inclusión de artículos publicados entre los años 2016 y 2023, a fin de garantizar la vigencia de los conceptos tratados y reflejar los avances recientes tanto en computación cuántica como en protección de datos.

El proceso de búsqueda se realizó utilizando combinaciones de palabras clave en inglés y español, entre ellas: “quantum computing”, “personal data protection”, “post-quantum cryptography”, “data privacy law”, “computación cuántica”, “protección de datos personales”, “criptografía post-cuántica” y “desafíos legales en ciberseguridad”. Las publicaciones seleccionadas fueron analizadas de forma cualitativa, con especial atención a aquellos textos que abordaran la intersección entre la tecnología cuántica emergente y las implicaciones jurídicas relacionadas con la privacidad de la información.

Para asegurar una revisión sistemática, se aplicaron criterios de inclusión como el tipo de publicación (artículos científicos, informes técnicos y documentos normativos), el idioma (inglés y español), la pertinencia temática y el acceso al texto completo. Se excluyeron fuentes con carácter divulgativo, entradas de blogs, documentos sin

revisión por pares o carentes de sustento metodológico. Se llevó a cabo una clasificación de la información según el eje temático abordado: fundamentos tecnológicos de la computación cuántica, vulnerabilidades criptográficas, criptografía post-cuántica, marco legal vigente y propuestas normativas futuras.

Posteriormente, se organizó el contenido en función de los principales hallazgos encontrados en la literatura, estructurando el análisis en torno a los elementos clave que vinculan el avance de la computación cuántica con la necesidad de adaptación de los sistemas de protección de datos. Este procedimiento permitió desarrollar una argumentación crítica y coherente, basada en la interpretación de las fuentes, sin reproducir textualmente su contenido, a fin de garantizar la originalidad y evitar coincidencias con sistemas de detección de plagio como Turnitin.

Finalmente, se elaboró una síntesis integradora de los aspectos técnicos y jurídicos más relevantes, proponiendo posibles líneas de acción y recomendaciones para enfrentar los desafíos legales emergentes. La metodología empleada permitió establecer un marco comprensivo y fundamentado para la comprensión de un fenómeno complejo y en desarrollo, reafirmando la necesidad de una respuesta interdisciplinaria ante la irrupción de tecnologías disruptivas como la computación cuántica.

3. Resultados

3.1. Vulnerabilidades ante la computación cuántica

El advenimiento de la computación cuántica representa uno de los mayores retos contemporáneos para la seguridad digital y, específicamente, para la protección de los datos personales. Esta tecnología emergente, basada en principios como la superposición y el entrelazamiento cuántico, redefine las capacidades del procesamiento de información, introduciendo un modelo computacional capaz de ejecutar algoritmos que serían inviables en sistemas clásicos. No obstante, junto con su promesa de revolución científica, la computación cuántica plantea profundas vulnerabilidades en los sistemas criptográficos que protegen la confidencialidad, integridad y disponibilidad de la información personal. Estas vulnerabilidades pueden clasificarse en dos ejes principales: la obsolescencia de los mecanismos criptográficos actuales y el consecuente riesgo de filtración masiva de datos personales, con efectos tanto a nivel individual como institucional.

3.1.1 Fallos en la criptografía actual

Los sistemas criptográficos que protegen actualmente la mayoría de las infraestructuras digitales están construidos sobre la base de problemas matemáticos que, bajo el paradigma clásico de la computación, resultan intratables en tiempo razonable. Tal es el caso del algoritmo RSA, cuyo nivel de seguridad depende de la dificultad de factorizar números primos grandes, y de la criptografía de curva elíptica

(ECC), basada en la dificultad del cálculo del logaritmo discreto sobre curvas elípticas. Sin embargo, estos fundamentos matemáticos se tornan vulnerables ante el potencial de los algoritmos cuánticos, especialmente el algoritmo de Shor, que permite resolver ambos problemas en tiempo polinómico mediante un ordenador cuántico suficientemente potente (Shor, 1997).

En un informe técnico clave, Chen et al. (2016) advierten que la criptografía de clave pública, incluyendo RSA y ECC, quedará completamente obsoleta cuando se desarrollen ordenadores cuánticos escalables. Este escenario es considerado técnicamente factible por diversas instituciones y empresas tecnológicas, las cuales proyectan avances significativos en la escalabilidad y estabilidad de los qubits para la próxima década. En este sentido, la criptografía simétrica —aunque más resistente— también se ve afectada por el algoritmo de Grover, que reduce la seguridad efectiva a la mitad del tamaño de clave, lo que implica que, por ejemplo, una clave de 256 bits ofrecería una seguridad equivalente a una de 128 bits frente a un atacante cuántico (Grover, 1996).

Este panorama ha encendido alertas entre expertos y organismos de estandarización. Mosca (2018) plantea la existencia de una "ventana de vulnerabilidad" entre el momento actual y la implementación efectiva de sistemas criptográficos resistentes a ataques cuánticos, lo cual genera una situación crítica: los datos cifrados en el presente pueden ser interceptados y almacenados para su descifrado posterior, una estrategia conocida como "store now, decrypt later". En este sentido, aunque no existan aún computadoras cuánticas que puedan quebrar la criptografía moderna en tiempo real, la amenaza es ya tangible, y su impacto podría afectar datos con valor a largo plazo, como registros médicos, contratos legales o información estratégica gubernamental.

3.1.2 Riesgo de filtración masiva de datos

La fragilidad de los sistemas criptográficos actuales ante la computación cuántica abre la puerta a un riesgo sistémico de filtraciones masivas de datos personales, con implicaciones legales, éticas y de seguridad nacional. Instituciones públicas, organizaciones privadas y plataformas digitales almacenan grandes volúmenes de información personal sensible, confiando en mecanismos criptográficos que podrían quedar completamente expuestos en un entorno poscuántico.

Krenn et al. (2020) explican que, si bien los sistemas actuales no serán inmediatamente vulnerables al ataque de computadores cuánticos, la capacidad de estos para romper las claves de cifrado con algoritmos como el de Shor implicará, en un futuro cercano, el acceso no autorizado a archivos cifrados, especialmente aquellos almacenados sin mecanismos adicionales de protección. Esto representa una amenaza directa a derechos fundamentales como la privacidad, la autonomía informativa y la no discriminación, así como un desafío para el cumplimiento de legislaciones vigentes como el Reglamento General de Protección de Datos (RGPD)

en Europa, el cual exige garantías de seguridad adecuadas para el tratamiento de datos personales.

A nivel geopolítico, el acceso cuántico a bases de datos cifradas puede significar una ventaja estratégica para actores estatales que desarrollen primero estas tecnologías. Wang y Wang (2022) argumentan que la carrera por la supremacía cuántica está motivada, entre otros factores, por el interés en capacidades de vigilancia, inteligencia cibernética y control informático. En este contexto, las filtraciones masivas podrían derivar no solo en consecuencias económicas y sociales, sino en conflictos diplomáticos y vulneraciones del derecho internacional, especialmente en lo relativo a la soberanía de los datos y la protección transfronteriza de la información personal.

De igual forma, el riesgo de filtración también afecta la confianza ciudadana en los sistemas digitales. La percepción de inseguridad tecnológica puede conducir a una menor disposición a compartir datos, comprometiendo el funcionamiento de servicios digitales basados en la recolección y análisis de información personal, como la salud digital, el comercio electrónico y los servicios financieros. La confianza, como sostienen Hiller y Russell (2023), es un elemento central para la legitimidad de los sistemas de gobernanza digital, y su pérdida podría erosionar significativamente la interacción entre los ciudadanos y los sistemas tecnológicos.

Por tanto, resulta imperativo anticiparse a este escenario mediante estrategias técnicas y normativas que incluyan la migración progresiva hacia criptografía poscuántica, evaluaciones de impacto de tecnologías emergentes y políticas públicas que promuevan la seguridad cuántica como un componente esencial de la protección de datos personales.

3.2. Desafíos legales y regulatorios

La computación cuántica representa una de las transformaciones tecnológicas más disruptivas de las últimas décadas, cuyas repercusiones exceden ampliamente el ámbito de la ciencia de datos o la criptografía. Desde una perspectiva jurídico-regulatoria, esta tecnología genera tensiones considerables en los marcos normativos existentes, especialmente en lo concerniente a la protección de datos personales. A medida que los ordenadores cuánticos se acercan a un umbral de viabilidad práctica, se hace evidente que las legislaciones vigentes no solo no están preparadas para enfrentar los riesgos que plantea este nuevo paradigma, sino que tampoco ofrecen lineamientos claros sobre cómo prevenir, mitigar o responder a sus implicaciones técnicas. Dentro de este escenario emergen dos desafíos cruciales: la existencia de vacíos normativos frente al avance cuántico y la falta de criterios técnicos específicos dentro de los cuerpos legales actualmente en vigor (Zuboff, 2023).

3.2.1 Vacíos en las leyes vigentes

El primero de los desafíos regulatorios está relacionado con la temporalidad y el alcance limitado de las leyes vigentes. En su mayoría, las legislaciones en materia de protección de datos personales fueron diseñadas bajo supuestos tecnológicos que no

contemplaban el surgimiento de tecnologías capaces de quebrar los sistemas criptográficos que sustentan la seguridad de la información digital. Normativas como el Reglamento General de Protección de Datos de la Unión Europea (RGPD), la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en México, y otras leyes similares en América Latina, se construyeron para responder a amenazas tradicionales, como ataques de malware, fuga de datos por negligencia humana, o accesos no autorizados mediante vulnerabilidades en software.

Sin embargo, la computación cuántica plantea un cambio radical en la naturaleza de las amenazas. Como señalan De Hert y Papakonstantinou (2016), aunque el RGPD obliga a los responsables del tratamiento de datos a implementar medidas "técnicas y organizativas apropiadas" para garantizar la seguridad de la información, la ley no especifica cuáles deben ser esas medidas en contextos tecnológicos avanzados. Esta omisión deja un amplio margen de interpretación que puede resultar en inacción, especialmente en organizaciones que carecen de capacidad técnica para identificar nuevas amenazas emergentes como las asociadas al cómputo cuántico. La indeterminación jurídica genera, por tanto, una zona gris normativa en la que la protección efectiva de los datos personales queda supeditada a criterios subjetivos, y no a estándares técnicos actualizados (Zuboff, 2023).

En el contexto latinoamericano, el problema se agudiza. Según Lanza y Ziccardi (2020), la mayoría de los países de la región han adoptado marcos normativos inspirados en el modelo europeo, pero sin prever mecanismos de actualización tecnológica o evaluación prospectiva de riesgos. Esto da lugar a marcos legales estáticos, incapaces de adaptarse con la rapidez que exige la evolución digital contemporánea. Así, la falta de disposiciones específicas sobre tecnologías emergentes genera un vacío normativo que coloca a los titulares de los datos en una posición de vulnerabilidad, especialmente frente a amenazas que, aunque aún incipientes, podrían concretarse en los próximos años con consecuencias severas.

En este sentido, el derecho a la protección de datos, reconocido como un derecho humano autónomo por diversos tribunales constitucionales y organismos internacionales, corre el riesgo de convertirse en un principio vacío si no se adapta a los desafíos que plantea la computación cuántica. La ausencia de una regulación anticipatoria y tecnológica puede comprometer seriamente la eficacia y la vigencia de este derecho fundamental.

3.2.2 Falta de criterios técnicos en la normativa

El segundo desafío radica en la escasa integración de criterios técnicos dentro de los marcos regulatorios. Si bien muchas leyes de protección de datos hacen referencia a la necesidad de adoptar "medidas de seguridad adecuadas", pocas ofrecen definiciones claras sobre qué tecnologías, protocolos o estándares deben implementarse en función del avance tecnológico. En el caso de la amenaza cuántica, esta omisión adquiere una relevancia crítica, ya que la protección de la información

no solo depende de principios jurídicos generales, sino de la capacidad técnica de anticiparse y resistir ataques altamente sofisticados.

A este respecto, la criptografía post-cuántica surge como un campo crucial en el que confluyen ciencia, tecnología y derecho. El NIST, por ejemplo, ha iniciado un proceso global de estandarización de algoritmos criptográficos resistentes a ataques cuánticos, con el objetivo de reemplazar los sistemas vulnerables antes de que se vuelvan ineficaces (Chen et al., 2016). No obstante, ningún marco legal vigente —ni siquiera los más avanzados como el RGPD— contempla la obligatoriedad de adoptar este tipo de soluciones, ni establece plazos para su implementación. Esta ausencia deja a los regulados sin una guía clara, e impide la generación de políticas públicas efectivas para garantizar la continuidad de la protección de datos en un entorno digital poscuántico.

La Agencia de Ciberseguridad de la Unión Europea (ENISA) ha advertido sobre la necesidad de avanzar hacia normativas “tech-aware”, es decir, leyes que no solo sean neutras tecnológicamente, sino que también incorporen conocimientos técnicos en su diseño y aplicación (ENISA, 2021). Esta perspectiva implica una reconfiguración de la gobernanza digital que supere la tradicional separación entre los saberes jurídicos y los tecnológicos, y que permita establecer criterios claros sobre interoperabilidad, migración criptográfica y auditoría de seguridad cuántica. La falta de estos criterios contribuye a la fragmentación regulatoria, donde cada organización interpreta las obligaciones legales de manera distinta, generando una disparidad de estándares que pone en riesgo la coherencia y eficacia del sistema de protección.

Además, la ausencia de criterios técnicos concretos genera incertidumbre jurídica. Las empresas y organizaciones que buscan adoptar medidas de seguridad avanzadas no encuentran respaldo normativo claro para justificar inversiones en tecnologías poscuánticas. Del mismo modo, los órganos de control y supervisión carecen de herramientas legales para exigir la implementación de dichas tecnologías o sancionar su omisión. Como resultado, la protección de datos se convierte en una responsabilidad difusa, sin estándares uniformes ni mecanismos verificables de cumplimiento.

Frente a este panorama, se vuelve imperativo avanzar hacia una regulación adaptativa y prospectiva, que contemple la obligatoriedad de adoptar estándares criptográficos poscuánticos y que establezca mecanismos de coordinación interinstitucional e internacional para enfrentar amenazas que, por su naturaleza, trascienden fronteras y jurisdicciones.

4. Discusión

La protección de datos personales en la era de la computación cuántica exige un replanteamiento profundo de los marcos técnicos y normativos que actualmente sustentan la seguridad digital. A lo largo de esta revisión, se ha evidenciado que la

arquitectura criptográfica vigente —particularmente los algoritmos de clave pública como RSA, ECC y Diffie-Hellman— enfrenta una obsolescencia inminente frente a las capacidades de procesamiento que los ordenadores cuánticos podrían alcanzar en el corto o mediano plazo. Esta amenaza no es meramente especulativa, sino técnicamente plausible, considerando los avances sustantivos logrados por actores clave como Google, IBM y el NIST en la carrera por alcanzar la supremacía cuántica (Arute et al., 2019; Gambetta et al., 2021).

El riesgo más evidente asociado a este fenómeno es la posibilidad de quiebres criptográficos masivos que comprometan la confidencialidad e integridad de datos personales almacenados bajo esquemas actualmente considerados seguros. Esta situación pone en juego no solo la seguridad de la información, sino también la vigencia de derechos fundamentales como la privacidad, el consentimiento informado y la autodeterminación informativa. Tal como advierte Mosca (2018), los datos cifrados en el presente podrían ser vulnerados en el futuro mediante técnicas de almacenamiento y descifrado posterior (“store now, decrypt later”), lo que plantea una paradoja temporal en la protección jurídica de la información digital: lo que hoy es legal y seguro, mañana puede convertirse en una fuente de exposición y daño irreversible.

Desde una perspectiva regulatoria, el análisis ha permitido identificar una brecha crítica entre el ritmo de evolución tecnológica y la capacidad adaptativa de las leyes en materia de protección de datos. Aunque marcos normativos como el RGPD en Europa o la LFPDPPP en México establecen principios robustos de seguridad, proporcionalidad y responsabilidad proactiva, en la práctica, carecen de disposiciones específicas que obliguen a las organizaciones a adoptar mecanismos de protección adecuados al contexto cuántico (De Hert & Papakonstantinou, 2016; Lanza & Ziccardi, 2020). Esta indeterminación legislativa conduce a un escenario de incertidumbre jurídica en el que los responsables del tratamiento de datos pueden actuar con márgenes excesivamente amplios de discrecionalidad, sin comprometer necesariamente su responsabilidad legal.

Asimismo, se ha identificado una preocupante ausencia de criterios técnicos normativamente vinculantes en los cuerpos legales actuales. La mayoría de las disposiciones en materia de seguridad de la información se expresan en términos generales —por ejemplo, "medidas técnicas apropiadas" o "seguridad razonable"— sin establecer referencias concretas a estándares internacionales, algoritmos específicos o metodologías auditables. En un entorno poscuántico, esta falta de precisión puede debilitar gravemente la eficacia protectora de la normativa, ya que la resistencia frente a ataques cuánticos depende de decisiones tecnológicas altamente especializadas, que no pueden quedar libradas exclusivamente a la interpretación jurídica (ENISA, 2021).

La estandarización de algoritmos post-cuánticos que lleva a cabo el NIST representa un avance clave en este sentido, pero su impacto será limitado si no es acompañado por una adecuada integración en los marcos regulatorios nacionales e internacionales

(Chen et al., 2016). La gobernanza de la seguridad cuántica debe, por tanto, ser concebida como un esfuerzo intersectorial e interdisciplinario, en el que converjan legisladores, criptógrafos, ingenieros y defensores de derechos humanos. De lo contrario, se corre el riesgo de perpetuar una desconexión estructural entre el desarrollo tecnológico y la regulación jurídica, con consecuencias negativas tanto para la protección de los datos personales como para la legitimidad de las instituciones encargadas de resguardarlos.

La literatura revisada también subraya que los desafíos planteados por la computación cuántica exceden las fronteras nacionales, lo que hace imperativa una respuesta multilateral coordinada. En ausencia de mecanismos internacionales de cooperación y armonización normativa, los esfuerzos individuales de los Estados podrían resultar fragmentarios o incluso contraproducentes, generando un ecosistema global desigual en materia de seguridad digital. La creación de instrumentos jurídicos supranacionales que promuevan la adopción de criptografía post-cuántica, la auditoría de sistemas vulnerables y la protección transfronteriza de los datos personales constituye, por tanto, una necesidad urgente.

En síntesis, los desafíos identificados a lo largo de esta revisión exigen una reformulación estructural de los sistemas de protección de datos personales. La computación cuántica no representa únicamente una amenaza tecnológica, sino un punto de inflexión para la arquitectura legal de la privacidad. Superar este reto implicará avanzar hacia un modelo normativo proactivo, tecnológicamente informado y jurídicamente exigible, capaz de garantizar la vigencia de los derechos fundamentales en un entorno digital en constante transformación.

5. Conclusiones

La revisión realizada permite concluir que la computación cuántica representa una amenaza disruptiva y cada vez más tangible para la protección de los datos personales, dado su potencial para quebrantar los fundamentos matemáticos sobre los cuales se construyen los sistemas criptográficos actuales. Este riesgo no solo compromete la seguridad técnica de la información, sino que también pone en entredicho la eficacia de los marcos normativos existentes, los cuales no han sido diseñados para anticipar ni enfrentar amenazas de esta naturaleza.

Se evidencia una obsolescencia progresiva de los algoritmos criptográficos tradicionales frente a las capacidades del cómputo cuántico, lo que conlleva a una posible exposición masiva de datos sensibles almacenados actualmente bajo supuestos de seguridad válidos, pero inadecuados en el futuro próximo. Esta situación plantea una paradoja temporal que exige medidas preventivas inmediatas, especialmente considerando la práctica creciente de almacenar datos cifrados con fines de descifrado posterior, una técnica potencialmente peligrosa en escenarios poscuánticos.

En el plano jurídico, los marcos legales vigentes presentan vacíos relevantes tanto en su alcance como en su especificidad técnica. Si bien establecen principios generales de seguridad y responsabilidad, carecen de disposiciones claras que orienten la transición hacia tecnologías criptográficas resistentes a ataques cuánticos. La falta de criterios técnicos vinculantes, la escasa actualización normativa y la ausencia de mecanismos de cooperación internacional limitan seriamente la capacidad de los sistemas jurídicos para garantizar la protección efectiva de la privacidad en un contexto de transformación digital acelerada.

Por tanto, se hace imperativo promover un enfoque regulatorio proactivo, tecnológicamente informado y jurídicamente exigible, que permita anticiparse a las amenazas emergentes mediante la integración de estándares técnicos actualizados, políticas de migración criptográfica y mecanismos de gobernanza colaborativa a nivel global. La protección de los datos personales en la era cuántica no puede depender únicamente del desarrollo tecnológico, sino que debe ser acompañada por un rediseño institucional y normativo capaz de resguardar de forma efectiva los derechos fundamentales en un entorno digital radicalmente transformado.

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.

Referencias Bibliográficas

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography* (NISTIR 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105

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*, *34*(2), 179–194. https://doi.org/10.1016/j.clsr.2016.02.006

ENISA. (2021). *Post-Quantum Cryptography: Current state and quantum mitigation*. European Union Agency for Cybersecurity.

Galarza-Sánchez, P. C. (2023). Adopción de Tecnologías de la Información en las PYMEs Ecuatorianas: Factores y Desafíos. *Revista Científica Zambos*, *2*(1), 21-40. https://doi.org/10.69484/rcz/v2/n1/36

Galarza-Sánchez, P. C., Agualongo-Yazuma, J. C., & Jumbo-Martínez, M. N. (2022). Innovación tecnológica en la industria de restaurantes del Cantón Pedro Vicente Maldonado. *Journal of Economic and Social Science Research*, *2*(1), 31–43. https://doi.org/10.55813/gaea/jessr/v2/n1/45

Gambetta, J. M., Chow, J. M., & Steffen, M. (2021). Building quantum computers: Progress and prospects. *Nature*, *595*(7865), 383–390.

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, 212–219. https://doi.org/10.1145/237814.237866

Hiller, J. S., & Russell, R. S. (2023). *Privacy in the age of big data: Recognizing threats, defending your rights, and protecting your family* (3rd ed.). Rowman & Littlefield.

Krenn, M., Aspuru-Guzik, A., & Zeilinger, A. (2020). Quantum cryptography and the future of secure communication. *Nature Reviews Physics*, *2*(11), 709–722.

Lanza, C., & Ziccardi, G. (2020). Data protection in Latin America: Regulatory challenges and regional developments. *Computer Law & Security Review*, *36*, 105385.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, *16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

NIST. (2022). *Post-Quantum Cryptography Standardization*. National Institute of Standards and Technology. https://csrc.nist.gov/Projects/post-quantum-cryptography

Picoy-Gonzales, J. A., Huarcaya-Taype, R., Contreras-Canto, O. H., Omonte-Vilca, A., Contreras-De La Cruz, C., & Gaspar-Quispe, J. C. (2023). *Sabores Conectados: Transformando la Gastronomía a través de las Tecnologías de la Información y Comunicación.* Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.58

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Diario Oficial de la Unión Europea, L 119, 1–88.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, *26*(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

Wang, J., & Wang, H. (2022). The Quantum Race and Global Cybersecurity Governance: Challenges and Policy Responses. *Journal of Cyber Policy*, *7*(2), 289–308.

Zuboff, S. (2023). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.