STAR OF SCIENCES
Multidisciplinary Journal

Revista Multidisciplinaria
ISSN: 3091-1885
Vol 3 Núm 1 (2026)
Artículo Original

Artículo Original

Fuentes normativas de ciberseguridad como regla de protección del servicio bancario panameño e internacional

Normative Sources of Cybersecurity as a Legal Safeguard Framework for the Protection of Panamanian and International Banking Operations

Lourdes C. Jean Pierre Barsallo

[1] *Universidad de Panamá, Panamá - Panamá*
Lourdes.jean@up.ac.pa , https://orcid.org/0009-0009-3817-6312

Autor de correspondencia: Lourdes C. Jean Pierre Barsallo, Lourdes.jean@up.ac.pa

Recepción: 11-Marzo-2026 **Aceptación:** 25-Marzo-2026 **Publicación:** 08-Abril-2026

Cómo citar este artículo: Jean Pierre Barsallo, L. C. . (2026). Fuentes normativas de ciberseguridad como regla de protección del servicio bancario panameño e internacional. *Star of Sciences Multidisciplinary Journal, 3*(1), 1-21. https://doi.org/10.63969/sjtdak48

RESUMEN

El presente artículo analiza algunas de las regulaciones normativas existentes en torno a la ciberseguridad del sector bancario, enfocándose en la interacción entre disposiciones panameñas y las disposiciones impuestas por los estándares internacionales. A partir de un enfoque descriptivo dogmático-jurídico y el enfoque del análisis de derecho comparado, se examinan las normas principales que rigen la gestión del riesgo tecnológico en las entidades financieras, así como tratados y acuerdos internacionales cuya incorporación en los ordenamientos jurídicos internos de los países firmantes resulta incompleta y/o inconsistente. Se definen conceptos esenciales en materia de seguridad de la información y profundiza su papel dentro de los sistemas bancarios para la comprensión de su estrecha relación. Asimismo, se revelan vacíos normativos en aspectos importantes del derecho, como lo es la responsabilidad civil bancaria frente a incidentes cibernéticos y su ineficiencia en el control y supervisión de sus manuales de gestión de riesgos tecnológicos. Finalmente, concluye en la necesidad de fortalecimiento de la integración normativa mediante la adopción homogénea y coherente de estándares internacionales que respondan a las particulares necesidades del entorno digital, tanto panameño como internacional.

Palabras clave: Ciberseguridad; Sistema bancario; Protección de datos; fuentes normativas; Derecho Internacional.

ABSTRACT

This article analyzes certain existing regulatory frameworks concerning cybersecurity in the banking sector, focusing on the interaction between Panamanian legal provisions and those imposed by international standards. Employing a doctrinal-descriptive legal approach, together with a comparative law

methodology, it examines the principal rules governing technological risk management within financial institutions, as well as international treaties and agreements whose incorporation into the domestic legal systems of signatory States remains incomplete and/or inconsistent. Essential concepts in the field of information security are defined, and their role within banking systems is further explored in order to elucidate their close interrelationship. The article also identifies regulatory gaps in significant areas of law, such as banking civil liability in relation to cyber incidents, and highlights deficiencies in the control and supervision of technological risk management frameworks. Finally, it concludes that there is a need to strengthen normative integration through the coherent and harmonized adoption of international standards that adequately address the specific demands of the digital environment, both in Panama and at the international level.

Keywords: Cybersecurity; Banking system; Data protection; normative sources; International Law.

INTRODUCCIÓN

El mundo nunca deja de evolucionar y el progreso de la tecnología y el cambio de las herramientas físicas a un plano digital han fungido como agente catalizador trascendental para la optimización de la cotidianidad del ser humano y ha simplificado los inconvenientes que se presentan en la rutina allanando el camino hacia una existencia más fluida y desarrollada en el plano físico.

El sector financiero no escapa de esta realidad. Sin embargo, con los nuevos descubrimientos tecnológicos y la idealización de digitalización como un faro de progreso se presentan nuevos retos intrínsecos a su utilización. Estas problemáticas emergentes, como fraudes cibernéticos y el robo masivo de datos, por mencionar algunos, demandan la cooperación de distintas disciplinas para abordar todas sus ramificaciones y hallar soluciones igual de innovadoras.

Por naturaleza, el Derecho Internacional Privado ya enfrenta los retos de la digitalización, pues con regularidad las controversias que surgen trascienden fronteras. El Convenio de Budapest es un ejemplo de cómo esta disciplina intenta establecer una normativa armónica que homogenice legislaciones dispares y contribuir con la resolución de conflictos rápida y efectiva.

Este escrito tiene por objeto las regulaciones existentes en materia de ciberseguridad bancaria a nivel nacional e internacional, abordando el concepto y evolución de la ciberseguridad, general y en el contexto bancario. Asimismo, examina ciertas prácticas bancarias actuales y el análisis de casos emblemáticos concluye la estructuración del documento.

Esta investigación invita a la reflexión de la efectividad de las normativas vigentes y su nivel de relevancia para los Estados y exhorta a la conversión de la ciberseguridad bancaria en una disciplina principal, en lugar de relegarla a una cuestión subsidiaria, recordando la relevancia que poseen los bancos en la economía nacional y global.

2.Generalidades de la ciberdelincuencia

Con el avance de la tecnología, la mayor parte de las actividades son realizadas a través de sistemas que permiten la transferencia de información variable entre dos puntos a distancia (Kularatna & Dias, 2004). Estos sistemas llevan por nombre sistemas de telecomunicaciones. Con la adición del internet, ese intercambio ha dado origen al “Ciberespacio”.

El Ciberespacio es un espacio digital y asimétrico que actúa como autopista por donde circula información digital, tanto de personas naturales como de organizaciones (Parra Cárdenas et al., 2017). Para el 2024, el 68 % de la población mundial es usuaria de internet, es decir, alrededor de 5,500 millones de personas, según cifras de la Unión Internacional de Telecomunicaciones (UIT), y está predestinado que ese porcentaje aumente (UIT, 2024).

El término ciberseguridad es relativamente reciente. Aparece a finales de los años 90 y principios de los años 2000. No obstante, antes de que fuese una palabra popularizada, diversos términos ocuparon supletoriamente su lugar cuando se habló respecto a temas de seguridad en el contexto cibernético. Es por ello que cuando surge, aunque es un término emergente, ya se tenía una noción respecto a lo que trataba, a su vez, la familiaridad que inspira induce a la confusión y suele ser interpretado de diversas maneras.

A criterio de este autor, la ciberseguridad es el conjunto de estrategias, prácticas y tecnologías diseñadas para proteger la confidencialidad, integridad y disponibilidad de la información y los sistemas informáticos contra amenazas digitales, garantizando así un entorno seguro y resiliente para las operaciones en el ciberespacio.

La integración entre finanzas y tecnología comenzó con hitos como la creación del cajero automático en los años 60, que permitió realizar retiros fuera del horario bancario mediante un código personal. Junto con la aparición de las tarjetas de crédito, estos avances representaron los primeros pasos hacia la automatización de los servicios bancarios y sentaron las bases del ecosistema bancario moderno.

En 1981, el New York City Bank (actual Citibank) comienza a ofrecer servicios de “banca en línea”, donde realizar podían consultar saldos y realizar algunas transacciones desde casa, a través de una línea telefónica; la banca en línea accesible mediante internet estuvo disponible en 1994. Mientras surgían empresas como Visa y MasterCard, que impulsaron los pagos electrónicos. A finales del siglo XX aparece PayPal, marcando un punto clave en la consolidación del Fintech como integración real entre tecnología y finanzas. Ya en el nuevo milenio, el sector financiero se transforma rápidamente con herramientas como el crowdfunding, las criptomonedas, el blockchain, la automatización de inversiones y los neobancos, reflejando la necesidad de equilibrio entre innovación y control bancario.

La ciberseguridad bancaria. Actualmente, no es visto como un concepto particular, sino que es definido de forma simplificada como ciberseguridad aplicada al contexto bancario. Ciertamente, para poder definir la ciberseguridad bancaria, es importante identificar si existe realmente alguna diferencia, ya sea particular o general, entre la ciberseguridad y la ciberseguridad bancaria, dado que puede generarse la duda respeto a ello. Como fue planteado anteriormente, la ciberseguridad bancaria no suele ser vista como concepto particular. Sin embargo, sí existe una diferencia sutil entre un concepto y otro.

La ciberseguridad bancaria es una rama subordinada dentro del ámbito más amplio de la ciberseguridad, lo que implica que las medidas y estrategias

implementadas en el sector bancario están intrínsecamente alineadas y son una extensión de los principios generales de protección y seguridad de la información.

Este enfoque específico en el ámbito bancario requiere adaptaciones particulares debido a la alta sensibilidad de los datos financieros y la necesidad de cumplir con regulaciones rigurosas, tanto a nivel nacional como internacional. Así, la ciberseguridad bancaria no solo incorpora las mejores prácticas del campo general de la ciberseguridad, sino que también implementa protocolos adicionales y medidas avanzadas para salvaguardar la integridad y la confianza en el sistema financiero.

En consideración a lo expuesto, la ciberseguridad bancaria puede ser conceptualizada como la adopción de estrategias y tecnologías avanzadas que preserven la privacidad, integridad y accesibilidad de los datos de quienes ofrecen servicios financieros y de sus clientes con el fin de salvaguardar los sistemas financieros y la información de estas entidades bancarias contra amenazas cibernéticas.

3.Régimen que regula la ciberseguridad bancaria en Panamá y su alcance

Para el sistema financiero global, el pilar fundamental para mantener su estabilidad y confianza yace en la ciberseguridad bancaria. Con la afluencia datos personales que se comparten diariamente a través de transacciones electrónicas y que su gestión crece de manera exponencial, la protección contra amenazas es primordial.

Panamá enfrenta desafíos únicos en materia de seguridad cibernética al ser un centro financiero internacional. Es decir, en ella se ubican gran cantidad de bancos, instituciones financieras, empresas multinacionales, inversores y profesionales de la industria financiera que están en busca de infraestructura avanzada, regulaciones favorables para así ganar acceso a mercados globales.

Soluciones Seguras, empresa especialista en ciberseguridad en Panamá, durante el “Cybersecurity Break”, un conversatorio sobre “Seguridad de los Datos y cumplimiento de las leyes y acuerdos vigentes”, reveló que “Panamá es el país que recibe más ciberataques a bancos y otras instituciones financieras” (Morris, 2023) y para el 2023 contabilizó 1.7 millones intentos de ataques de phishing. Esto conlleva a que alrededor del 80-90% de los ataques informáticos en Panamá van destinados a fraudes informáticos con intereses económicos, así como es el caso de España y demás países de la Unión Europea (Contreras, 2025). Reportan, además, que el gobierno panameño recibe alrededor de 803 ataques semanales. Estas amenazas son en 36% locales, mientras que el 64% restante proviene de Estados Unidos, Rusia y Ecuador.

Siendo la ciberseguridad un entorno consolidado relativamente reciente, son muchos los países que no han logrado solidificar una regulación que les permita resolver aspectos relativos a la protección de los datos detalladamente ni mucho menos establecer una normativa que abogue por la prevención de ataques en el plano digital.

En la República de Panamá desde lo más alto del eslabón normativo se ven reflejados, ya sea de manera directa o indirecta, derechos diseñados para la protección de datos personales. Así mismo, dentro de tratados internacionales suscritos, códigos, leyes, decretos y jurisprudencia.

Para el cuerpo normativo panameño, el concepto de privacidad y el de intimidad están íntimamente relacionados al abordar el espacio personal y la autonomía del individuo, haciendo fundamental regular cualquier ocasión en donde se realice o no una intromisión a este espacio. Por ende, se manejan dos premisas: la inviolabilidad de la propiedad privada y la inviolabilidad de las comunicaciones personales.

A nivel constitucional, las autoridades son responsables de velar por la protección de “la vida, honra y bienes de los nacionales dondequiera se encuentren y a los extranjeros que estén bajo su jurisdicción”, según el artículo 17 y más adelante, en el artículo 29, se establece que “la correspondencia y demás documentos privados son inviolables y no pueden ser examinados ni retenidos, sino por mandato de autoridad competente y para fines específicos”. En el tercer párrafo de ese mismo artículo, de igual manera se menciona la inviolabilidad de las comunicaciones privadas y que estas “no podrán ser interceptadas o grabadas, sino por mandato de autoridad judicial”.

Las garantías anteriormente expuestas son respaldadas por el artículo sexto de la Ley No. 31 de 8 de febrero de 1996, el artículo 13 del Código Procesal Penal panameño y los artículos 575 y 576 del Código de la Familia, y consecuentemente las normas punitivas en caso de infracción.

Específicamente en materia de protección y manejo adecuado de datos está la figura del Habeas Data. Originalmente concebida gracias a la promulgación de la Ley No. 6 de 22 de enero de 2002 y posteriormente elevada a rango constitucional, el Habeas Data, desde la óptica de esta investigación, es un derecho que se ejerce mediante una acción de inconstitucionalidad que lleva el mismo nombre. Consiste en permitir a las personas “acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión” (Constitución Política de la República de Panamá, 1972, Art. 42).

Naturalmente, con el paso del tiempo el carácter técnico de la ciberseguridad ha evolucionado y reconoce que necesita del involucramiento de aspectos legales, éticos y sociales. La protección de datos sensibles, tanto de la organización como de los clientes bancarios, y evitar la incidencia de fraudes requieren una colaboración estrecha entre la tecnología y la normativa legal.

El principio de legalidad es una garantía fundamental. Supone una característica esencial para constituir un Estado de Derecho, pues evita que los derechos fundamentales de los ciudadanos sean socavados por parte del poder público al hacer juzgamientos sin fundamento legal. Está consagrado en el artículo 31 de la Constitución Política de Panamá que señala que “sólo serán penados los hechos declarados punibles por Ley anterior a su perpetración y exactamente aplicable al acto imputado”.

Como bien lo establece la constitución, el principio de legalidad asegura que el Estado opere dentro de un marco legal previamente establecido y claro, cónsono, conceptualmente, con los ideales de justicia e igualdad ante la ley. Es decir, toda acción u actuación del poder público debe estar fundamentada y regulada por una ley previa.

El Capítulo III del Título II que versa sobre los “delitos contra la libertad” del Libro Segundo del Código Penal sanciona a quien se apodere indebidamente contenido de mensajes, sustraiga, destruya o extravíe, intercepte sin autorización comunicaciones o haga público el contenido de un mensaje privado, pudiendo ser estos físicos o virtuales; además, a quien utilice artefactos de escucha, transmisión, grabación o reproducción de conversaciones privadas sin autorización, prohibiendo también la persecución sin autorización de una persona con fines ilícitos. Las normas expuestas son la representación de conservación

del derecho a la intimidad o privacidad, garantía que es inherente de cada ser humano, es decir, se trata de la protección de un derecho humano.

A su vez, el Título VIII del Código Penal de la República de Panamá, sobre los delitos contra la "Seguridad Jurídica de los Medios Electrónicos" regula los delitos contra la seguridad informática. Allí regula determinadas conductas delictivas, como ingresar o utilizar de bases de datos, red o sistemas informáticos y apoderarse, copiar, utilizar o modificar datos en tránsito o contenidos en bases de datos o sistemas informáticos, o interferir, interceptar, obstaculizar o impedir la transmisión, y sus respectivas penas.

El Código Penal sanciona los delitos tradicionales que se llevan a cabo mediante el uso de esos medios electrónicos. Estas conductas dentro del código están consagradas como una modalidad o agravantes en el caso figuras delictivas independientes. Por lo tanto, hay una distinción entre los ataques contra los sistemas y los delitos que se cometen utilizando estos sistemas como herramientas. Estos casos de delincuencia cibernética son investigados a través de la Unidad de Investigaciones de Delitos Informáticos, dependiente de la Dirección de Investigación Judicial, y a través de la Fiscalía Superior Especializada en Delitos contra la Propiedad Intelectual y Seguridad Informática.

No es hasta que es introducida la Ley No. 81 del 26 de marzo de 2019 que se establece un régimen general de protección de datos personales con "el objeto de establecer los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales de las personas naturales en la República de Panamá" (artículo 1). Esta fue reglamentada, seguidamente, por el Decreto Ejecutivo No. 285 de 28 mayo de 2021 y reconoce que los derechos que tienen los titulares de los datos personales son irrenunciables.

Dentro de la Ley 81 de 2019, de igual forma, están descritos en nueve numerales los principios por los cuales debe regirse el tratamiento de datos. El primero de ellos es el principio de lealtad, que quiere decir que los medios por los cuales se adquieran los datos deben ser lícitos, sin recurrir al fraude, engaño o deslealtad.

El segundo principio es el de finalidad, el cual establece que los datos deben ser recolectados con un propósito específico y no pueden ser utilizados ulteriormente para fines distintos ni conservados más allá del tiempo requerido para su tratamiento. De manera similar, el principio de proporcionalidad indica que únicamente deben solicitarse los datos estrictamente necesarios para cumplir con el objetivo establecido.

El principio de veracidad y exactitud aboga por que prime la precisión y actualidad de los datos, es decir, no solo implica la exactitud de la recolección de datos, sino también la responsabilidad de mantener dichos datos actualizados.

El principio de seguridad de los datos, como su nombre bien lo indica, alude al resguardo de los datos mediante la creación de procesos organizativos y medidas técnicas que garanticen su preservación, con mayor énfasis en los datos considerados sensibles y, en caso de la seguridad sea vulnerada o sustraída, informar con brevedad al titular de los datos.

Las comunicaciones e información suministrada al titular de los datos relativa al tratamiento de estos deben ser realizada mediante un lenguaje sencillo y claro, e informarle sobre sus derechos, así como establece el principio de transparencia. Por ejemplo, los derechos ARCO son parte del repertorio de garantías que posee el titular de los datos. Sus siglas representan los derechos de acceso, rectificación, cancelación y oposición,

es decir, toda persona, como titular de sus datos personales o a través de su representante, tiene derecho a acceder a ellos, a rectificarlos, a solicitar su cancelación u oponerse a su tratamiento (Centro Nacional de Control del Gas Natural, 2021).

En la actualidad, se agrega una garantía adicional, la garantía de la portabilidad, es decir, el derecho del titular a obtener una copia de sus datos personales, estructurados, en formato genérico y común para que puedan ser compatibles con distintos sistemas y/o transmitirlos a otro responsable, siempre que los datos hayan sido proporcionados directamente por el titular, se trate de un volumen significativo cuando el tratamiento de los datos se fundamente en el consentimiento del titular o sea necesario para la ejecución de un contrato. Pasarían de ser los derechos ARCO a ser los derechos ARCOP.

El principio de confidencialidad manifiesta la obligación de las personas que intervengan en el tratamiento de datos de mantener el secreto en relación a estos, incluso después de haber terminado la relación con el titular. El principio de portabilidad señala que el titular de los datos puede solicitar una copiar de los datos por parte del responsable y este debe entregarlo en un formato genérico. Guarda similitud con el derecho al acceso a los datos, parte de los derechos ARCO.

Uno de los principios con más relevancia y/o que causa controversia es el principio de licitud precisamente debido al Acuerdo No. 5 del 2021. Este principio explica que el tratamiento de un dato personal es considerado lícito siempre que en su recolección medie “el consentimiento previo, informado e inequívoco del titular del dato o por fundamento legal” (Ley 81 de 2019, 2019, Artículo 2). Existe un roce entre este principio y este acuerdo debido a que no se respeta el consentimiento del usuario a la hora de solicitar de forma obligatoria validación biométrica. Esto implica que el titular de los datos o cliente bancario no tiene la potestad de elegir entre utilizar el nuevo sistema de implementación de seguridad. De negarse a hacerlo, pierde la capacidad de realizar movimientos bancarios a cuentas de terceros.

Los bancos aclaran que la medida se realiza como forma de fortalecimiento de la seguridad tanto de los usuarios como de la plataforma, pero este tratamiento de datos no constituye según la ley una excepción al consentimiento ni hace a este tipo de instituciones financieras designadas, configuradas o capacitadas para el tratamiento de datos sensibles.

Otro principio en pugna con este acuerdo es el de proporcionalidad, pues el banco no informa con qué fin está recolectando ese tipo de información. Sin mencionar la expansión de la brecha que económica que existe, pues es irrisorio pensar que todos los usuarios de la plataforma tienen acceso a un dispositivo móvil con cámara frontal, poniendo en desventaja a aquellos de recursos limitados.

Diversos juristas consideran estas medidas arbitrarias como directas violaciones no sólo a la Ley de Protección de Datos, sino a la Constitución misma y a los demás tratados internacionales de los que la República de Panamá es signatario, pues vulneran el derecho a la privacidad y al principio del consentimiento libre, previo e informado (IPANDETEC, 2024) al no presentar alternativas, por lo que impera la obligatoriedad.

La ley bancaria aborda el manejo de la información de los usuarios, en donde principalmente se recalca que está prohibido compartir en cualquier modo o medio información de los clientes bancarios sin su

consentimiento, salvo ciertas condiciones, como para la prevención del delito de blanqueo de capitales, financiamiento del terrorismo y demás delitos relacionados. Consistentemente, la Superintendencia de Bancos publica el Acuerdo No. 001-2022 del 24 de febrero de 2022 que establece lineamientos especiales para la protección de datos personales tratados por las entidades bancarias.

En materia de cibercrimen, Panamá ratificó el Convenio sobre la Ciberdelincuencia, también llamado Convenio de Budapest. Dicho convenio fue motivado por “la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional" (Convenio de Budapest sobre la ciberseguridad, 2021, Preámbulo).

Este convenio se ha mantenido relevante, a pesar de su carácter punitivo, gracias a la constante actualización, a manos del Cybercrime Convention Committee (T-CY), y su ánimo de incluir discusiones referentes a la protección de los derechos fundamentales, es por ello que ha subsistido como base legal para la estructuración de la cooperación internacional y ha servido como guía para la formulación de legislaciones nacionales posteriores.

De esta convención es importante resaltar la motivación para la creación satisfactoria de una red de puntos de contactos entre los países firmantes con el compromiso de permanecer disponibles las veinticuatro horas del día para prestar atención inmediata cuando les sea solicitado a efecto de investigaciones, recolección de pruebas electrónicas y procedimientos referentes a ciberdelitos. En Panamá, el punto de contacto es la Dirección de Investigación Judicial de la Policía Nacional, específicamente, la Oficina de Interpol Panamá.

Posteriormente se publican dos protocolos adicionales. El primer protocolo se titula “Primer Protocolo Adicional relativo a la penalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos (STCE 189)” es publicado el 1 de marzo de 2006. Hasta la fecha 46 países son signatarios y, de ellos, sólo 36 lo han ratificado (Consejo de Europa, 2023).

El segundo protocolo adicional de nombre “Segundo Protocolo Adicional relativo a la cooperación internacional reforzada y la divulgación de pruebas electrónicas (STCE 224)” fue publicado el 17 de noviembre de 2021 y su misión principal consiste en crear un marco legal que facilite la divulgación de la información sobre el registro de nombres de dominio, promueva la cooperación directa con proveedores de servicios para obtener datos de suscriptores y de tráfico, asegure una respuesta rápida en situaciones de emergencia, impulse mecanismos de asistencia mutua y garantice la protección de los datos personales (Consejo de Europa, 2003).

Este protocolo es resultado de las dificultades que presentaban los Estados “para acceder a los datos privados en función de cuestiones como la territorialidad, la computación en la nube y el alcance de las jurisdicciones” (Martins Dos Santos, 2022). Luego varias discusiones al respecto, se determinó que era necesaria la creación de este nuevo protocolo. Este tiene hasta la fecha 44 países signatarios, donde sólo dos de ellos lo han ratificado (Consejo de Europa, 2023), en consecuencia, el protocolo no ha entrado en vigencia. La República de Panamá actualmente no es signatario, por ende, tampoco ha ratificado este protocolo.

Según el Consejo de Europa, el segundo protocolo se presenta como una actualización esencial para hacer del Convenio de Budapest un instrumento más eficaz. Este protocolo revisa temas como el acceso transfronterizo a los datos y la cooperación legal mutua, además de establecer directrices más claras para la colaboración directa entre las autoridades y los proveedores de servicios digitales, incluyendo a aquellos que operan infraestructuras de internet (Zachar, 2021).

A pesar de las ventajas que se ventilaron respecto a este documento, organizaciones que representan a la sociedad civil, como Derechos Digitales, Electronic Frontier Foundation y Al Sur advirtieron en su momento sobre las consecuencias que puede tener la emisión de este texto.

Denunciaron fallas en el cumplimiento de los principios multisectoriales de transparencia, rendición de cuentas e inclusión. Una de sus mayores preocupaciones es la vulneración de los derechos humanos al facilitar el acceso a los datos de la ciudadanía por parte de las autoridades, violando así su derecho a la intimidad y privacidad, además de la posibilidad de criminalizar la libertad de expresión.

Así mismo muestran su inquietud respecto a la violación del principio de legalidad y legitimidad dentro de las investigaciones, pues temen que no se respeten las garantías procesales penales, normativa sobre protección de datos y legislación internacional sobre derechos humanos.

Señalan que no se puede garantizar que cualquier interferencia en el derecho a la intimidad sea ser legítima, necesaria y proporcional, y basada en leyes accesibles al público, precisas y no discriminatorias, mucho menos podría garantizarse la fiscalización imparcial para asegurar que se respeten la inmunidad y los privilegios legales, aun cuando sea por parte de una autoridad judicial competente, sabiendo que podrían actuar sin autorización.

Pese a los diversos intentos realizados, el protocolo es una realidad, por lo que sólo queda alertar sobre estos riesgos a los países con miras a ratificarlo. No obstante, esta iniciativa no es la única en la materia en discutirse recientemente. La Organización de las Naciones Unidas, a través de su Asamblea General, creó un comité ad hoc para elaborar un nuevo tratado internacional que aborde los delitos cibernéticos.

La resolución que le da vida a la idea plantea que el comité estará compuesto por especialistas de diversos partes del mundo que busquen combatir el uso de las tecnologías como un arma. Países como Estados Unidos y bloques como la Unión Europea comunican su descontento, mientras que la propuesta es bien recibida por países como China, Camboya y Rusia, que figura como el impulsor de esta idea.

Paralelamente, la sociedad civil internacional ha puesto en tela de duda la necesidad de promover un nuevo tratado, cuando el Convenio de Budapest sigue vigente, y la celeridad con la que se prevé hacerlo. Más allá, resulta inquietante que los países que apoyan esta visión puedan utilizarlo para emplear la tecnología a modo de coerción, control y represión, volviéndolo una fórmula para el tecno-autoritarismo.

4.La evolución jurisprudencial en materia de responsabilidad bancaria de ciberseguridad en el derecho comparado

Resulta imperioso el estudio de decisiones judiciales extranjeras pues es clave para entender las distintas interpretaciones legales y obtener nuevos enfoques judiciales frente a problemas que comparten factores de

extraterritorialidad, especialmente en áreas de rápida evolución, como la responsabilidad bancaria por motivo de violación de protección de datos o vulneración de sistemas de seguridad.

Este análisis no solo reúne diversas interpretaciones, sino que permite comparar los fundamentos legales adoptados por cada y sus efectos en la práctica, tanto para los individuos, como para las entidades involucradas. Permitirá, además, evaluar y destacar las falencias y el atraso normativo entre cada jurisdicción, mostrando elementos de estas resoluciones que podrían ser adaptables a otros territorios, proporcionando una base más sólida para futuras reformas legislativas o interpretaciones judiciales.

En un caso relativamente reciente, el Cuarto Tribunal Regional de Tubinga, una ciudad alemana dirimió un conflicto relacionado con un ciberataque sufrido por una empresa asegurada, cuyo contrato de ciberseguro fue cuestionado por la aseguradora debido a supuestas omisiones en las obligaciones precontractuales de información.

La demandante es una empresa alemana dedicada a la fabricación de componentes para sistemas de calefacción ecológicos. En 2020, su infraestructura IT incluía varios servidores, algunos de los cuales estaban desactualizados y no contaban con las últimas actualizaciones de seguridad del sistema operativo Microsoft Windows. Parte de su infraestructura estaba subcontratada a una empresa externa.

Durante el mes de mayo de ese mismo año, la empresa fue víctima de un ataque cibernético mediante un método conocido como "Pass-the-Hash". Este ataque permitió a los atacantes obtener derechos de administrador en todos los servidores conectados. El ataque se ejecutó tras la apertura de un archivo malicioso adjunto a un correo electrónico de phishing por parte de un empleado. Esto permitió a los atacantes introducir un ransomware que encriptó los servidores de la empresa, interrumpiendo completamente las operaciones.

Como consecuencia, la empresa fue víctima de diversas afectaciones, que incluyeron la paralización total de la infraestructura IT, amenazas de publicación de datos sensibles por parte de los atacantes y costos significativos para reconstruir el sistema, lo cual tomó varios meses.

La demandante contaba con un contrato de ciberseguro celebrado en abril de 2020. Este contrato cubría, entre otros riesgos, interrupciones operativas derivadas de ciberataques. La suma asegurada era de 5 millones de euros. El contrato incluía obligaciones de información previa para la empresa asegurada sobre el estado de su infraestructura IT.

Sin embargo, la aseguradora se negó a cubrir el daño alegando que la demandante había incumplido su obligación de informar sobre el estado de sus servidores. Argumentó que la empresa no reveló que varios servidores no estaban actualizados y carecían de medidas de seguridad adecuadas, lo que consideró un incumplimiento de las condiciones precontractuales y una causal del ataque.

El conflicto giró en torno a si el incumplimiento de las obligaciones precontractuales por parte de la demandante (omisión de información sobre actualizaciones de servidores) justificaba la negativa de la aseguradora a pagar, y si existía un vínculo causal entre estas omisiones y el alcance del daño ocasionado por el ciberataque. En este contexto, la aseguradora sostuvo que la empresa había respondido incorrectamente a las preguntas precontractuales relacionadas con el estado de sus medidas de seguridad

IT, reflejando negligencia o dolo, y que, de haber sabido el estado de las estructuras de IT de la empresa, no se hubiese firmado el contrato en primer lugar, por consiguiente, esto invalidaba la cobertura del seguro. Por su parte, la empresa refuto esas acusaciones. Sostuvo que las preguntas realizadas por la aseguradora fueron contestadas con el nivel de entendimiento sobre los sistemas de tecnología de la información que poseían al momento de efectuada la reunión con la aseguradora. Además, argumentan que la aseguradora conoce los riesgos y vulnerabilidades que pueden presentarse en la esfera cibernética.

Esto demuestra como el desconocimiento en materia cibernética por parte de los involucrados juega un papel importante a la hora de determinar la solución de una controversia, sin dejar de lado la implicación del dolo o negligencia insinuada dentro del proceso, y como con ese razonamiento, se pretende desestimar la acusación.

Este caso ejemplifica como el examen del desconocimiento o de la omisión de información sobre los servidores desactualizados determina si este influyó en la ocurrencia del ataque y en la magnitud del daño y si la empresa debió reforzar sus medidas de seguridad después de firmado el contrato con la aseguradora. Consecuentemente, el Tribunal de Regional de Tubinga concluyó que la aseguradora era responsable de indemnizar a la empresa por los daos causados. El tribunal baso su decisión en que se demostró que la no actualización del sistema IT de la demandante no influyo en la ocurrencia ni en la magnitud del ataque. El "Pass-the-Hash" explotó una debilidad inherente al diseño de Windows.

Por otra parte, el tribunal concluyó que no hubo dolo ni intención de engañar por parte de la empresa, frente al argumento de dolo y negligencia enunciado por la aseguradora y que estos últimos conocían los riesgos tecnológicos a los que se enfrentaban al asegurar la empresa y tampoco pactaron implantas requisitos de seguridad más rigurosos.

Luego de un cálculo que utilizaba un método basado en el balance económico de la empresa antes y después del ciberataque, la corte concluyo que la aseguradora debía pagar un monto de 2,858,923.54 € (3,017,879.69 USD) más intereses a la demandante.

En febrero de 2016, el Banco Central de Bangladesh fue víctima de un robo cibernético sin precedentes. Los atacantes lograron infiltrarse en el sistema de transferencia de fondos de la Sociedad para las Comunicaciones Interbancarias y Financieras Mundiales y emitieron solicitudes fraudulentas para transferir 1,000 millones de dólares aproximadamente desde las cuentas del Banco de Bangladesh en la Reserva Federal de Nueva York.

Un año antes, en enero de 2015, enviaron un correo electrónico de apariencia inofensiva a varios empleados del Banco de Bangladesh. Provenía de un solicitante de empleo que se hacía llamar Rasel Ahlam e incluía una invitación para descargar su CV y carta de presentación de un sitio web. Al menos una persona dentro del banco cayó en la trampa, descargó los documentos y se infectó con los virus ocultos en su interior.

Sin embargo, no actuaron hasta el año siguiente, escogiendo meticulosamente la fecha del ataque. Ubicada en una habitación protegida con medidas de alta seguridad en el décimo piso de la oficina principal del ente en Dhaka, estaba la impresora clave para el atraco. La máquina era utilizada para imprimir registros de las transferencias multimillonarias que entraban y salían del banco.

Los ladrones esperaron hasta que el banco cerró a las 8:00 p.m. el jueves 4 de febrero de 2016 para atacar, aprovechando que aún era de día en Nueva York. Se conectaron al sistema del Banco de Bangladesh y enviaron treinta y cinco órdenes de pago a bancos en otras jurisdicciones (Das & Spicer, 2018).

El Banco de la Reserva Federal de Nueva York señaló treinta de las órdenes de pago porque necesitaba más información para confirmar que las órdenes no implicaban a países o personas sancionadas y comenzó a enviar mensajes al Banco de Bangladesh para aclarar estas órdenes. Sin embargo, ya había procesado cinco órdenes cuando descubrió las señales de alerta y comenzó a investigar las órdenes de pago (Das & Spicer, 2018).

Uno de los pedidos que se recibieron fue a Pan Asian Bank en Sri Lanka, por valor de 20 millones de dólares. El banco de Sri Lanka pensó que el pago parecía inusualmente grande para un país del tamaño de Sri Lanka. También se dio cuenta de que el nombre del titular de la cuenta parecía estar mal escrito, decía "Fandation" en lugar de "Foundation".

El Pan Asian Bank retuvo los fondos mientras se verificaba con un banco corresponsal para confirmar que había recibido la orden correctamente. Este retraso significó que el Banco de Bangladesh pudo recuperar los 20 millones de dólares enviados a través de esa orden (Quadir, 2016). Las otras cuatro órdenes, sin embargo, se enviaron con éxito a la Rizal Commercial Banking Corporation, una institución financiera en Filipinas (Hammer, 2018).

El viernes 5 de febrero de 2016, el personal del organismo descubrió que la impresora no estaba funcionando. Asumieron que era un problema común, como cualquier otro día, pues fallos así habían ocurrido antes. Un empleado intentó que las órdenes se imprimieran, pero no pudo, así que pidió a otra persona que arreglara la impresora y se fue a casa (Das & Spicer, 2018). Era el comienzo del fin de semana en Bangladesh, que se extiende de viernes a sábado. Así que la sede del banco en Daca comenzaba dos días libres.

El sábado 6 de febrero, Cuando el personal del banco reinició la impresora, descubrieron lo sucedido. Intentaron contactar con el banco neoyorquino, pero a pesar de haber reconfigurado la impresora, su sistema SWIFT seguía inoperante. Encontraron una dirección de correo electrónico en línea y le enviaron tres mensajes diciendo que su cuenta había sido hackeada. Pero esa dirección de correo electrónico en la Reserva Federal no era monitoreada durante los fines de semana. También llamaron y enviaron un fax, pero tampoco eran monitoreados durante los fines de semana (Das & Spicer, 2018).

El dinero fue transferido a un banco en Manila, capital de Filipinas. El lunes 8 de febrero fue el primer día del Año Nuevo Lunar, un feriado nacional en toda Asia.

Por lo que, aunque el banco estadounidense estaba abierto y el Banco de Bangladesh ya tenía su sistema SWIFT operativo, el banco filipino estaba cerrado y no recibió los 100 mensajes enviados por parte del banco bengalí (Allison, 2018). Para cuando RCBC finalmente actuó, el dinero había desaparecido (Das & Spicer, 2016). En total, los delincuentes tuvieron un periodo de 5 días para la ejecución de su plan. El dinero fue lavado a través de casinos, figuras que no están reguladas bajo la ley de blanqueo de capitales de Filipinas. Curiosamente, después del robo, el Banco de Bangladesh inicialmente contrató a una empresa de TI con

sede en los Estados Unidos para borrar las pruebas del incidente, en lugar de centrarse inmediatamente en recuperar los fondos robados (Kabir & Hosen, 2024).

El Departamento de Investigación Criminal identificó a 76 individuos de ocho países diferentes (Nazrul, 2024) como participantes activos en el robo. Los medios internacionales cubrieron el incidente por primera vez cuando el Banco de Bangladesh presentó una denuncia ante un tribunal filipino para solicitar la restitución del dinero robado, después de que los medios nacionales se enteraron del robo.

El caso planteó diversos conflictos legales y técnicos. La pregunta más evidente es quién responde por el dinero perdido. En definitiva, si se pudiesen señalar a los perpetradores, serían ellos los obligados a responder por el acto, pero no es el caso.

Inicialmente, el banco bengalí anunció que procedería a demandar al Banco de la Reserva Federal de Nueva York, alegando que estos eran responsables del procesamiento de las 35 transacciones bancarias fraudulentas para que consecuentemente restablecieran los fondos perdidos (Quadir, 2016).

La gran mayoría de los bancos comerciales y de los bancos centrales de todo el mundo confían en el canal de comunicación seguro de SWIFT y en sus protocolos de autenticación como método principal para verificar que las instrucciones bancarias recibidas de las contrapartes son auténticas (Baxter, Jr., 2016). Suponiendo que el Banco de Bangladesh firmara el acuerdo estándar con el Fed, el banco bengalí aceptó la autenticación de las órdenes de pago únicamente por medio de SWIFT.

Demandar bajo el argumento que el sistema SWIFT es insuficiente contraría su propia postura. Después del incidente se implementaron nuevas medidas de seguridad al momento de procesar órdenes de pago para evitar que el hecho se suscitara nuevamente. Dichas medidas de seguridad incluían llamadas interbancarias hasta en 3 ocasiones a altos funcionarios del Banco de Bangladesh cuyas muestras de voz habían sido compartidas al Fed con anterioridad (Quadir, 2016). Para deshacerse de la trabajosa y demorada disposición, el banco bengalí configuró sus medidas de seguridad de forma que el sistema SWIFT fuese la única forma oficial de autenticación de las transferencias otra vez. Este cambio fue probablemente la razón por la que el banco asiático decidió no formalizar el reclamo contra el banco de Nueva York ante los tribunales.

Actualmente, están activas varias investigaciones al respecto. En 2019, el Banco de Bangladesh demandó en The United States District Court for the Southern District of New York a la institución financiera filipina RCBC. La demanda plantea la restitución de los fondos perdidos por el banco bengalí. RCBC niega todas las acusaciones. A la fecha, el caso aún sigue abierto, pero las partes se inclinan a un acuerdo privado para poner fin a la controversia.

Por su parte, la exdirectora de RCBC fue hallada culpable de los 8 cargos de blanqueo de capitales que se le imputaban luego de investigaciones del propio gobierno filipino. Enfrenta de 4 a 7 años de cárcel por cada cargo y fue condenada a pagar 109 millones de pesos filipinos (alrededor de $1,900,000.00 dólares) por sus fallos a la hora de prevenir las transacciones del dinero robado (GNDiario, 2019). Junto con ella, otros 5 trabajadores de la institución fueron imputadas, pero debido a falta de respuesta y colaboración de China y Sri Lanka el caso se ha estancado (Kaium, 2025).

De igual manera, el Bangko Sentral ng Pilipinas, luego de una investigación propia, multó a RCBC con un monto de mil millones de pesos filipinos ($18,000,000 de dólares aproximadamente).

Este caso tiene muchos puntos que discutir, pero en un intento de ser breve sólo se alumbraran aquellos que más saltan a la vista. Lo primero es determinar cuál de todos los involucrados tiene la responsabilidad de resarcir los daños causados. Como se mencionó anteriormente, si se pudiese dar con los responsables del hecho, serían ellos. Actualmente se le atribuye el ataque a un grupo de hackers norcoreanos llamado “Grupo Lazarus”, sin embargo, no hay certeza de que fuesen ellos los perpetradores.

Con esta modalidad de delitos a través de plataformas digitales esta incógnita resurgirá una y otra vez, pues el anonimato es casi una garantía que no le es indiferente este tipo de transgresiones. Pero un desarrollo posterior del tema pecaría de extralimitación.

Queda determinar si el Banco de Bangladesh cumplió con sus obligaciones de ciberseguridad. La respuesta es sencilla, no. La tarea delincuencial se desarrolló con tal elegancia que es obvio que más allá de una evidente experticia, la seguridad –o la falta de ella- les permitió moverse con comodidad dentro de los sistemas del banco sin detectados por un año. No hubo capacitación alguna al personal sobre los riesgos cibernéticos más comunes ni de cómo evitarlos. No hubo recomendación ni instrucción alguna. Tampoco seguían directrices de seguridad básicas, que debían ser obligatorias para centros de tal importancia. Todas las computadoras de banco estaban conectadas entre sí ya la misma red de internet, además no estaban dotadas de firewall. Como si no fuese obvio, un oficial del banco bengalí afirmo comenzadas las investigaciones que “puede haber habido una deficiencia en el sistema (Quadir, 2016).

Pese a todo esto, no existe ninguna investigación o acusación de negligencia dirigida al Banco de Bangladesh.

Otra interrogante es si el sistema SWIFT puede ser considerado responsable por el hecho. Se conoce que los atacantes no explotaron una debilidad del sistema SWIFT, sino que aprovecharon la ciberseguridad laxa del banco. Como proveedor de servicios de mensajería seguros entre bancos, el sistema SWIFT no tiene la responsabilidad de fiscalizar los sistemas internos del banco ni sus protocolos de seguridad. Dicho esto, SWIFT sí extiende a sus clientes recomendaciones de seguridad, pero es desconocido si dentro de sus obligaciones en ese momento se hallaba la de supervisión sobre la obediencia de dichas recomendaciones.

A decir verdad, después de este primer ataque, el sistema SWIFT sufrió muchas otras vulneraciones, la mayoría no de conocimiento público, por lo que, seguido el incidente, el sistema SWIFT modificó su SWIFT Customer Security Program indicando que, para seguir operando con ellos, todas las entidades adheridas debían cumplir con el nuevo Customer Security Controls Framework , de lo contrario, cancelarían la suscripción de no cumplir con dicho marco de ciberseguridad (Benitez, 2021).

En materia de Derecho Internacional Privado, surge la duda de si Estados Unidos era competente para conocer de la demanda que el Banco de Bangladesh le sigue a RCBC. Para ello es necesario determinar la competencia judicial internacional.

La competencia judicial internacional es, en palabras del Dr. Gilberto Boutin (2018), el quid del Conflicto de jurisdicción y “se establece a través de la verificación que hace el propio juez del foro para conocer si

verdaderamente la regla de competencia judicial u ordenamiento judicial le atribuye conocimiento a la hipótesis en examen" (p.181).

La determinación de la competencia judicial internacional tiene dos modalidades, la competencia judicial directa y la competencia judicial indirecta. El Dr. Boutin (2018) explica que la competencia judicial directa es "el método por medio del cual el juez es competente cuando sus propias reglas de atribución judicial lo designan como competente para conocer de in litigio de carácter internacional" (p. 181), mientras que la competencia judicial indirecta es "la verificación que hace el juez del foro sobre la competencia judicial internacional del juez extranjero que ha emitido un fallo para producir sus efectos en su territorio" (p.182).

Según lo que se desprende, solo corresponde enfocarse en el primero, la competencia judicial internacional directa. De acuerdo con lo señalado, la competencia directa "se resume como el conjunto de reglas que le atribuyen conocimiento al juez del foro sobre la base de su criterio de conexión determinado" (Boutin, 2018, p. 181), es decir, "es el orden judicial que reglamenta el ámbito de conocimiento que tiene el juez de la causa para conocer o no de un litigio de carácter internacional" (Boutin, 2018, p. 182).

En este contexto, RCBC presentó tres mociones para desestimar la reclamación formulada por el Banco de Bangladesh. La primera moción solicita que se desestime por forum non conviniens. Como bien dicta el Dr. Gilberto Boutin (2018), es "la apreciación instintiva [...] que tiene el juez anglonorteamericano [...] para rechazar el conocimiento de un negocio jurídico cuando él considera que el tribunal más justo no es el tribunal del foro, sino de otro ordenamiento jurídico" (p.186), es decir, el juez evaluó en base a doctrina si es o no competente para conocer el caso.

Para determinarlo, se basó en 3 criterios: (1) la consideración que se debe conceder a la elección del foro por el demandante; (2) la adecuación del foro alternativo propuesto por los demandados; y (3) el equilibrio entre los intereses públicos y privados implicados en la elección del foro.

Luego del examen de la Corte, el juez determinó que no había forum non convieniens, pues, a pesar de que la Regla General establece que "la elección de un foro de los Estados Unidos por un demandante extranjero tiene derecho a menos deferencia" en comparación con el foro doméstico del demandante, la demanda tiene ciertamente una conexión de bona fide con los Estados Unidos y el foro de elección y lo declaran obvio al considerar que el robo tuvo lugar en el distrito en donde fue presentada la demanda y que atacaron una importante institución de Estados Unidos ubicada en New York.

El demandado también alegó que la demanda era producto de forum shopping. El forum shopping es una "manipulación de la competencia judicial internacional que ejerce un demandante [...] frente a otra [parte] [...] para interponer una demanda ante un Estado en donde pueda sacar una mayor ventaja de carácter judicial o patrimonial" (Boutin, 2018, p. 178).

Si bien se puede argumentar que el banco bangladesí eligió estratégicamente el foro estadounidense para presentar su demanda basados en la posibilidad de obtener una mayor indemnización o en las dificultades procesales que podían presentar demandando en el domicilio del banco filipino, no se puede desconocer que las transacciones realizadas fueron autorizadas por un banco estadounidense, lo que evidencia un criterio de conexión legítimo con la jurisdicción de Estados Unidos.

Para determinar si el foro alternativo propuesto es adecuado, los demandados deben susceptibles de notificación del proceso allí, y debe permitir el litigio del objeto de la controversia. Teniendo en cuenta estas características, Filipinas era un foro adecuado para conocer la reclamación.

En el tercer criterio, el demandado alegó como factores de interés privado la facilidad de acceso a pruebas, la disponibilidad y costo de asegurar la asistencia de testigos, la posibilidad de hacer cumplir una sentencia para facilitar un juicio eficiente y económico.

Sus factores de interés público se basaron en las dificultades administrativas por la congestión judicial, el interés local en resolver disputas en su jurisdicción, la conveniencia de un foro familiarizado con la ley aplicable, la evitación de conflictos legales innecesarios y la equidad en evitar imponer deberes de jurado a ciudadanos no relacionados con el caso.

La Corte determinó que los factores de interés privado eran neutrales, pues la mayoría de las pruebas e información relevante se encontraba en formato electrónico, accesible desde ambas jurisdicciones; mientras que encontró los factores de interés público ligeramente inclinados a su foro, ya que es usual que casos de naturaleza transfronteriza tomen de 10 a 20 años en llegar a una conclusión en los tribunales filipinos. Es así como fundamentan la denegación a la moción de desestimación de la reclamación.

La segunda moción también pedía desestimar la reclamación fundamentándose en la Regla de Procedimiento Civil 12 que dicta que un tribunal federal puede desestimar un caso por falta de jurisdicción conforme a la Regla 12(b)(1) si carece del poder constitucional o legal para resolverlo; es decir, si son “totalmente insustanciales o frívolas” o si se presentan únicamente para obtener jurisdicción. La Corte negó la moción porque la reclamación bajo la Ley RICO no era “totalmente insustancial o frívola”.

La tercera moción que pretendía la desestimación basada en la no declaración de una reclamación RICO si fue concedida, pues al no quedar ninguna reclamación federal viable, la Corte rechazó ejercer jurisdicción suplementaria sobre las reclamaciones de derecho estatal. Esto quiere decir que, aunque la Corte retuvo inicialmente la jurisdicción federal, la desestimación de la reclamación RICO dejó sin fundamento la competencia para atender las reclamaciones estatales.

A la fecha de publicado este escrito, no ha sido resuelto este caso. El Banco de Bangladesh recuperó una parte de los fondos desviados, no obstante, la mayor parte de los 81 millones de dólares sigue sin localizarse. Las autoridades de Bangladesh tienen su propia investigación en pie, sin embargo, está estancada y la fecha de presentación del informe final ha sido extendida por octagésima ocasión. Esto debido a la falta de cooperación judicial internacional. A pesar de existir un convenio que trata la cooperación internacional en materia de cibercrimen, las autoridades bangladesíes continúan a la espera de respuesta a las Solicitudes de Asistencia Jurídica Mutua en Asuntos Penales enviadas a China y Sri Lanka. Sin la información solicitada no podrá ser posible completar el informe.

CONCLUSIÓN

El presente artículo de investigación identifica las diferentes normativas existentes en materia de ciberseguridad, profundizando en aquellas que puedan tener relación con el cuidado y protección de datos en el ámbito bancario. En esa misma medida, ha puesto en manifiesto la gran fractura negligida entre la

rápida evolución de las tecnologías y la normativa que debe regularlas, tanto a nivel nacional como internacional.

El Convenio de Budapest es un tratado que al momento de su celebración intentó suplir de forma apresurada la necesidad repentina de estructurar algo que a luces se notaba desconocido. Pero al hacerlo de forma general, sobra decir que existen vacíos que hoy día aún faltan por llenar, concretamente en la esfera del derecho bancario, siguiendo el hilo de este escrito. Adicional, lo anterior demuestra como la disposición juega un rol determinante en el cumplimiento de las normas.

Para que cumpla su cometido real todos los Estados deben comprometerse a adoptar las disposiciones que el convenio plantea. Debe existir un deseo real de resolución de conflictos supranacionales utilizando el marco normativo, que, aunque superficial y en muchos casos insuficiente ante los retos de la digitalización, se erige como el más idóneo al momento, para evitar conflictos de Derecho Internacional Privado con una provocada fragmentación normativa.

Un punto crítico de la investigación fue la importancia de los bancos y demás instituciones financieras como sistemas críticos de un país. Una posición como esa va acompañada de una importancia significativa. Un poder como el que ostentan este tipo de instituciones debe ser regulado con más ímpetu para evitar acrecentar la brecha que ya existe entre el banco y su cliente bancario. La protección de los derechos de los consumidores bancarios amerita una mejor reglamentación, además de una fiscalización efectiva.

Finalmente, resulta imperativo que se le dé la importancia que amerita a las incógnitas que han surgido y seguirán surgiendo dentro de la ciberseguridad bancaria, y eso se logra a través de la creación de nuevas normativas nacionales e internacionales, que sean amigables con el usuario, estrictas con las instituciones bancarias y severas con aquellos que las infringen. No se puede olvidar que el campo tecnológico tiene un ánimo cambiante, siempre buscando crecer, por lo que los limites deben crecer con él para procurar siempre transparencia y armonía con los usuarios en general.

REFERENCIAS BIBLIOGRÁFICAS

Acuerdo No. 003-2012. Por el cual se establecen lineamientos para la gestión del riesgo de la tecnología de la información. Superintendencia de Bancos de Panamá. 22 de mayo de 2012.

Acuerdo No. 005-2021. Por medio del cual se modifica el artículo 15 del Acuerdo No. 6-2011. Superintendencia de Bancos de Panamá. 23 de noviembre de 2021.

Agencia de Noticias Panamá. (2024, 11 abril). Ciberdelincuentes intentaron 1.7 millones de ataques en Panamá durante el 2023. https://www.anpanama.com/Ciberdelincuentes-intentaron-17-millones-de-ataques-en-Panama-durante-el-2023-16355.note.aspx

Alzoubi, H.M., Ghazal, T.M., Hasan, M.Z., Alketbi, A., Kamran, R., Al-Dmour, N.A., e Islam, S. (2022). Cyber Security Threats on Digital Banking. 1st International Conference on AI in Cybersecurity (ICAIC), págs. 1-4, doi: 10.1109/ICAIC53980.2022.9896966.

Asaad, R. R. (2020). Implementation of a Virus with Treatment and Protection Methods. icontech international journal, 4(2), 28–34. https://doi.org/10.46291/ICONTECHvol4iss2pp28-34.

Autoridad Nacional Para La Innovación Gubernamental (s. f.). Legislación. Panamá Cibersegura. https://panamacibersegura.gob.pa/index.php/legislacion/

Bauer, Paula. (2022, diciembre 9). Protocolo Adicional Segundo al Convenio de Budapest sobre Ciberdelincuencia. C. R. & F. Rojas Abogados. https://rojas-lawfirm.com/protocolo-adicional-segundo-al-convenio-de-budapest-sobre-ciberdelincuencia/

BBC News Mundo. (2017, junio 27). La curiosa historia de cómo nació el cajero automático. https://www.bbc.com/mundo/noticias-40417156

Beermann Hemmerling, Kurt. (2024). la ciberdelincuencia en panamá y el convenio de budapest de 2001: Especial atención al Proyecto de Ley 632 de 2021. Boletín de Ciencias Penales, No. 21, https://facderecho.up.ac.pa/sites/facderecho/files/2023-12/07.%20KURT%20BEEERMANN%20LA%20CIBERDELINCUENCIA%20EN%20PANAMA.%20EL%20CONVENIO%20DE%20BUDAPESTA%2C%20Y%20PROYECTO%20DE%20LEY%20633%20DE%202021.pdf

Benitez, Carlos. (2021, junio 6). Ataque de seguridad informática a SWIFT. Cybers on the Storm. https://cybersonthestorm.com/ataque-de-seguridad-informatica-a-swift/

Brown, Deborah. (2021, Agosto 13). Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights. Human Rights Watch. https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights

Centro Nacional de Control del Gas Natural (2021, octubre 12). Los derechos ARCO. Gobierno de México. https://www.gob.mx/cenagas/acciones-y-programas/los-derechos-arco

Código Civil de la República de Panamá. Ley No. 2 de 1916. 22 de agosto de 1916 (Panamá).

Código Penal de la República de Panamá. Ley No. 14 de 2007. 18 de mayo de 2007 (Panamá).

Consejo de Europa. (2023, abril 19). Adhesión al Convenio sobre la Ciberdelincuencia: Beneficios: Convenio sobre la Ciberdelincuencia. Consejo de Europa. https://rm.coe.int/cyber-buda-benefits-19april2023-es/1680aafa3f

Consejo de Europa. (2023, octubre 7). Chart of signatures and ratifications of Treaty 189. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=189

Consejo de Europa. (2023, octubre 7). Chart of signatures and ratifications of Treaty 224. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224

Constitución Política de la República de Panamá (reformada en 2004). 11 de octubre de 1972 (Panamá).

Contreras Filiciotto, Ángel Gabriel. (2024). La problemática de la competencia y de la protección en la legislación de datos personales: Desafíos y soluciones. Revista Gestión Pública, Edición No. 23, 31-39.

Contreras Filiciotto, Ángel Gabriel. (2025). La ciberdelincuencia dentro del E-Commerce como consecuencia de un mal tratamiento de datos personales (Análisis de dos marcos jurídicos). [Tesis de Maestría, Universitat Oberta de Catalunya].

Convenio de Budapest sobre la Ciberdelincuencia. 23 de noviembre de 2001.

Crespillo Campos, Sergio. (2022). cyber-security framework for banks [Tesis de Licenciatura, Universidad Complutense de Madrid]. https://docta.ucm.es/rest/api/core/bitstreams/131c7064-e1f8-4e38-8c7e-4dd61a3307ae/content

Decreto Ejecutivo No. 285 de 2021. Que reglamenta la Ley No. 81 de 2019 sobre protección de datos personales. Gaceta Oficial No. 29296-A.

Decreto Ejecutivo No. 52 de 2008. Que adopta el texto único del Decreto Ley No. 9 de 26 de febrero de 1998, modificado por el Decreto Ley No. 2 de 22 de febrero de 2008. 30 de abril de 2008. Gaceta Oficial No. 26,035.

Federal Reserve Bank of New York. (2016, Agosto 11). New York Fed Responds to Freedom of Information Request. https://www.newyorkfed.org/newsevents/statements/2016/foia-cbias

Freedom of Information Act (FOIA). 5 U.S.C. § 552 (1966).

GNDiario. (2019, enero 10). Exbanquera filipina condenada a prisión por robo a banco central bangladeshí. https://www.gndiario.com/exbanquera-filipina-condenada-prision-por-robo-banco-central-bangladeshi

Government of United Kingdom. (2022). Solicitud de asistencia jurídica mutua en asuntos penales: Guía para las autoridades externas al Reino Unido. https://assets.publishing.service.gov.uk/media/65256ce8aea2d00013219b1d/MLA_Guidelines_-_Spanish.pdf

Government of United Kingdom. (2024, mayo 2). Request for mutual legal assistance in criminal matters: guidelines for authorities outside of the UK (accessible version). https://www.gov.uk/government/publications/mla-guidelines-for-authorities-outside-of-the-uk/request-for-mutual-legal-assistance-in-criminal-matters-guidelines-for-authorities-outside-of-the-uk-accessible-version

IBM. (2024, agosto 9). Ciberataque. https://www.ibm.com/es-es/topics/cyber-attack

International Organization for Standardization. (2018). ISO/IEC 27000:2018 – Information technology – Security techniques – Information security management systems – Overview and vocabulary.

Ipandetec. (2018, octubre 4). La necesidad de legislar sobre cibercrimen en Panamá. Derechos Digitales. https://www.derechosdigitales.org/12378/la-necesidad-de-legislar-sobre-cibercrimen-en-panama/

Juan, Jordi. (2023, abril 24). La ciberdelincuencia sigue en aumento: los ciberataques se multiplican. EY. https://www.ey.com/es_es/insights/cybersecurity/la-ciberdelicuencia-sigue-aumento-los-ciberataques-se-multiplican

Kabir, Musnun y Hosen, Mosharaf. (2024). A Study of Financial Crimes in the Banking Sector of Bangladesh. International Journal Of Law And Public Policy (IJLAPP), 6(2), 49-57. https://doi.org/10.36079/lamintang.ijlapp-0602.677

Kaium, Tousif. (2025, enero 5). Reserve heist among 10 cases stuck over lack of info from respective countries. The Business Standard. https://www.tbsnews.net/bangladesh/crime/reserve-heist-among-10-cases-stuck-over-lack-info-respective-countries-1035021

Kiener-Manu, Katharina. (2020). Key Issues: Cybercrime in Brief. United Nations Office on Drugs and Crime (UNDOC). https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html

Ley No. 31 de 1996. Que regula las telecomunicaciones en Panamá. 8 de febrero de 1996. Gaceta Oficial No. 22,971.

Ley No. 45 de 2007. Que dicta normas de protección al consumidor y defensa de la competencia y otras disposiciones. 31 de octubre de 2017. Gaceta Oficial No. 25,914.

Ley No. 81 de 2019. Que dicta normas sobre la protección de datos personales. 26 de marzo de 2019. Gaceta Oficial No. 28743-A.

Martins Dos Santos, Bruna. (2022). Convenio de Budapest sobre la Ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México.

Morris, Ciara. (2023, marzo 23). Panamá, el país que recibe más ciberataques a bancos. ECOTV. https://www.ecotvpanama.com/eco-news/programas/panama-el-pais-que-recibe-mas-ciberataques-bancos-n5861594

Naciones Unidas. (s. f.). Declaraciones y Convenciones que figuran en las resoluciones de la Asamblea General. https://www.un.org/spanish/documents/instruments/terminology.html

Nazrul, Islam (2024, febrero 4). BB reserve heist: Liability of 12 central bank officials identified. Prothomalo. https://en.prothomalo.com/bangladesh/crime-and-law/jsv5k1ia4m

Pardo Gato, José Ricardo. (2021). La cultura de la ciberseguridad y la abogacía. Revista de Derecho de la Cultura, número 4.

Racketeer Influenced and Corrupt Organizations Act (RICO). 18 U.S.C. §§ 1961–1968 (1970).

Reglamento General de Protección de Datos (GDPR). 4 de mayo de 2016.

SOLUSOFT. (s. f.). Protección de datos personales en entidades bancarias en Panamá. https://www.solusoft.com/proteccion-de-datos-personales-en-entidades-bancarias-en-panama/

SWIFT. (s. f.). Customer Security Programme (CSP). https://www.swift.com/myswift/customer-security-programme-csp

SWIFT. (s. f.). Swift Customer Security Controls Framework. https://www.swift.com/myswift/customer-security-programme-csp/security-controls

The DPO Centre. (2021, 9 agosto). The Data Protection Act 2018: The 7 principles of the GDPR. https://www.dpocentre.com/the-data-protection-act-2018-the-7-principles-of-the-gdpr/

Unión Internacional de Telecomunicaciones (UIT). (2024). Facts and Figures 2024: Measuring digital development. Unión Internacional de Telecomunicaciones.

Zachar, D. (2021). CCDCOE. Recuperado 29 de noviembre de 2024, de https://ccdcoe.org/library/publications/battling-cybercrime-through-the-new-additional-protocol-to-the-budapest-convention/.

Conflicto de Intereses: Los autores declaran que no tienen conflictos de intereses relacionados con este estudio y que todos los procedimientos seguidos cumplen con los estándares éticos establecidos por la revista. Asimismo, confirman que este trabajo es inédito y no ha sido publicado, ni parcial ni totalmente, en ninguna otra publicación.

CONTRIBUCIÓN DE AUTORÍA

Lourdes C. Jean Pierre Barsallo (LCJPB)

Indicar las funciones desempeñadas por cada autor:

Conceptualización: (LCJPB)

Curación de datos: (LCJPB)

Análisis formal: (LCJPB)

Adquisición de fondos: (LCJPB)

Investigación: (LCJPB)

Metodología: (LCJPB)

Administración del proyecto: (LCJPB)

Recursos: (LCJPB)

Software: (LCJPB)

Supervisión: (LCJPB)

Validación: (LCJPB)

Visualización: (LCJPB)

Redacción – Borrador original: (LCJPB)

Redacción – Revisión y edición: (LCJPB)