PONTIFICIA UNIVERSIDAD
CATÓLICA DEL PERÚ

FACULTAD DE DERECHO

Programa de Segunda Especialidad en Derecho de Protección al Consumidor

¿Me devolverán mi dinero?: Análisis del marco normativo en protección al consumidor del comercio electrónico en el Perú

Trabajo académico para optar el título de Segunda Especialidad en Derecho de Protección al Consumidor

Autor:
Nicole Cristina Velazco Velazco

Asesor:
Armando Rafael Prieto Hormaza

Lima, 2024

Informe de Similitud

Yo, PRIETO HORMAZA, ARMANDO RAFAEL, docente de la Facultad de Derecho de la Pontificia Universidad Católica del Perú, asesor(a) del Trabajo Académico titulado "¿Me devolverán mi dinero?: Análisis del marco normativo en protección al consumidor del comercio electrónico en el Perú", del autor(a) VELAZCO VELAZCO, NICOLE CRISTINA, dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 23%. Así lo consigna el reporte de similitud emitido por el software Turnitin el 09/12/2024.

- He revisado con detalle dicho reporte y el Trabajo Académico, y no se advierten indicios de plagio.

- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lima, 12 de diciembre del 2024

PRIETO HORMAZA, ARMANDO RAFAEL	
DNI: 20054321	Firma: 
ORCID: https://orcid.org/0000-0003-3084-6149	

RESUMEN

El presente artículo buscará evidenciar cómo se encuentra regulado el comercio electrónico en nuestro país y, particularmente, analizará el caso de las medidas de seguridad incorporadas por las instituciones financieras con la finalidad de garantizar una validación de todas las transacciones realizadas por los consumidores. En ese escenario, hemos podido identificar que las operaciones no reconocidas terminan siendo consecuencias frecuentes de la falta de implementación adecuada de estas medidas.

En primer lugar, se abordará cuál es la regulación de las operaciones en el marco del comercio electrónico en el Perú y cómo viene adaptándose a los avances tecnológicos. En segundo lugar, abordaremos como esta regulación viene siendo implementada por las instituciones financieras para lo cual se analizará cuáles son las medidas de seguridad impuestas por la normativa sectorial para los casos de operaciones a través de canales digitales. De igual manera, presentaremos como viene desarrollándose la regulación sobre las operaciones fraudulentas en la legislación comparada. En tercer lugar, buscaremos identificar cómo la regulación existente tiene un rol importante en la predictibilidad de las resoluciones del Instituto Nacional de Defensa de la Competencia y Propiedad Intelectual (en adelante, el Indecopi) y explicaremos los cambios de criterio de la autoridad al momento de resolver los casos de operaciones no reconocidas.

Mediante este artículo podremos concluir que, si bien la regulación peruana sobre comercio electrónico buscará proteger a los consumidores, el avance tecnológico y el crecimiento de riesgos cibernéticos es más célere. En esa línea, uno de los principales problemas podría encontrarse en la implementación de estas medidas realizadas por las instituciones financieras que, a pesar de estar obligadas a cumplir con la normativa sectorial vigente, suelen no implementar todas las medidas de seguridad exigidas, generando un perjuicio a los consumidores. Asimismo, los cambios de criterio del Indecopi en la interpretación de la normativa aplicable a los casos de operaciones no reconocidas han afectado la predictibilidad y seguridad jurídica de sus resoluciones.

Palabras clave

Medidas de seguridad, comercio electrónico, instituciones financieras, consumos no reconocidos, predictibilidad

ABSTRACT

The purpose of this article is to show how e-commerce is regulated in our country and, in particular, to analyse the case of the security measures implemented by financial institutions to guarantee the validation of all transactions carried out by consumers. In this scenario, we have been able to see that unrecognised transactions are often the result of the lack of adequate implementation of these measures.

Firstly, we will discuss the regulation of e-commerce transactions in Peru and how it is adapting to technological advances. Secondly, we will discuss how this regulation is implemented by financial institutions, providing an overview of the security measures required by sectoral regulations for transactions through digital channels. We will also show how the regulation is developing in comparative law. Finally, we will try to identify how the existing regulation plays an important role in the predictability of the decisions of the National Institute for the Defence of Competition and Intellectual Property (hereafter Indecopi), and we will explain the changes in the authority's criteria when resolving cases of unrecognised transactions.

From this article, we will be able to conclude that although Peruvian e-commerce regulation aims to protect consumers, the speed of technological progress and the growth of cyber risks are greater. In this regard, one of the main problems is that financial institutions, although obliged to comply with the sectoral regulations in force, often fail to implement all the necessary security measures, to the detriment of consumers. Similarly, the changes made by Indecopi to the interpretation of the rules applicable to cases of unrecognised transactions have affected the predictability and legal certainty of its decisions.

Keywords

security measures, electronic commerce, financial institutions, unrecognised transactions, predictability

ÍNDICE

INTRODUCCIÓN

El comercio electrónico se encuentra regulado en diferentes cuerpos normativos, estas disposiciones fueron previstas para brindar protección a todos los usuarios que buscan realizar sus compras y adquisiciones de productos y/o servicios mediante canales digitales. En ese escenario, el avance de la tecnología y el crecimiento de los riesgos cibernéticos pone a la palestra una problemática para los usuarios de estas modalidades de compras.

El Indecopi, a través de sus resoluciones, ha buscado aplicar la normativa sectorial vigente e interpretarla en los casos de operaciones que los consumidores señalan no haber realizado y/o que fueron realizadas por un tercero ajeno al titular de la tarjeta sin consentimiento al respecto. Estas transacciones suelen ser conocidas como “operaciones no reconocidas”, pues el titular de una tarjeta sea de crédito o débito, desconoce haber autorizado dicha transacción u operación controvertida.

A fin de brindar un análisis más completo al respecto, utilizaremos las resoluciones emitidas por el Indecopi los últimos 5 años, con lo cual determinaremos cómo vienen resolviéndose estos casos por la autoridad de protección al consumidor y qué factores son los que se toman en cuenta para declarar fundada o infundada una denuncia presentada por un consumidor al respecto.

El análisis realizado en el presente artículo es relevante debido a que nos muestra un escenario de cómo vienen conviviendo los avances de la tecnología y la regulación sobre la materia. Nos permite analizar el marco legal del comercio electrónico, evaluando si se actualiza con la celeridad necesaria para acompañar el avance tecnológico. Además, se examinan las medidas implementadas por las instituciones financieras y la forma en que el Indecopi ha gestionado denuncias relacionadas con operaciones no reconocidas. De igual manera, se presentan los enfoques adoptados por otros países y el análisis de la predictibilidad basado en los pronunciamientos del Indecopi.

SECCIÓN I: ¿La normativa sobre comercio electrónico se actualiza con suficiente celeridad para adaptarse a los avances tecnológicos?

En la presente sección, analizaremos cuál es la normativa actual para realizar operaciones en el marco del comercio electrónico y, de igual manera, evaluaremos si la normativa sobre comercio electrónico se actualiza con la suficiente celeridad para atender a los avances tecnológicos.

En la actualidad, las controversias suscitadas en el ámbito del comercio electrónico han ido en aumento a nivel global. Esta situación se acrecentó con lo ocurrido durante la pandemia, debido a que cada gobierno ordenaba realizar el aislamiento obligatorio de sus habitantes, conforme fuera necesario, razón por la cual las compras a través de plataformas tecnologías y canales digitales aumentó de manera exponencial. El Perú no fue ajeno a dicha situación, por ello, en aras de garantizar la protección al consumidor en la nueva realidad en la que nos encontrábamos viviendo, la normativa establecida para el comercio electrónico se fue modificando, incluyendo nuevos supuestos e implementando mayores medidas de seguridad. No obstante, ello fue un proceso de larga duración y que, hasta la actualidad, continúa modificándose.

Cabe precisar que, con la finalidad de atender estos avances de las nuevas tecnologías, en el año 2021, el Indecopi presentó una propuesta para regular el comercio electrónico, garantizar la seguridad y protección de los consumidores en las transacciones en línea. En la propuesta se buscaba establecer disposiciones normativas que favorezcan la celebración de contratos de consumo mediante canales digitales, otorga derechos a los administrados y recogía las recomendaciones brindadas por la Organización para la Cooperación y Desarrollo Económico (en adelante, OCDE) y la Organización Mundial del Comercio (OMC).

Asimismo, el congresista José Luna Gálvez presentó el Proyecto de Ley 415/2021-CR, en el cual proponía la modificación del Código de Protección y Defensa del Consumidor (en adelante, el Código), buscando incluir regulaciones adicionales para proteger al consumidor como crear una ventanilla de atención para la prevención de fraudes informáticos, permitirle al consumidor poner fin al contrato de manera unilateral, entre otros. No obstante, hasta la fecha, ambas propuestas continúan siendo evaluadas por el Congreso.

1.1¿Cuál es la normativa actual para operaciones realizadas por comercio electrónico?

En principio, cabe precisar que nuestro ordenamiento no ha establecido una normativa propia que compile toda la regulación para el comercio electrónico, como sí se ha presentado en otros países como Estados Unidos con la Uniform Electronic Transactions Act, la Directiva de Comercio Electrónico de la Unión Europea, la Ley de Comercio Electrónico de China. En Latinoamérica, los países han optado por incorporar dentro de sus normativas aplicables para la protección al consumidor normas específicas o sectorizadas que regulen las transacciones y el comercio electrónico propiamente, asimismo, cuentan con normas de protección de datos personales, firmas digitales, entre otras.

En el Perú, el comercio electrónico se encuentra regulado a través de diversas normativas expedidas por el legislador como, por ejemplo, el Código, el cual contiene normas y principios orientados para proteger los derechos y establecer obligaciones para los consumidores y los proveedores de bienes y servicios; el Reglamento de Tarjetas de Crédito y Débito (en adelante, Reglamento de Tarjetas), el cual determina el uso de tarjetas en las operaciones y gestiones comerciales y, adicionalmente, establece las medidas de seguridad que deben ser incorporadas por las entidades de operaciones múltiples para el uso de tarjetas (presente y no presente); y, el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad (en adelante, Reglamento de Ciberseguridad), el cual señala las medidas de ciberseguridad que deben implementar las empresas que tengan presencia en el ciberespacio, entre otros.

En el presente artículo, nos centraremos en el análisis de la normativa aplicable a las operaciones realizadas por los consumidores a través del comercio electrónico, es decir, mencionaremos las principales obligaciones y derechos que tienen los proveedores y consumidores en este ámbito y explicaremos las disposiciones más relevantes al momento de regular las operaciones realizadas en línea.

Como parte del contexto, debemos tener en cuenta que el artículo 65 de nuestra Constitución establece, como deber estatal, velar y defender los intereses de los consumidores en el mercado, reconociendo así la necesidad de garantizar la protección a los consumidores en los distintos sectores, por ejemplo, garantizando la implementación de medidas mínimas requeridas de protección y seguridad para el uso de sus tarjetas.

Primero, el Código, el cual fue publicado bajo la Ley Nº 29571 en el 2010, nos brinda los lineamientos para entender los supuestos en los cuales nos encontramos dentro de

una relación de consumo. Asimismo, busca garantizar que los consumidores tengan acceso a productos y servicios idóneos y que tengan a su disposición los derechos y mecanismos efectivos para su protección. Esto incluye, también, la reducción de la asimetría de información y la corrección, prevención o eliminación de conductas y prácticas que puedan perjudicar sus intereses legítimos.

En esa línea, el artículo III del Título Preliminar del Código precisa que su ámbito aplica a aquellas situaciones en las que se establezca, ya sea de manera indirecta o directa, una relación de consumo entre proveedores y consumidores, abarcando incluso la fase precontractual (anterior a su formalización), celebrada o llevada a cabo dentro del territorio nacional. Conforme lo señalado por Tirado, la relación de consumo surge cuando la oferta presentada por una parte (el proveedor) es aceptada, recibida, o al menos puesta en conocimiento de la otra parte (el consumidor). Esto crea de manera inmediata un vínculo jurídico, que puede implicar derechos y obligaciones para ambas partes (2021, p.50).

Asimismo, el Código nos permite entender a las partes que constituyen una relación de consumo, la cual se compone de la concurrencia de tres elementos: el consumidor, el proveedor y un bien o servicio objeto de transacción económica. Se define a un consumidor como aquella persona natural o jurídica que, como destinatario final, adquiere, utiliza o disfruta productos o servicios, siempre que ello no guarde relación con su actividad profesional o empresarial. De igual modo, se define como proveedor a quienes, de manera habitual, se dedican a fabricar, elaborar, manipular, acondicionar o prestar servicios de cualquier tipo de naturaleza a los consumidores.

En palabras de Tirado, la relación de consumo se genera cuando dos partes, que ocupan posiciones distintas dentro de un proceso productivo, crean un vínculo entre sí, generando una relación jurídica. Este vínculo surge cuando la oferta presentada por un proveedor es aceptada, recibida o, al menos expuesta ante el consumidor, lo cual produce un intercambio de productos y/o servicios a cambio de una contraprestación. De esta manera, se genera de inmediato una relación jurídica que conlleva derechos y obligaciones para ambas partes (2021, p.50).

Cabe precisar que el Código en su artículo 1, establece los derechos de los consumidores, entre los cuales está el acceso a una información oportuna, veraz, suficiente y fácilmente accesible, que sea relevante para tomar una decisión adecuada de consumo y en idioma castellano. Asimismo, se encuentra el derecho a elegir

libremente entre productos y servicios idóneos que sean ofrecidos en el mercado; a la reparación o reposición del producto; a un trato justo y equitativo en la transacción comercial; entre otros. A su vez, también se encuentran las obligaciones mínimas que debe ofrecer el proveedor cuando decide brindar un producto o servicio al mercado, siendo que tiene el deber de brindar la información relevante, en las condiciones descritas anteriormente; garantizar la idoneidad de los productos y/o servicios que ofrece a los consumidores; cumplir con su deber general de seguridad; entre otros.

El sector financiero se caracteriza por ser complejo y especializado, con características particulares, las cuales no necesariamente son conocidas o entendidas por un consumidor, por ello, la protección al consumidor financiero es clave para garantizar el cumplimiento de los derechos de los consumidores dentro de este sector, en el cual la asimetría informativa entre las partes se acrecienta (Álvarez, 2017, p.12). Es importante señalar la relevancia de regulación en este sector, sobre todo, en el comercio electrónico. Por ello, el Código desempeña una función importante al contar con disposiciones que permiten que los consumidores se encuentren en un entorno seguro al realizar el pago de sus productos o servicios a través de las diversas herramientas que existen en el mundo digital, exigiendo a los proveedores cumplir con un nivel de protección e información mínima.

De esta manera, podemos ver que la regulación respecto a la formación de una relación de consumo, los derechos que tiene el consumidor, así como las obligaciones de los proveedores, se encuentran plenamente establecidas en el Código. En el caso del comercio electrónico, la regulación no cambia, pues lo único que cambia es el entorno en cual se desarrolla esta relación consumidor-proveedor, debido a que se desplaza de la presencialidad a los medios digitales en el ciberespacio. En este escenario, la contraprestación brindada por el producto o servicio en cuestión se traslada a ese mismo espacio, razón por la cual el uso de tarjetas en plataformas digitales va en aumento y, a este crecimiento, se le suma la incursión de las billeteras digitales.

Ante ello, resulta pertinente mencionar al Reglamento de Tarjetas de Crédito y Débito, el cual, como señalamos, nos plantea el uso adecuado de tarjetas, las medidas de seguridad que les son aplicables, las obligaciones que deben adoptar las empresas de operaciones múltiples, entre otros. Este reglamento, emitido por la Superintendencia de Banca y Seguros (SBS) en el año 2013, tenía como objetivo regular las condiciones aplicables y establecer límites de responsabilidad para el uso óptimo de las tarjetas.

El mencionado reglamento presenta algunas disposiciones que son aplicables en el marco del comercio electrónico. Como señalamos anteriormente, el Código se encarga de regular las relaciones de consumo, las cuales se generan con la participación de los actores mencionados (consumidor y proveedor). En el intercambio de productos y/o servicios que se producen dentro la relación de consumo, es requerido el pago de una contraprestación, razón por la cual, entra a la palestra el uso de tarjetas para realizar los pagos en línea.

Las tarjetas son medios de pago que pueden tener forma física o una representación electrónica o digital, asimismo, estas se clasifican en tarjetas de crédito, es decir, aquel instrumento de pago vinculado a una línea de crédito, que cuenta con un límite determinado y otorgado por la entidad emisora; y, de débito, definidas como aquellos instrumentos de pago que permite realizar transacciones con cargo a fondos previamente constituidos, conforme lo establecido en el contrato. En esa línea, el reglamento define el canal como cualquier medio físico o virtual al que tiene acceso el usuario para poder realizar sus operaciones, sea de banca por internet, cajeros automáticos, plataformas digitales, puntos de venta, entre otros.

El mencionado reglamento reconoce como parte de los servicios adicionales asociados a las tarjetas, tanto de crédito, en su artículo 7, como de débito, en su artículo 13, las operaciones realizadas a través de internet, lo cual incluye páginas web y/o aplicaciones de dispositivos móviles, dejando abierta la posibilidad a los nuevos mecanismos provistos por las entidades financieras. Para garantizar la adquisición de estos servicios, los proveedores tienen la obligación de informar a los usuarios las condiciones aplicables y los riesgos asociados que conlleva su uso, así como, las medidas de seguridad que deben ser adoptadas con la finalidad de resguardar el uso personal de las tarjetas. Por ello, este servicio adicional debe ser incorporado solo previo consentimiento del titular.

En esa línea, como parte de las medidas de seguridad que deben adoptar las entidades financieras, el artículo 16 numeral 4 establece que la totalidad de operaciones que sean cargadas a las tarjetas, sean operaciones realizadas con de manera física o electrónica, deben ser notificadas al titular mediante algún mecanismo de comunicación inmediata pactada previamente (mensaje de texto, correo electrónico, llamadas, entre otros). Este artículo es relevante, debido a que permite que cualquier operación que se cargue a nuestras tarjetas será notificada al titular, reduciendo el riesgo de operaciones no reconocidas o fraudulentas, pues ante dicha alerta el titular podrá tomar acciones

inmediatas y pertinentes para evitar que se siga produciendo su detrimento patrimonial. Asimismo, el artículo 15 numeral 4, establece que, si se utiliza un soporte distinto al físico, deben asegurarse los mecanismos de autenticación y evitar exponer los datos de la tarjeta.

Por su parte, el numeral 7.2 del artículo 7 del citado cuerpo normativo determina que para las operaciones con tarjeta no presente se requieren dos factores, siendo el primero los datos contenidos en la tarjeta y, el segundo, un código de verificación dinámico de la tarjeta u otro factor verificable en línea. Asimismo, el numeral 7.3 establece que para operaciones con billeteras móviles de terceros basadas en *tokenización* de tarjetas y un segundo factor de naturaleza distinta. Cabe precisar que las billeteras móviles o digitales son aquellos medios de pago basados en una aplicación móvil que permite realizar operaciones por cuantías menores sin necesidad de contar con una tarjeta asociada a una cuenta de ahorros. Suele ser considerado como sustituto de billetes y monedas, y, cuenta con métodos de seguridad para su acceso (Ramos, 2022, p.88).

Adicionalmente, el artículo 17 del reglamento exige a todas las entidades financieras que incorporen un sistema de monitoreo que permita detectar operaciones que sean inusuales en la actividad de consumo habitual de los usuarios y, con eso, generar una alerta inmediata a fin de evitar el daño a las cuentas de los consumidores. El mencionado reglamento también establece como responsabilidad de las empresas demostrar que las operaciones fueron debidamente autenticadas y registradas, estableciendo supuestos de exclusión de responsabilidad por parte del usuario en el caso de operaciones no reconocidas.

Otro reglamento que resulta de relevante en el marco del comercio electrónico es el Reglamento de Ciberseguridad, emitido por la SBS y publicado en el año 2021. Este reglamento definió la ciberseguridad como aquella protección de los activos de información a través de la prevención, detección, respuesta, y recuperación ante incidentes que puedan comprometer su disponibilidad, confidencialidad o integridad en el entorno cibernético. Este entorno se caracteriza por ser un sistema complejo sin una existencia física concreta, en el cual interactúan personas, dispositivos y sistemas informáticos. El ciberespacio va más allá de la definición de internet, pues no se limita al hardware, software y sistemas de intercambio de datos, sino que, además de los citados elementos, incorpora la posibilidad de una interacción social compleja entre

cibersujetos (personas y organizaciones) dentro del entorno interconectado (Santana-Soriano & Báez, 2022).

Al momento de realizar compras a través de internet, el consumidor y/o usuario ingresa a este entorno en el cual requiere compartir información personal y respecto al uso de sus mecanismos de pago, por esta razón, la ciberseguridad cobra gran importancia para el comercio electrónico, pues permite que a través de mecanismos idóneos la información compartida se encuentre más protegida y se requieran mayores métodos de autenticación para validar las operaciones que se puedan cargar a las tarjetas.

De esta manera, el Reglamento de Ciberseguridad incorporó detalles respecto a la implementación de los mecanismos y/o procesos de autenticación, enrolamiento y la autenticación reforzada, necesarios para acceder a los servicios por canales digitales y realizar operaciones. El artículo 19 del mencionado reglamento señala que el objetivo de contar con una autenticación reforzada para realizar operaciones por canales digitales radica en disminuir el riesgo de operaciones fraudulentas o cualquier abuso del servicio que pueda perjudicar a los usuarios. Para lograr una autenticación reforzada se requiere: a) emplear una combinación de factores de autenticación que pertenezcan a dos categorías distintas y que no dependan entre sí; b) implementar controles contra ataques en el medio, que puede incluir un código único generado bajo métodos criptográficos; y, que c) una vez realizada la operación, esta sea notificada de manera inmediata al usuario.

A fin de garantizar que las empresas cumplan con la autenticación reforzada, el numeral 3 del artículo 20, modificado recientemente, señala que las empresas serán responsables de las pérdidas por las operaciones no reconocidas por efectuadas por los clientes a través del canal digital, si no cumplen con este método de autenticación reforzada. En otras palabras, ahora son las empresas las que tienen la responsabilidad de demostrar que cumplieron con el mecanismo estipulado por el reglamento, considerando que poseen la información necesaria y disponible. De lo contrario, serán señaladas como responsables de manera automática. Conforme se analizará en el siguiente apartado, esta reciente modificación aún está en proceso de adecuación.

En ese sentido, en el marco del comercio electrónico, la autenticación reforzada se ha convertido en determinante para evaluar la responsabilidad del proveedor, pues se encuentra obligado a incorporar dicho mecanismo para garantizar la protección del usuario en el ciberespacio al momento de hacer sus compras y/o adquisiciones.

Como mencionamos al inicio del presente acápite, al generalizarse el uso del comercio electrónico, nos vemos en la necesidad de prestar atención a las transacciones que se realizan en el entorno digital. Algunos ejemplos de esto es la regulación e implementación medidas de seguridad en el ciberespacio, así como las propuestas orientadas a desarrollar una regulación específica para este entorno.

1.2 ¿Cómo se ha ido adaptando la normativa a los avances tecnológicos?

En este apartado, nos pronunciaremos respecto a los cambios más significativos que han ocurrido en la normativa señalada anteriormente que se relacionen a los avances de la tecnología, es decir, estas modificaciones e inclusiones que surgen a raíz del incremento de uso de las nuevas tecnologías y esta necesidad de contar con mayor protección en el ciberespacio.

Código de Protección y Defensa del Consumidor

El Código ha tenido diversos cambios desde su publicación oficial en el año 2010, sin embargo, en lo relacionado a las nuevas tecnologías todavía estamos en proceso. Conforme señalamos anteriormente, el Código se centra en la protección de la relación de consumo, siendo que las modificaciones hasta la actualidad vienen incluyendo ese propósito.

El 28 de julio de 2022, bajo la Ley N°31537, se modificó el artículo 47 del Código, relacionado a la protección mínima del contrato de consumo, dejando como regla que los proveedores tenían lo obligación de proporcionar a los usuarios, en un plazo máximo de quince (15) días, las copias de los contratos y demás documentación relacionada. Asimismo, establecía en su literal f) que en caso se haya realizado una contratación por canales digitales o vía telefónica, el proveedor debería acreditar fehacientemente que la información mínima fue puesta oportunamente a disposición del consumidor y se produjo la respectiva aceptación.

Esa modificación impone a los proveedores el deber de informar con todos los documentos relacionados al consumidor sobre el producto y/o servicio adquirido, como, por ejemplo, lo sería adquirir la tarjeta. Ello, resulta relevante pues en dichos documentos se advierte la posibilidad de realizar las compras en línea con la tarjeta y de poder establecer condiciones para realizarlo, así como las medidas de seguridad que deben adoptar los usuarios.

Asimismo, el 4 de junio de 2023, la Ley N° 31763, buscaba uniformizar los plazos de atención de reclamos en los sectores del sistema financiero y de seguros, de esta manera, se redujo un plazo de treinta (30) días calendario a quince (15) días hábiles, recalcando que puede haber una ampliación de manera excepcional si se cumple con las condiciones requeridas por la SBS. Con ello, vemos que los consumidores tendrán una atención más rápida a sus reclamos, con lo cual podrán adoptar las medidas pertinentes en caso obtengan una respuesta desfavorable.

En ese contexto, observamos que los cambios mencionados, junto con las reformas que brindan más recursos para el ejercicio de los derechos, han favorecido la protección del consumidor. Si bien se han incorporado algunos supuestos a distancia o bajo modalidades digitales, estos se han dirigido más a una inclusión de posibilidades de uso de las nuevas tecnologías que a establecer reglas o parámetros que ofrezcan protección en esos entornos.

Reglamento de Tarjetas de Crédito y Débito (Reglamento de Tarjetas)

Por su parte, desde el año 2013 hasta la actualidad, el Reglamento de Tarjetas ha tenido gran cantidad de modificaciones y, también, ha incluido algunas modificaciones e incorporado supuestos sobre el uso de las nuevas tecnologías. Además de las condiciones para ofrecer y otorgar tarjetas, este reglamento establece las obligaciones que deben adoptar las entidades financieras respecto a sus sistemas operativos y las medidas de seguridad mínimas que deben implementar para garantizar una adecuada protección a los consumidores.

Como, por ejemplo, antes el reglamento establecía como regla general que los estados de cuenta podían ser entregados a través de 2 mecanismos como la entrega física y el uso de medios electrónicos. Bajo la Resolución SBS N°1278-2020, se estableció que las empresas deben enviar como mínimo, mensualmente, a través de medios electrónicos el estado de cuenta, siendo que ahora es una facultad del cliente solicitar que se entregue por medios físicos. Considero que este cambio se debe al hecho de que, en la actualidad, el uso de los medios digitales permite tener un contacto directo e inmediato con el cliente, puesto que, apenas emitido el estado de cuenta, este puede llegar a conocimiento del consumidor en cuestión de segundos, situación que no ocurre cuando se debe programar una entrega física.

Otro de los cambios relevantes en el reglamento es el hecho de que, bajo Resolución SBS N° 5570-2019 del 28 de noviembre del 2019[1], se incluyó y enfatizó la importancia

[1] Posteriormente modificada por la N° 1278-2020 que amplió el plazo de adecuación establecido en la primera Resolución.

de que el titular de la tarjeta pueda habilitar y deshabilitar los servicios adicionales de manera inmediata y sin mayor complicación, cuantas veces considere necesario, permitiendo así que sea el usuario quien tiene la facultad de decidir cuándo y en qué momento puede activar su servicio de compras por internet o en el extranjero. En caso este servicio no haya sido activado por el titular, no se puede procesar ninguna operación por internet o en el exterior. Los proveedores deben acreditar que el titular brindó su consentimiento informado para activar este servicio.

De igual manera, parte de los cambios relevantes se encuentra en la incorporación de medidas de seguridad. En particular, respecto al artículo 16 numeral 4 relacionado a las notificaciones ante cualquier operación cargada a la cuenta; el mejoramiento y rigurosidad en los procesos de autenticación, las acciones a adoptar ante una operación posiblemente fraudulenta, entre otras.

Una de las últimas modificaciones a este reglamento vino con la Resolución SBS N° 02286-2024 del 28 de junio de 2024, mediante la cual se buscaba atender el actual funcionamiento de los productos y servicios de las empresas de los sistemas financieros y el impacto del uso de las nuevas tecnologías. Estos cambios incluían procesos de autenticación del usuario, con lo cual las empresas deben poner a disposición de los consumidores mecanismos únicos y dinámicos de identificación, generados mediante técnicas criptográficas y, adicionalmente, emplear un segundo factor de autenticación (independiente del primero).

Uno de los cambios que, si bien ya fueron incorporados al reglamento, se encuentran en un periodo de adecuación hasta el 1 de julio del 2025, es respecto a la responsabilidad de los proveedores ante una operación no reconocida. Esta nueva modificación que, a la fecha de la redacción de este artículo, todavía no es exigible para las empresas, señala que serán responsables de las pérdidas producidas por las operaciones no reconocidas, salvo que acrediten la responsabilidad del usuario, en ese sentido, podemos ver que se ha producido un traslado expreso de responsabilidad a los proveedores y se ha invertido la carga de la prueba, puesto que ahora deberán acreditar que el usuario fue responsable de dicha operación, caso contrario, asumirán la totalidad de la pérdida.

Personalmente, considero que, una vez terminado el proceso de adecuación, este cambio será muy significativo debido a que el sistema financiero y bancario suele ser el más sancionado, siendo que las operaciones no reconocidas encabezan la lista de las

razones de los reclamos y/o denuncias[2]. En ese sentido, los proveedores implementarán todas las medidas de seguridad mínimas requeridas y buscarán mejorar sus sistemas de ciberseguridad a fin de garantizar que se utilicen los métodos adecuados al momento de cargar una operación a las cuentas personales de los usuarios. Caso contrario, además de incumplir con el artículo 17 del reglamento, también serán responsables por los daños patrimoniales que se produzcan al usuario. Ello permitiría reducir el nivel de riesgo de operaciones no reconocidas o fraudulentas realizadas por terceros ajenos al titular de la tarjeta.

Reglamento de Ciberseguridad

Por último, este reglamento surgió a raíz del avance de las nuevas tecnologías en el año 2021, pues el legislador pudo notar que nos estábamos enfrentando a un entorno digital del cual no había mucho conocimiento ni requerimientos mínimos de seguridad, es así como entra a la palestra la ciberseguridad. La ciberseguridad es definida por el propio reglamento como aquella protección de activos de información a través de la prevención, detección, respuesta y recuperación ante eventos que dañen su integridad en el ciberespacio. Siendo de obligatorio cumplimiento para todas las entidades financieras establecidas en su artículo 4.

Cabe precisar que, por parte de la doctrina, la ciberseguridad ha sido abordada desde un punto de vista de la seguridad colectiva, considerando la necesidad de cooperación internacional. Esto se debe a que se puede generar un problema de trazabilidad de la actividad cibernética, puesto que podría atravesar distintas jurisdicciones nacionales y problemas de identificación de los responsables al haber anonimato en la red (Segura, 2017, p.292).

En ese sentido, resulta fundamental considerar que la ciberseguridad, no solo implica una cuestión de seguridad técnica, sino también un enfoque de seguridad colectiva. Esto cobra relevancia especialmente en el uso de medios de pago como tarjetas para el desarrollo de comercio electrónico a través de canales digitales, pues estos deben enfrentar los desafíos que plantea la trazabilidad de las actividades cibernéticas y la protección de los usuarios ante los riesgos emergentes.

En ese contexto, este reglamento detalla cuáles son estos mecanismos de autenticación y autenticación reforzada que se mencionan en el Reglamento de Tarjetas. Estos mecanismos deben poder controlar el acceso a los servicios brindados a los usuarios por canales digitales, para lo cual deberán evaluar la tecnología utilizada para su

[2] Portal “Mira a quién le compras” – INDECOPI. Recuperado de https://enlinea.indecopi.gob.pe/miraaquienlecompras/#/ranking-sector

implementación de manera constante a fin de descubrir los nuevos riesgos que pueden aparecer. Asimismo, en su artículo 17 señala que se debe proteger todos los registros de lo actuado en cada enrolamiento del usuario, intento de autenticación y cada operación que este puede realizar, de igual manera, se debe implementar el monitoreo de transacción para reducir las operaciones fraudulentas.

Por su parte, el enrolamiento (Artículo 18) permite identificar al usuario de manera particular y poder reducir la posibilidad de supuestos de suplantación de identidad, incluyendo el uso de factores biométricos y factores independientes de autenticación. En esa línea, la autenticación reforzada (Artículo 19) exige que todas las empresas implementen una combinación de factores de autenticación, incluyendo un control como un código de uso único por métodos criptográficos y la notificación al usuario. Se encuentran exentas de este requisito las operaciones en línea realizadas de manera periódica a un beneficiado registrado permanente o cuando el beneficiado es el mismo cliente; así como las operaciones con un nivel de riesgo de fraude bajo.

Otra de las implementaciones necesarias para el uso de las nuevas tecnologías se encuentra en el artículo 21 del reglamento. Dicho artículo indica que las empresas deben contar con el uso de interfaces de programación de aplicaciones, para lo cual deben tomar en cuenta los estándares y marcos internacionales.

En ese sentido, hemos visto que ha habido un cambio normativo significativo en nuestro país, que busca adaptarse a la realidad en la que nos encontramos y los avances de la tecnología. No obstante, la regulación todavía se encuentra en desarrollo y en periodo de implementación con lo cual muchas de las disposiciones normativas si bien se encuentran en vigencia, todavía no son de obligatorio cumplimiento. Nuestro ordenamiento ahora refleja el uso de una autenticación reforzada para canales digitales, un crecimiento en la seguridad de la información en el ciberespacio, mayor rigurosidad en la adopción de medidas y sistemas de las entidades financieras, sin embargo, cabe precisar que ello obedece a modificaciones ocurridas durante y posteriores a la pandemia, puesto que años anteriores no habría habido cambios relevantes en esta materia.

El Código resulta ser aplicable y complementado por la normativa sectorial, no obstante, en el caso del Reglamento de Tarjetas, este no ha tenido tantos cambios entre el periodo del 2013 y 2019. A partir del 2019, los cambios fueron incrementándose. Como mencioné anteriormente, considero que, en la actualidad, si bien nos estamos acercando a una protección integral y acorde a los riegos cibernéticos, una de las principales complicaciones que se pueden observar es lo largo de los periodos de

adecuación que existen, inicialmente se plantea el periodo de seis (6) meses o un (1) año y, finalmente, termina siendo extendido por una nueva resolución por seis (6) u ocho (8) meses más. Es decir, durante un periodo de más de un (1) año que se emite la disposición, está recién es obligatoria de manera posterior, lo que ocasiona que, durante ese periodo, se siga contando con un nivel de menor protección para los consumidores y menor exigencia para las entidades financieras.

Desde el 2019, en países latinoamericanos como México, Chile y Argentina, y desde el 2015 en la Unión Europea y Estados Unidos aproximada[3], los proveedores son responsables por el detrimento patrimonial de las operaciones no reconocidas, salvo prueben la responsabilidad del usuario. Este claro ejemplo refleja el significativo atraso en el que nos encontramos, lo cual es preocupante, ya que las nuevas tecnologías y los riesgos cibernéticos evolucionan constantemente.

Mientras otras jurisdicciones están adoptando normativas más estrictas para hacer frente a las amenazas emergentes, obligando a las empresas a adoptar mayores medidas de seguridad, protegiendo de manera efectiva al consumidor y trasladando la carga de la prueba a quién se encuentra en mejor posición de afrontarla, nuestra legislación sigue rezagada, exponiendo a los consumidores a riesgos crecientes sin el respaldo de un marco legal adecuado.

En el Perú, podemos ver que hay modificaciones que hoy en día todavía se encuentran en periodo de adecuación hasta mediados del 2025. Sin embargo, nada garantiza que ese plazo brindado no se pueda expandir hasta finales del 2025 o inicios del 2026, con lo cual, la nueva disposición de responsabilidad de los proveedores, en la que se invierte la carga de la prueba y son ellos los encargados de acreditar la responsabilidad del usuario en el caso de operaciones no reconocidas, seguirá en espera. Hasta la fecha, se ha ido superando esta postergación regulatoria con algunas decisiones del Indecopi a través de sus resoluciones.

Si bien las regulaciones suelen tener procesos largos de desarrollo y aprobación, esta situación puede generar un desfase entre la implementación de las normas y la realidad tecnológica del momento en el cual son efectivamente aplicables, más aún, considerando la celeridad con la que evoluciona la tecnología y la constante aparición de nuevas amenazas en el ámbito digital. En otras palabras, aunque una regulación haya sido diseñada para abordar los problemas actuales, cuando finalmente se haga efectiva, la tecnología podría haber avanzado, dejando obsoleta la regulación y, en

[3] Datos extraídos de las respectivas normativas de los países citados.

consecuencia, a las empresas y usuarios desprotegidos frente a nuevas vulnerabilidades.

Particularmente, considero que un punto de inicio para mejorar dicha situación lo encontraríamos estableciendo disposiciones dinámicas que se adapten a los avances tecnológicos como la inteligencia artificial, big data, blockchain, entre otros. De esta manera, se fomentaría la protección ante riesgos informáticos. También, deberían considerarse las regulaciones propuestas y aplicadas en el plano internacional, de igual manera, una alternativa de solución radicaría en proponer plazos de adecuación razonables, fiscalizando que cada uno de los actores cumpla con implementar las medidas de seguridad necesarias, evitando extender los plazos de adecuación propuestos originalmente. Asimismo, resulta importante seguir trabajando en la educación a los consumidores, siendo que la SBS podría liderar campañas para conocer los riesgos del ciberespacio, así como el correcto uso y protección de cuentas bancarias.

A lo largo de este acápite, hemos podido llegar a las siguientes conclusiones:

- El comercio electrónico en el Perú se encuentra regulado en diferente normativa, principalmente, en la que protege directamente a las partes de la relación jurídica (Código de Consumo), la relacionada a los medios de pago (Reglamento de Tarjetas) y respecto a la protección en el ciberespacio (Reglamento de Ciberseguridad). Toda esta normativa busca proteger a los consumidores que realizan compras a través de canales digitales y plataformas web.

- Si bien hubo cambios, inclusiones y modificaciones desde la promulgación de las normas citadas, estos han ido sumándose con el tiempo y cuentan con un largo periodo de adecuación, lo cual genera que sea más lenta la adaptación a las nuevas tecnologías y los riesgos que conllevan, dejando una ventana de tiempo más amplia en la que los consumidores se encuentran expuestos.

SECCIÓN II: ¿Cómo ha sido implementada la regulación de comercio electrónico por las instituciones financieras?

La presente sección abordará la implementación de la regulación sobre comercio electrónico por parte de las instituciones financieras, con el objetivo de evaluar si dicha implementación ha sido realizada de manera integral y viene siendo respetada por estas instituciones.

Como vimos en la sección anterior, partimos de la premisa de que existe una deficiencia en la regulación de las operaciones en línea. Si bien algunos de los supuestos se encuentran contemplados en la normativa vigente, parte de los errores radica en la implementación de esta realizada por las empresas de operaciones múltiples y el retraso en la entrada en vigencia, de manera efectiva, de las disposiciones normativas. Esto se debe a que, si bien se encuentran publicadas en El Peruano, cuentan con un periodo de adecuación entre 6 y 12 meses, es decir, terminan siendo exigibles hasta un año después. Esta situación genera que los usuarios se encuentren en un escenario de vulnerabilidad, al encontrarse expuestos a mayores riesgos en sus operaciones cotidianas como el fraude cibernético, phishing, operaciones no reconocidas, entre otros.

A continuación, se detallarán las medidas implementadas para las transacciones realizadas en el marco del comercio electrónico y los canales digitales. Asimismo, a través de las resoluciones y casos resueltos por el Indecopi, se examinarán los mecanismos utilizados por las instituciones financieras para incorporar dichas medidas. De igual manera, comentaremos brevemente cuáles son las medidas adoptadas por la legislación comparada.

Las conclusiones de esta sección servirán de base para analizar en la siguiente sección cómo el Indecopi evalúa las medidas adoptadas por las instituciones financieras y de qué manera ello incide en la predictibilidad de sus resoluciones.

2.1. ¿Cuáles son las medidas de seguridad implementadas para los casos de comercios electrónicos y canales digitales?

En la actualidad, cada vez más personas se afilian a los distintos servicios financieros ofrecidos por estas empresas, las cuales han tenido que responder a este incremento de afiliados, ampliando su oferta y adaptándose a los avances tecnológicos, lo que ha permitido una mayor agilidad en la afiliación, uso y disfrute de estos por parte de los consumidores. Por ejemplo, la mayoría de las empresas bancarias en el Perú cuentan con una banca móvil digital, lo cual permite al usuario poder revisar sus movimientos, realizar operaciones, pagar sus servicios, entre otros, desde la comodidad de su hogar a través de su celular.

En esa línea, como parte de las innovaciones tecnológicas y de sistemas operativos implementados, destacan los canales de distribución, que incluyen diversas plataformas mediante las cuales se ofrecen productos y servicios financieros a los clientes sucursales, cajeros automáticos (ATM), receptores de cheques y dinero en efectivo,

dispositivos POS, sistemas de respuesta automática (IVR), centros de atención telefónica (*Call Center*) o a través de mensajería instantánea (*WhatsApp*), sistemas de acceso remoto (RAS), internet y aplicaciones móviles. Todos estos medios deben operar y garantizar la seguridad y confianza, conforme a las disposiciones normativas emitidas por el supervisor bancario, en el caso peruano, la SBS (Anaya, 2012).

El incremento de estas tecnologías en las operaciones cotidianas genera un nuevo espacio en el cual los consumidores y proveedores se relacionan, lo cual también genera ciertos riesgos en este entorno digital. Uno de los principales riesgos se produce durante las operaciones, debido a que los usuarios tienen la posibilidad de acceder de manera libre a internet y en cualquier momento, por lo cual las entidades bancarias deben contar con sistemas de autenticación que aseguren que terceros no autorizados no puedan acceder a ninguno de los productos y/o servicios de los usuarios, ni a los fondos del propio banco. Cabe precisar que la mayoría de los reclamos que se presentan ante el Indecopi se originan por las fallas de los sistemas electrónicos y las medidas de seguridad implementadas, abriendo el camino para que se produzca cobros indebidos, operaciones no reconocidas, el fraude electrónico, entre otros (Indecopi, 2021).

En atención a ello, como parte de la normativa sectorial, tanto el Reglamento de Tarjetas como el Reglamento de Ciberseguridad establecen los mecanismos y medidas que deben ser implementadas por las empresas de operaciones múltiples como empresas bancarias, financieras, cajas municipales de ahorro y crédito, entre otras, así como los sistemas de ciberseguridad y autenticación, los cuales forman parte de la garantía del Estado de proteger a los consumidores. Por ello, nos centraremos en el análisis de las medidas incorporadas en los citados documentos normativos.

Cabe precisar que en la norma no hay una definición en concreto de lo que es una medida de seguridad, pero en este contexto, podríamos entenderlas como estrategias o procedimientos implementados por las entidades financieras de carácter inmediato a fin de garantizar una mayor protección a los usuarios de tarjetas. Por ejemplo, las medidas de seguridad aplicables a las tarjetas se encuentran establecidas entre los artículos 15 y 20 del Reglamento de Tarjetas. Es importante resaltar que la totalidad de las disposiciones normativas señaladas en dicho reglamento son de obligatorio cumplimiento para las entidades financieras, siendo que la inobservancia de alguna de ellas podría determinar su responsabilidad administrativa.

De esta manera, el Indecopi, a través de sus resoluciones, ha resaltado la importancia del artículo 17 del Reglamento de Tarjetas, el cual se encuentra orientado a establecer

las medidas de seguridad respecto a las operaciones, es decir, su monitoreo y realización. El citado artículo señala que las empresas deben adoptar al menos las siguientes medidas: implementar sistemas de monitoreo de transacciones que detecten operaciones fuera del comportamiento habitual de consumo, establecer procedimientos complementarios para gestionar las alertas generadas por dicho monitoreo, identificar patrones de fraude a través del análisis de información histórica de las transacciones, y establecer límites y controles en los diversos canales de atención con el fin de reducir las pérdidas por fraude.

En ese mismo sentido, el Reglamento de Ciberseguridad cuenta con disposiciones orientadas a garantizar la autenticación del usuario, es decir, verificar la identidad de la persona que se encuentra detrás de la pantalla o aparato tecnológico empleado y establecer límites mínimos para la navegación en el ciberespacio de manera segura. Es inevitable que las instituciones financieras consideren los riesgos cibernéticos en su transformación digital, ya que estos representan un desafío creciente en la gestión de riesgos para el sector bancario. Estos riesgos abarcan el robo de datos sensibles de los usuarios, robo de información confidencial por parte de ciberdelincuentes, hackers y grupos criminales, con el propósito de cometer fraudes electrónicos o cibernéticos.

En aras de brindar un entorno digital seguro, el artículo 17 del Reglamento de Ciberseguridad incluye requisitos específicos que deben cumplir las entidades financieras para implementar un proceso de autenticación, con especial atención en las operaciones que puedan causar algún perjuicio al usuario por el riesgo de fraude. El numeral 4 del artículo mencionado, precisa la obligación de las empresas de contar con herramientas para garantizar el monitoreo de operaciones, lo cual permitiría que, realizada una transacción fuera del patrón habitual de consumo, esta pueda ser detectada de manera inmediata y, por ende, se tomen acciones preventivas. Conforme lo establecido en la última resolución de cambio de criterio, las entidades financieras deben garantizar que todas las operaciones se hayan realizado de forma correcta[4]. Esa disposición fue pensada para disminuir la probabilidad de operaciones fraudulentas y será desarrollada a profundidad en la siguiente sección.

Asimismo, establece que, si no se cumple con la autenticación reforzada o se aplica algún supuesto de exoneración, conforme a lo señalado por el artículo 23 del

[4] Mediante la Resolución N° 2293-2024/SPC-INDECOPI (19 de agosto de 2024), la Sala establece un cambio de criterio, en el cual precisa que para que una operación sea realizada de forma correcta, debe considerarse si se encuentra dentro de su comportamiento habitual de consumo y cumplió con los requisitos de validez necesarios para autorizar la operación en cuestión.

Reglamento de Tarjetas, la responsabilidad de atender cualquier reclamo debe ser asumido por la empresa. Asimismo, se precisa la importancia de incluir más de dos factores biométricos o de categorías diferentes e independientes (algo que el usuario es, conoce y posee), así como incluir credenciales asignadas a cada usuario, cumplir con estándares criptográficos, implementar códigos únicos de autenticación de un solo uso, un sistema de notificaciones inmediatas, entre otras.

Es importante mencionar que el Indecopi ha generado una distinción en el análisis entre las operaciones producidas en el marco del comercio electrónico con las operaciones generadas a través de canales digitales, pues en función a ello, ha determinado la aplicación normativa correspondiente. Al respecto, según lo definido por el Reglamento de Ciberseguridad en el literal d) del artículo 2, un canal digital viene a ser aquel "*medio empleado por las entidades financieras para proveer servicios cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits*".

Esta definición de canal digital suele ser un poco escueta, razón por la cual el Indecopi, en una interpretación conjunta de las disposiciones del Reglamento, ha visto conveniente emitir una definición[5]. En esta definición se destaca que el término "canales digitales" hace referencia a aquellos medios que permiten al usuario efectuar un enrolamiento con anterioridad a la realización de cualquier operación y algunas de las operaciones del artículo 19 de la referida norma. Es decir, un enrolamiento es aquel procedimiento que permite verificar la identidad del usuario mediante el uso de factores biométricos o de factores de diferentes categorías al momento de realizar una operación a través de un canal digital. Este procedimiento tiene como objetivo reducir la posibilidad de casos de suplantación de identidad. Con estas limitantes, conforme lo visto en las resoluciones del Indecopi, el uso de "canal digital" quedaría restringido solo a lo que conocemos como banca móvil, banca por internet, billeteras digitales o cualquier otra plataforma digital con características similares.

Asimismo, mediante Resolución N° 201-2024/SPC-INDECOPI, el Indecopi ha buscado precisar los supuestos en los cuales se aplica el Reglamento de Tarjetas y el Reglamento de Ciberseguridad. De esta manera, se contempla que, para el análisis de casos en los cuales el servicio se desarrolló por un canal digital, estos deben ser analizados considerando también las disposiciones establecidas en el Reglamento de Ciberseguridad y lo establecido en el Reglamento de Tarjetas. Por su parte, las

[5] Encontramos una definición de canales digitales en la Resolución N° 0201-2024/SPC-INDECOPI.

operaciones realizadas netamente a través de una plataforma distinta a las antes mencionadas (comercio electrónico) serán analizadas bajo lo dispuesto en el Reglamento de Tarjetas.

2.2. ¿Cómo han sido implementadas las medidas de seguridad para operaciones en línea por las instituciones financieras?

Como vimos anteriormente, con los avances de las nuevas tecnologías, las entidades financieras deben adaptarse tanto a las nuevas condiciones del entorno competitivo como a las demandas de los consumidores en esta nueva era. Este proceso ha tenido tres etapas: primera, la innovación en productos y canales de información; segunda, la adecuación de la infraestructura tecnológica; y, finalmente, la reestructuración organizacional necesaria para competir en el mercado digital (Cuesta, Ruesta, Tuesta, & Urbiola, 2015). A fin de entender cómo estas medidas han sido implementadas por las instituciones financieras como los bancos, utilizaremos como parámetro las resoluciones emitidas por el Indecopi.

Las entidades financieras se encuentran obligadas a contar con todas las medidas de seguridad, procesos y mecanismos de autenticación, verificación, monitoreo, entre otros, tal cual ha sido establecido por la SBS en sus reglamentos. Cabe precisar que, al encontrarse contenidas en los reglamentos, constituyen una garantía legal, es decir, son de obligatorio cumplimiento por las partes y no pueden pactar dejarlas sin efecto, siendo que el incumplimiento de alguna de las disposiciones normativas constituiría una infracción inmediata al deber de idoneidad.

A pesar de ello, uno de los principales problemas se produce con la inobservancia de alguna de estas disposiciones por parte de las empresas, como regla general, el Indecopi ha puntualizado que, en función de la garantía legal, el parámetro de idoneidad en la prestación de servicios y productos financieros, especialmente en lo que respecta a la afectación de cuentas o líneas de crédito de los usuarios, está inequívocamente vinculado a las medidas de seguridad atribuidas por la normativa sectorial[6]. Esto incluye, ineludiblemente, el deber de monitorear y detectar consumos inusuales o sospechosos, realizando un seguimiento exhaustivo y particular de las operaciones en tiempo real. A continuación, veremos algunos ejemplos:

[6] Resoluciones: 0201-2024/SPC-INDECOPI, 0741-2024/SPC-INDECOPI, 0736-2024/SPC-INDECOPI, 1146-2024/SPC-INDECOPI, 0793-2024/SPC-INDECOPI, entre otras.

Mediante Resolución 0741-2024/SPC-INDECOPI, la Sala Especializada en Protección al Consumidor (en adelante, la Sala) declaró fundada la denuncia interpuesta contra Scotiabank, al determinarse que no adoptó las medidas de seguridad correspondientes al no alertar una operación fuera del patrón habitual del consumidor ascendente a S/. 10 060,00, permitiendo que se realicen 7 operaciones posteriores con cargo a su cuenta de ahorros. Dentro del análisis del caso, se determinó que la empresa habría validado la operación con los métodos de autorización, autenticación y verificación establecidos por la normativa correspondiente. Sin embargo, se confirmó que el sistema de monitoreo de Scotiabank no habría detectado la operación inusual (S/. 10 060,00). Concluyendo que, si bien había cumplido con validar la operación, no contaría con los mecanismos idóneos para detectar una operación fuera del comportamiento habitual del usuario, generando un detrimento patrimonial al consumidor.

Asimismo, a través de la Resolución 0201-2024/SPC-INDECOPI, la Sala revocó lo resuelto en primera instancia y declaró infundada la denuncia interpuesta contra el Banco BBVA. En este caso, la Sala analizó previamente si nos encontrábamos en el marco de la aplicación del Reglamento de Ciberseguridad, pues ya se encontraba vigente para la fecha en la que ocurrieron los hechos controvertidos. No obstante, conforme lo señalado en el acápite anterior, para que se aplique dicho reglamento debemos encontrarnos en los supuestos de canales digitales (banca móvil, por internet, billeteras digitales, entre otros). En este caso en particular, se confirmó que no nos encontrábamos en dichos supuestos, siendo únicamente de aplicación el Reglamento de Tarjetas.

En el análisis se confirmó, primero, que ninguna de las operaciones controvertidas se encontraba fuera del patrón habitual de consumo del usuario. En segundo lugar, el Banco BBVA acreditó, a través de los medios probatorios aportados, que la operación se había autorizado y procesado cumpliendo los requisitos de validez necesarios (clave, código CVV, códigos dinámicos de autorización). Con ello se verificó que, para este caso, la entidad financiera sí había cumplido con todas las medidas establecidas en el reglamento.

La Resolución 0426-2024/SPC-INDECOPI incluye el análisis del canal de "*Homebanking"* del Banco Pichincha. En ese caso, la Sala revocó, en parte, lo resuelto por la primera instancia, al comprobarse que la empresa no habría adoptado las medidas de seguridad referidas a la validez de las operaciones. Como parte del criterio de la Sala, se indicaba que se debía considerar el importe individual de las operaciones

que el consumidor realiza de manera cotidiana en el producto cuestionado a fin de establecer un patrón habitual. La Sala reconoce la necesidad de contar con todas las medidas de seguridad establecidas en el Reglamento de Tarjetas, siendo que determinó que el sistema de monitoreo no tendría que haber levantado una alerta de posible operación sospechosa, puesto que ninguna de las operaciones controvertidas se encontraba fuera del consumo habitual del usuario. Asimismo, el cliente se había afiliado válidamente al canal de *homebanking*, no obstante, se comprobó que no se habría utilizado las claves de seguridad y códigos dinámicos remitidos al correo electrónico del usuario para autorizar las operaciones. Con ello, se concluyó atribuir la responsabilidad administrativa al Banco Pichincha.

Por último, la Resolución 1146-2024/SPC-INDECOPI confirmó lo resuelto en primera instancia y declaró fundada la denuncia contra el Banco Interbank al no haber adoptado las medidas de seguridad pertinentes para cargar 6 operaciones a la cuenta de ahorros de la denunciante y 3 operaciones a su línea de crédito. En este caso, se determinó que no correspondía aplicar el Reglamento de Ciberseguridad toda vez que las operaciones controvertidas habían sido realizadas a través del comercio electrónico, medio distinto al de canales digitales, conforme lo establecido en anteriores pronunciamientos.

Para el análisis de este caso, también se consideró verificar si el Interbank contaba con todas las medidas de seguridad establecidas en la normativa correspondiente (artículo 17 del Reglamento de Tarjetas). A diferencia de los casos anteriormente citados, en este caso, el Interbank, más allá de haber argumentado que la consumidora autorizó las operaciones por vía mensaje de texto, no presentó ningún medio probatorio que acreditara que estas operaciones cuestionadas habían sido válidamente autorizadas por la usuaria utilizando los sistemas y mecanismos mínimos de autenticación. Por esta razón, se confirmó que el Interbank no había adoptado las medidas de seguridad correspondientes, generando un perjuicio patrimonial al consumidor.

Como podemos ver de los casos citados, uno de los mayores problemas de las entidades financieras es no cumplir con la totalidad de las medidas establecidas por la SBS, siendo que la falta de adopción o el funcionamiento parcial de alguna de ellas constituye una infracción al deber de idoneidad, pues no se habría cumplido con las garantías legales exigidas por el ordenamiento. Al respecto, cabe precisar que, para estos casos, hemos podido identificar que las entidades financieras se encontrarían en mejor posición para probar y acreditar el cumplimiento de las medidas exigidas. Este

último punto viene siendo considerando en la legislación comparada, y, recientemente, incluido en nuestro Reglamento de Tarjetas.

2.3. ¿Cuáles son las medidas de seguridad adoptadas para operaciones en línea no reconocidas en la legislación comparada?

Con el desarrollo del comercio electrónico, los avances de la tecnología y el desarrollo de los canales digitales las entidades financieras a nivel global han tenido que adaptarse a estos nuevos entornos. En el plano internacional, cada país cuenta con normativa para regular las operaciones en el entorno digital, sea en un solo cuerpo normativo o a través de diversa regulación sectorial.

Las instituciones bancarias actuales manejan el 90% de sus activos en formato digital. No obstante, este avance tecnológico en sus modelos de negocio también implica un aumento en los riesgos, debido a que la ciberdelincuencia se ha incrementado y se aprovecha de los vacíos o vulnerabilidad de los sistemas de defensa cibernética, siendo la adaptación lenta a las nuevas tecnologías clave para enfrentar dicha problemática (Gutiérrez, 2017).

Con ese contexto, la normativa de cada país se ha orientado a cubrir supuestos relacionados a la seguridad y verificación en las compras en línea, por ejemplo, en Estados Unidos, mediante la *Uniform Electronic Transactions Act* (UETA) se regulan las transacciones comerciales, transacciones de negocios y las transacciones gubernamentales, así como la manifestación de voluntad a través de medios tecnológicos y respecto a las firmas digitales (Rojas, 2007, p.547). En el caso de la protección al consumidor, bajo la Ley de Transferencia Electrónica de Fondos (Electronic Fund Transfer Act) y la Ley de Facturación Justa de Crédito (Fair Credit Billing Act), los consumidores están protegidos contra transacciones no autorizadas realizadas con sus tarjetas o el conocido fraude cibernético.

Ambas leyes limitan la responsabilidad del consumidor a un monto ascendente a 50 dólares, en caso este reporte la transacción no autorizada dentro de los dos (2) días hábiles posteriores a su notificación. De esta manera, se genera que la carga de la prueba recaiga sobre el proveedor, quien se encuentra en mejor posición y posee más información respecto a la transacción, pues en caso busque eximirse de responsabilidad debe acreditar la responsabilidad del consumidor.

En España y Alemania cuentan con una regulación adicional, pues se guían con lo establecido y regulado respecto al comercio electrónico de la Unión Europea. En esa línea, cuentan adicionalmente con normativa específica y sectorial dirigida a otorgar una

mayor protección a los consumidores. Por ejemplo, a través del Real Decreto-Ley 19/2018, en España se establece que los usuarios no son responsables por las transacciones no autorizadas en sus tarjetas, siempre y cuando, se notifique al proveedor de servicios de pago sin demora indebida una vez descubierta la operación no reconocida y dentro de los trece (13) meses posteriores a la fecha del débito. En este país, la responsabilidad del usuario está limitada hasta 50 euros por pérdidas derivadas de transacciones y la carga de la prueba recae sobre el proveedor del servicio. En otras palabras, si se comprueba que el usuario actuó de forma fraudulenta o con negligencia grave, deberá asumir la responsabilidad por dichas operaciones.

Del mismo modo, en Alemania, la responsabilidad del usuario se limita a un máximo de 50 euros, siempre que informe al proveedor al detectar la operación no reconocida. El banco o proveedor de servicios de pago deberá reembolsar el importe cuestionado de manera inmediata, dentro del plazo de un día hábil posterior a la notificación de la operación controvertida, conforme lo señalado por la Ley de Supervisión de Pagos.

La regulación del comercio electrónico y operaciones en línea de los países latinoamericanos cuentan con características diferentes como, por ejemplo, plazos para la atención y respuesta de la queja de un consumidor que asegura ser víctima de un fraude cibernético o no reconoce las operaciones cargadas a sus puestos; así como, procedimientos para el reembolso o reversión del pago y; por último, montos establecidos para limitar la responsabilidad del usuario.

Primero, en Argentina, el artículo 26 de la Ley 25.065, que regula el funcionamiento de tarjetas y compras, establece que los titulares pueden impugnar sus estados de cuenta dentro de los treinta (30) días de recibida, detallando la operación no reconocida o errada (impugnación del resumen). A través de un reclamo ante la entidad bancaria, se impugna y se solicita la reversión de los cargos cuestionados. De no obtener una respuesta en siete (7) días hábiles, el usuario puede dirigirse al Banco Central de la República de Argentina, quienes redireccionarán su reclamo a la Dirección de Defensa del Consumidor.

Segundo, en Chile, la Ley de Fraudes, Ley 21.234, protege a los usuarios de medios de pago y transacciones electrónicas, también limita su responsabilidad en casos de delitos financieros como extravío, hurto, robo o fraude. Si el usuario no reconoce una operación, debe informar a la entidad financiera para que proceda con el bloqueo respectivo de manera inmediata. Desde el aviso, la entidad tiene cinco (5) días hábiles para restituir la totalidad de los cargos cuestionados si la cuantía es menor a 35 unidades de fomento y tendrá siete (7) días hábiles, si es mayor. La ley también recalca que la carga de la

prueba recae sobre la entidad bancaria, quien, si quiere exonerarse de responsabilidad, deberá demostrar que la transacción fue por dolo o culpa grave del usuario.

Finalmente, la Ley 1480 de Colombia establece en su artículo 51 que, si las transacciones no reconocidas se originan por canales digitales y el medio de pago fue un instrumento electrónico, como tarjetas, se debe "reversar" el pago cuestionado por el consumidor si este manifiesta haber sido víctima de fraude, sea una operación no solicitada, el producto adquirido no sea recibido, o el producto entregado sea defectuoso. Si se verifica o se emite una resolución judicial que determine la responsabilidad del usuario, se debitará el monto cuestionado de su cuenta corriente o de ahorros.

En nuestro país, las últimas modificaciones incorporadas a nuestra normativa vigente se encuentran orientadas a brindar una mayor protección al consumidor, siendo uno de los cambios más resaltantes el traslado de la carga de la prueba al proveedor, lo cual ya viene siendo desarrollado por la autoridad.

En esa línea, nos encontramos de acuerdo con lo señalado por el Indecopi mediante Resolución 201-2024/SPC-INDECOPI, en la cual señala que, para un consumidor, no es posible demostrar un hecho negativo, como la no realización de una transacción con su tarjeta. Sin embargo, la entidad financiera, como proveedora del servicio, se encuentra en mejor posición de demostrar que dicha operación se llevó a cabo utilizando las medidas de seguridad implementadas por ella misma y que se encuentran a disposición del cliente. Esto se justifica en la ventaja que tiene el banco en términos de acceso a la información y los medios necesarios para probar que la transacción fue efectivamente realizada, cumpliendo los mecanismos mínimos requeridos de autenticación y validez.

Como indicamos, ello va en línea con lo regulado por la legislación comparada y con la disposición incorporada al Reglamento de Tarjetas, la cual entrará en vigencia recién el 1 de julio de 2025. En dicha disposición se establece que "*la empresa es responsable de las pérdidas en operaciones no reconocidas, salvo que acredite la responsabilidad del usuario, conforme a lo establecido en los numerales 9 y 10 del artículo 23 del Reglamento*"[7]. Es decir, a partir de la fecha mencionada, en nuestro país, considerando la mejor posición de información, infraestructura y seguimiento que tienen las entidades financieras respecto a las operaciones que realizan los usuarios de sus servicios, estas

[7] RESOLUCIÓN SBS N° 02286-2024: Modifican el Reglamento de Tarjetas de Crédito y Débito, el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, el Reglamento de Gestión de Conducta de Mercado del Sistema Financiero y el Reglamento de Reclamos y Requerimientos

serán responsables por las pérdidas generadas en el caso de operaciones no reconocidas.

Me encuentro de acuerdo con dicha disposición, debido a que no solo se alinea a lo establecido en la normativa comparada sino también brinda al consumidor mayor seguridad respecto al seguimiento de sus operaciones y genera que las entidades financieras tengan mayor diligencia al momento de implementar sus medidas de seguridad.

A raíz de todo lo expuesto en la presente sección, como conclusión, podemos señalar lo siguiente:

- En el marco del comercio electrónico, las medidas de seguridad referidas a la configuración de operaciones a través de medios digitales se encuentran establecidas en el Reglamento de Tarjetas y el Reglamento de Ciberseguridad, siendo aplicable como base el de Tarjetas y, en caso exclusivo de canales digitales, el de Ciberseguridad.
- Las instituciones financieras se encuentran obligadas a cumplir con la normativa sectorial vigente en su totalidad. No obstante, conforme lo hemos visto en los casos resueltos por el Indecopi, en nuestro país, la implementación de las medidas de seguridad suele ser parcial o incompleta, lo cual genera que se produzcan transacciones realizadas por terceros.
- En la legislación comparada, los diferentes países regulan el comercio electrónico y el tratamiento a casos de posibles fraudes cibernéticos, siendo el más común, las operaciones no reconocidas. Para ello, la carga de la prueba recae sobre los proveedores, al considerar que se encuentran en mejor posición probatoria.

SECCIÓN III: ¿Cómo incide la regulación sobre comercio electrónico en la predictibilidad de las resoluciones del Indecopi?

En la presente sección se analizará la incidencia de la regulación actual sobre el comercio electrónico en las resoluciones emitidas por el Indecopi y cómo puede repercutir en la predictibilidad de estas, lo cual termina afectando el principio de seguridad jurídica dentro de un procedimiento administrativo. Para determinar ello, revisaremos las resoluciones emitidas por la autoridad e identificaremos cuáles han sido los principales cambios de criterio que se han producido en los últimos cinco (5) años.

En esa línea, explicaremos el rol del Indecopi en la interpretación y aplicación de la normativa correspondiente, siendo fundamental que la norma sea precisa, pueda cubrir los supuestos requeridos y se encuentre a la vanguardia de los avances tecnológicos. Asimismo, desarrollaremos el actual criterio emitido por la Sala del Indecopi bajo la Resolución 2293-2024/SPC-INDECOPI, en el cual reconoce que es determinante que las entidades financieras puedan contar con mecanismos tecnológicos suficientes que garanticen la validez de las operaciones realizadas por los usuarios.

3.1. ¿Cuáles han sido las variaciones de criterios de interpretación utilizados por el Indecopi a lo largo de los últimos 5 años?

Para desarrollar este apartado, es necesario tener en cuenta a qué nos referimos con predictibilidad y cómo esta se relaciona con el principio de seguridad jurídica en la resolución de controversias administrativas. En función a ello, analizaremos cuáles han sido los cambios de criterio en las resoluciones emitidas por el Indecopi para los casos de operaciones no reconocidas realizadas a través del comercio electrónico y/o canales digitales.

Conforme lo señalado por Morón, el principio de la predictibilidad se encuentra reconocido en la Ley de Procedimiento Administrativo General y prescribe que la autoridad administrativa debe brindar a los administrados información veraz, completa y confiable sobre cada uno de los procedimientos a su cargo, lo cual incluye que el administrado tenga comprensión sobre los posibles resultados que se podrían obtener en cada caso concreto y cuál va a ser la actuación de la administración al aplicar el Derecho, retirando cualquier riesgo de incertidumbre (2017, p.383). Es decir, los administrados deben tener una expectativa razonablemente fundada sobre cuál será la aplicación e interpretación de la normativa sectorial aplicable y, en función a ello, cómo será resuelto el caso.

El principio de predictibilidad o confianza legítima busca brindar seguridad jurídica a los administrados en el marco de un procedimiento administrativo, siendo que la Administración no puede modificar unilateralmente sus decisiones sin que medie una justificación concreta (Morón, 2017, p.129). En ese sentido, vemos que la autoridad administrativa debe considerar que, a través de sus resoluciones, brinda más que un resultado a los administrados, sino también transmite información que puede guiar su comportamiento, un mensaje de confianza y una expectativa legítima de la interpretación normativa.

Cabe precisar que, la predictibilidad puede permitir conocer a los administrados cuál sería el resultado de manera previa, sin embargo, esta debe admitir excepciones, pues se pueden generar situaciones que concluyan con una modificación de la decisión final de la autoridad (Cortés, 2024). En ese sentido, considero que, si se va a producir algún cambio de criterio, debe mediar una justificación concreta, la cual permitiría que el administrado tome conocimiento y entienda por qué en su caso recibió un resultado diferente al esperado.

Teniendo en consideración lo señalado, a continuación, analizaremos cómo han venido cambiando los criterios respecto a la resolución de casos relacionados a las operaciones no reconocidas bajo canales digitales y/o comercio electrónico en los últimos años. Al respecto, cabe precisar que, el artículo 17 del Reglamento de Tarjetas, referido a las medidas de seguridad que deben adoptar las entidades financieras para el monitoreo de operaciones, ha sido de suma importancia para el análisis de casos de transacciones en línea.

En el año 2019, la Sala consideraba que la finalidad del artículo 17 se encontraba en proteger a los usuarios de cualquier transacción que podría constituir un fraude, pues para ello, exigía el análisis del movimiento histórico de los usuarios. Asimismo, la Sala consideraba que debe analizarse primero el patrón de consumo y, posteriormente, la validez de las operaciones. Lo curioso de las resoluciones emitidas durante este periodo[8] es que se estableció como criterio que era la entidad bancaria o financiera quien debía determinar qué factores considerar para hacer el análisis sistemático del conocido “patrón” habitual de consumo. Es decir, el proveedor se encontraba facultado de elegir qué factores consideraba determinantes para evaluar el patrón de consumo de los usuarios, sin que medien parámetros mínimos para ello, a nuestra consideración, dejando abierta una posibilidad más a la trasgresión del principio de predictibilidad.

Posteriormente, para los casos resueltos en el 2022, la Sala señaló de manera expresa la necesidad de analizar la totalidad de los consumos efectuados por periodos, ello con la finalidad de obtener un patrón de consumo más preciso. Asimismo, incluyó dentro de su pronunciamiento que las entidades financieras debían cumplir con “todas” las medidas de seguridad establecidas en el artículo 17 del Reglamento de Tarjetas, puesto que la inobservancia de alguna de ellas implicaría un servicio inidóneo. Para esta

[8] Resoluciones 0226-2019/SPC-INDECOPI, 0063-2019/SPC-INDECOPI y 0141-2020/SPC-INDECOPI.

oportunidad, la Sala buscaba brindar un criterio más objetivo, para lo cual estableció que, para identificar si la operación se encontraba fuera del patrón de consumo del usuario, se debía tomar en cuenta el "importe individual" de las operaciones que el consumidor usualmente realizaba con el producto objeto de denuncia[9]. Vemos que la Sala empieza a reconocer la necesidad del cumplimiento de todas las medidas de seguridad de manera obligatoria y, además, reconoce que debía brindar a las entidades financieras un criterio objetivo que les permita identificar cualquier operación fuera del patrón habitual del usuario y no dejarlo a su libre consideración.

Para el año 2023, hubo diferentes cambios al momento de evaluar los casos de operaciones no reconocidas producidas en línea y se introdujeron nuevas aristas en las que vale la pena profundizar. Podemos empezar señalando que, si bien se buscó continuar con la línea de contar con un criterio objetivo para el análisis del comportamiento habitual de consumo del usuario, se introdujeron nuevos factores a considerar. Se resolvía tomando en cuenta el "importe" de las operaciones que el consumidor usualmente realizaba con el producto objeto de denuncia, dejando de lado el término importe "individual"[10]. Asimismo, se precisa que el análisis debe considerar la totalidad de canales utilizados previamente por el consumidor, así como su frecuencia. La Sala concluye que estos elementos por sí solos no pueden llevar a determinar que una operación es inusual, sino deben ser analizados de manera conjunta.

Considero que, en este punto, se toma consciencia de que el producto debe ser visto de manera integral y tomando en cuenta determinados periodos de tiempo (mientras la tarjeta estuvo activa, inactiva, tiempo de uso, entre otros). Adicionalmente, la Sala concluía que una operación no podía ser considerada inusual o sospechosa solo porque se realizaba por "primera vez" en un establecimiento distinto o con una frecuencia diferente, pues también en esos casos se debía estudiar si el monto individual difería de lo que usualmente consumía el usuario en sus cuentas. En ese sentido, coincido con lo señalado por la Sala, pues para concluir si una operación es inusual o fraudulenta se debe contar con más de un elemento que permita acreditar ello.

Un elemento controvertido en las resoluciones emitidas por la Sala recaía en el momento de otorgar medidas correctivas. Desde el 2022, la Sala había determinado que, si se cumplía con los requisitos de validez de la primera operación sospechosa, al

[9] Resoluciones 2609-2022/SPC-INDECOPI y 2611-2022/SPC-INDECOPI.
[10] Resoluciones 0031-2023/SPC-INDECOPI, 0005-2023/SPC-INDECOPI y 0068-2023/SPC-INDECOPI.

no ser un sistema de naturaleza predictiva, la operación se concretaba de manera válida y, por ende, no correspondía otorgar la devolución al consumidor de este monto, sino por los posteriores consumos que se realicen. Ello se fundamentada en que el sistema de monitoreo del Banco no podía ser de naturaleza predictiva, sino que se construye con cada operación efectuada por el consumidor, de ser predictivo, podría impedir que el consumidor realicé por primera vez una operación diferente a las anteriores. Es decir, si resultaba fundada la denuncia al comprobarse que la entidad bancaria no habría adoptado las medidas exigidas del Reglamento de Tarjetas, pero la primera operación fuera del patrón habitual de consumo había cumplido con los requisitos de validez, solo se otorgaba la devolución por las operaciones siguientes que hubiera realizado este tercero.

En resumen, a través de los últimos años, la autoridad ha ido considerando nuevos factores para resolver los casos de operaciones no reconocidas, siendo que, en el 2019, cada entidad bancaria determinaba qué factores debía considerar para evaluar el patrón de consumo de cada uno de sus clientes. Para el año 2022, a fin de realizar un análisis igual para todos los casos, la Sala consideraba como guía el “importe individual” de todas las transacciones realizadas por el usuario. Para el año siguiente, buscó profundizar dicho análisis, determinando la naturaleza de los procedimientos que debían implementar los proveedores para el seguimiento y monitoreo de operaciones, señalando que al no tener naturaleza predictiva, no podían “prever” la primera operación fuera del patrón habitual de consumo y detenerla, simplemente debían generar la alerta respectiva y comunicar al usuario y/o bloquear la tarjeta conforme lo indica el artículo el artículo 21 del Reglamento de Tarjetas. Asimismo, consideraba necesario analizar distintos factores como canal, frecuencia, establecimiento para determinar el patrón de consumo del usuario, ello se mantuvo así hasta julio de 2024.

En el mes de agosto de 2024, se produjo un último cambio de criterio, mediante la Resolución 2293-2024/SPC-INDECOPI (en adelante, Resolución con nuevo criterio), para el análisis de casos de operaciones no reconocidas. Este cambio de criterio introdujo un nuevo escenario, principalmente en lo referido a la primera operación, dejando de lado la idea de que los mecanismos exigidos por el artículo 17 del Reglamento de Tarjetas no tienen naturaleza predictiva, lo cual analizaremos en el siguiente acápite.

Como hemos podido identificar, en un periodo de cinco (5) años aproximadamente han ido cambiando los factores a considerar por parte de la autoridad para analizar este tipo

de casos, lo cual ha generado poca predictibilidad al respecto. Por ejemplo, un caso ocurrido en el 2021, en el cual se trate de una sola operación, al considerarse que los mecanismos de seguridad exigidos a las entidades financieras no tienen naturaleza predictiva y validarse la operación, no sería sujeto a devolución como parte de la medida correctiva a pesar de encontrarse fuera del patrón habitual de consumo del usuario. No obstante, a partir de agosto de 2024, con este nuevo criterio, de confirmarse que la operación controvertida estaba fuera del patrón habitual de consumo, sí correspondería devolver el monto de la operación al usuario.

De lo expuesto, tenemos claro que la autoridad debe permitir que el administrado conozca la interpretación que hace respecto a la normativa aplicable a su caso, de manera que puede evitar que se generen denuncias sin fundamento, pues sabrán de antemano cuál sería el resultado que obtendrían. Asimismo, también, permite que el administrado conozca los medios probatorios que requiere para poder sustentar su posición, ahorrando así costos de transacción para la Administración.

En ese sentido, si se trasgrede el principio de predictibilidad y seguridad jurídica, termina dañándose la confianza de los administrados en la autoridad administrativa y genera incertidumbre respecto a sus casos (Cortés, 2024). Por ello, es importante que la autoridad administrativa, en sus diferentes instancias, busquen garantizar la predictibilidad en sus resoluciones, pues se genera una legítima expectativa en los administrados. Si bien los criterios pueden ir cambiando debido a la modificación de la normativa aplicable, supuestos que generan una situación nueva o particular, entre otras, estos cambios deben venir acompañados de una razón justificada y obedeciendo al contexto en el que se desarrolla.

Cabe precisar que, para los casos citados, podemos ver que la normativa aplicable continuaba siendo el artículo 17 del Reglamento, por lo cual el cambio de criterio de estos últimos años obedecía a la interpretación realizada por el Indecopi. De igual manera, es importante recalcar que la Sala señalaba que la primera operación debía constituir una alerta, más, si se determinaba su validez, esta tendría que procesarse. Con ello, el consumidor se encontraba expuesto a que su patrimonio se viera afectado si se determinaba la validez de la primera operación, debido a que el sistema de monitoreo no tendría una naturaleza predictiva (Que pudiera prever la operación), sino era de seguimiento y de generación de alerta para evitar un detrimento patrimonial causado por las siguientes operaciones.

En ese sentido, debemos tener en cuenta la importancia de contar con disposiciones normativas claras y precisas, pues, a partir de cómo se encuentran redactadas y estructuradas, la autoridad administrativa buscará aplicarlas para el caso en concreto o interpretarlas, de ser necesario, garantizando una mayor predictibilidad en lo resuelto por los diferentes órganos que componen el Indecopi a nivel nacional.

3.2. A la luz de la regulación actual, ¿cuáles son los criterios adoptados por el Indecopi para evaluar operaciones realizadas por comercio electrónico?

En la actualidad, como parte de la regulación y normativa sectorial aplicable para casos de operaciones no reconocidas en línea tenemos al Reglamento de Tarjetas y el Reglamento de Ciberseguridad. Conforme lo señalado por el Indecopi, cuando se trate de una operación realizada mediante canales digitales, se aplicará también el Reglamento de Ciberseguridad.

A fin de determinar si se brindó un servicio idóneo o inidóneo a los usuarios, el Indecopi verifica que la entidad financiera haya cumplido con la normativa sectorial vigente, empezando con la totalidad de medidas establecidas en el artículo 17 del Reglamento de Tarjetas, el cual comentamos anteriormente y forma parte de las expectativas razonables que tiene un consumidor al contar con un producto financiero. Este artículo, en particular, establece todas aquellas medidas y procedimientos que deben implementar las entidades financieras, siendo fundamental que permitan dar seguimiento a las operaciones que se realicen en tiempo real y, de ser inusual, generar una alerta.

De tratarse de un canal digital, se debe tener en cuenta también las disposiciones de los artículos 17, 18 y 19 del Reglamento de Ciberseguridad, las cuales desarrollamos en la sección anterior, pues están relacionados con la autenticación de los usuarios al momento de realizar operaciones en línea. Estos artículos se encuentran relacionados entre sí pues permiten la autenticación y el enrolamiento en estos canales digitales, buscando que quien realice las operaciones sea efectivamente el titular, disminuyendo la posibilidad de operaciones fraudulentas.

Como señalamos anteriormente, la normativa sectorial exige que las entidades financieras cuenten con un registro del historial de consumo de cada uno de sus usuarios con el objetivo de obtener el patrón habitual de consumo, el cual debe ser generado a partir de diferentes factores como frecuencia, canal, tipos de comercio, entre otros. Con la finalidad de poder identificar si alguna operación se encuentra fuera del

patrón habitual de consumo, las entidades financieras deben implementar las medidas de seguridad exigidas por el Reglamento de Tarjetas y considerar que estas deben ser eficaces en reconocer si la operación controvertida se aleja de las operaciones cotidianas del consumidor para poder generar la alerta correspondiente. Asimismo, también es determinante verificar la validez de la operación, es decir, si esta cumplió con los requisitos mínimos necesarios para poder procesarse como código CVV, datos de la tarjeta, factores de autenticación reforzada, entre otros.

Para entender mejor cómo se analiza un caso sobre operaciones no reconocidas en la actualidad revisaremos el análisis realizado por la Sala en la Resolución con nuevo criterio, la cual establece cambio en el análisis de la primera operación. Este cambio tiene como objetivo que, ante la alerta de una operación sospechosa o inusual, no se genere un perjuicio patrimonial al consumidor. A diferencia del criterio anterior sostenido por la Sala señalando que la naturaleza de estos mecanismos exigidos era únicamente alertar la operación sospechosa y evitar que se continúen produciendo mayores operaciones, actualmente, la Sala ha concluido que, de detectarse una operación sospechosa, esta "primera operación" tampoco debería ser procesada.

En este caso, el señor Medina habría denunciado a Interbank por permitir el cargo de 7 operaciones que no reconocía a su tarjeta de crédito, las cuales se encontraban fuera de su patrón habitual de consumo, quedando acreditado que el Banco no habría cumplido con adoptar las medidas de seguridad necesarias. En el análisis realizado por la Sala se concluyó que, considerando la información histórica y revisando los estados de cuenta del señor Medina, la operación de mayor valor realizada en un periodo entre setiembre del 2021 y octubre de 2022 ascendía a S/. 35.90. Sin embargo, la operación controvertida ascendía a S/. 4 994.50, lo cual superaba en exceso el consumo habitual del señor Medina. A pesar de ello, la entidad financiera en cuestión no identificó esta operación como inusual ni alertó al consumidor al respecto.

Como hemos visto en el acápite anterior, la Sala siempre ha considerado determinante el patrón habitual de consumo del usuario, el cual se obtiene de este análisis histórico y sistemático de las operaciones realizadas por el consumidor, para la evaluación de este tipo de controversias. En ese sentido, ahondando en lo resuelto por la Sala, podemos identificar que la entidad financiera no cumplió con lo establecido en el artículo 17 del Reglamento de Tarjetas, generando así un detrimento patrimonial al señor Medina. De igual forma, la Sala consideró necesario aclarar este cambio de criterio pues considera que las entidades financieras deben contar con mecanismos que permitan garantizar al usuario que solo se le cargarán operaciones "correctas", es decir, que se encuentren

dentro de su patrón habitual y que cumplan con los requisitos de validez necesarios dependiendo del tipo de operación.

Asimismo, concluye que, si una operación se encuentra fuera del patrón habitual de consumo del usuario, debe ser identificada, producir una alerta y es la entidad financiera quien debe adoptar las medidas necesarias para evitar que se cargue la transacción controvertida y las posteriores, pues se encuentra en mejor posición para prever que esta operación sospechosa se concretice. Por ello, declaró fundada la denuncia y sancionó a Interbank por no haber cumplido con adoptar las medidas de seguridad establecidas en la normativa sectorial, infringiendo su deber de idoneidad.

Me encuentro de acuerdo con este análisis propuesto en tanto cumple con el rol tuitivo del Estado respecto a la protección al consumidor y, además, busca garantizar que las entidades financieras pongan atención en los sistemas, medidas y mecanismos que implementan para brindar seguridad de manera efectiva a los usuarios cuando utilizan sus productos financieros. De igual manera, permite que las entidades financieras, quienes se encuentran en mejor posición de asumir el riesgo y el control de la situación al contar con la tecnología necesaria para monitorear las operaciones en tiempo real, sean las encargadas de acreditar el cumplimiento de sus obligaciones. En el caso de operaciones no reconocidas, resulta imposible que el usuario pueda identificar si un tercero realizó una operación con sus tarjetas, salvo se encuentre revisando sus movimientos en todo momento o se le notifique de ello. Situación distinta ocurre con la entidad financiera, quien se encuentra obligada a realizar un seguimiento y monitorear todas las operaciones, pues forma parte de una garantía legal ofrecida a los consumidores.

Como mencionamos en la primera sección, en el Reglamento de Tarjetas hay algunas disposiciones que, a la fecha de cierre de este artículo, todavía no son exigibles a las entidades financieras porque se encuentran en periodo de adecuación hasta el 1 de julio de 2025. Sin embargo, es probable que cuando inicien su obligatoriedad habrá modificaciones al momento de analizar los casos por parte de la autoridad e, inclusive, podría haber un nuevo cambio de criterio. Ello en atención a que esta modificación traslada la carga de la prueba ante operaciones no reconocidas al proveedor, en este caso, las entidades financieras, pues ahora deben acreditar responsabilidad del usuario, caso contrario serán responsables por las pérdidas en las que incurra el consumidor.

A modo de reflexión, debemos tener en cuenta que, estos cambios en la interpretación normativa respecto al análisis realizado en el caso de operaciones no reconocidas, genera poca predictibilidad en lo resuelto por el Indecopi. Si bien señalamos

anteriormente que nos encontramos de acuerdo con que existan cambios, estos deben ser fundados a fin de garantizar que los administrados conozcan y entiendan las razones de los cambios para así poder guiar su actuación.

De lo expuesto anteriormente, podemos sacar las siguientes ideas principales:

- El principio de predictibilidad busca que la Administración brinde a los administrados información clara y confiable sobre los procedimientos y pronunciamientos a su cargo, con la finalidad de que puedan conocer de manera previa la aplicación normativa e interpretativa realizada por la autoridad, generando una expectativa razonable al administrado sobre su posible resultado.
- En estos últimos años, la normativa ha ido modificándose, sin embargo, también se han producido diferentes cambios de criterios para analizar operaciones no reconocidas. Con ello, ha habido algunas discrepancias en lo resuelto y se ha venido afectando el principio de predictibilidad. Si bien reconocemos que los criterios pueden ir cambiando, estos cambios deben estar justificados y obedecer a alguna situación razonable en el caso concreto. De ser cambios arbitrarios y sin mayor fundamento, se genera una pérdida en la confianza legítima y se vulnera la seguridad jurídica.
- El último criterio utilizado por la Sala para el análisis de operaciones no reconocidas busca proteger en mayor medida al consumidor, obligando a la entidad financiera a contar con mecanismos efectivos para garantizar un correcto monitoreo de operaciones, poder identificar las posibles transacciones fraudulentas y evitar que estas sean procesadas. De esta manera, evitaría que se produzca un detrimento patrimonial en los consumidores, con lo cual nos encontramos de acuerdo.

CONCLUSIONES

Además de las conclusiones específicas de cada sección, a continuación, presentamos las principales conclusiones generales de este artículo:

a) Sección I: Celeridad de actualización en la normativa del comercio electrónico

   i) La regulación del comercio electrónico en el Perú se encuentra distribuida en diferentes normas, siendo que nuestro ordenamiento busca garantizar, a través de estos diferentes cuerpos normativos, un buen resguardo a los consumidores que realizan compras en línea.

   ii) Las regulaciones responden a necesidades de la sociedad, al ser una sociedad dinámica, resulta razonable que sea necesario que se adapten a los avances de la tecnología y sus nuevos riesgos, es decir, que se encuentren a la vanguardia de los nuevos cambios y actualizaciones en la realidad social.

   iii) La normativa que busca proteger al consumidor en línea existe, no obstante, la tecnología avanza cada día, generando que se encuentre un paso atrás de las necesidades de la sociedad. Si bien vemos intenciones del legislador por dotar de mayor protección a los consumidores y algunas propuestas de modificatoria normativa, consideramos que todavía nos encontramos lejos.

b) Sección II: Implementación de la regulación por las instituciones financieras

   i) Las medidas de seguridad que deben adoptar las instituciones financieras para garantizar las compras realizadas mediante comercio electrónico y canales digitales se rigen por el Reglamento de Tarjetas y el Reglamento de Ciberseguridad, siendo cada vez un mayor estándar de rigurosidad.

   ii) A pesar de que las instituciones financieras se encuentran obligadas a implementar todas las medidas de seguridad establecidas en la normativa vigente, a través de los casos resueltos en el Indecopi, podemos ver que suele haber una implementación parcial, lo cual genera un escenario de vulnerabilidad para los consumidores del cual terceros se aprovechan.

   iii) De la experiencia comparada revisada, podemos ver que, en los casos de operaciones no reconocidas, la carga de la prueba es trasladada a los proveedores, al ser quienes se encuentran en mejor posibilidad de acreditar la validez de las operaciones.

c) Sección III: Incidencia de la regulación en la predictibilidad de las resoluciones

i) El principio de predictibilidad, establecido en nuestra normativa, tiene como objetivo garantizar que los administrados tengan información con claridad y consistencia respecto a los procedimientos y resoluciones emitidas por la Administración a fin de anticipar razonablemente la línea interpretativa de la misma.

ii) Los cambios de criterio, por parte del Indecopi, en el análisis de operaciones no reconocidas han generado diferencias en las resoluciones, afectando la predictibilidad y seguridad jurídica de las mismas.

Por todo lo señalado anteriormente, vemos que la normativa sectorial y las interpretaciones del Indecopi han tratado de encontrarse a la vanguardia de los avances tecnológicos, no obstante, es un proceso en el cual seguimos trabajando para garantizar una reducción de riesgos y de pérdidas económicas para los usuarios.

BIBLIOGRAFÍA

Álvarez, W. (2017). Protección del consumidor financiero: preservando el carácter técnico en la interpretación legal de la autoridad de consumo. Revista de Actualidad Mercantil, (5), pp. 11-21. Recuperado de: http://revistas.pucp.edu.pe/index.php/actualidadmercantil/article/view/19523

Anaya, C. (2012). Riesgos en las transacciones electrónicas bancarias. Una carga que debe ser asumida por la Banca. En Revistas Universidad Externado de Colombia. Recuperado de: https://revistas.uexternado.edu.co/index.php/emerca/article/view/3206/3332

Congreso de la República. (01 de septiembre de 2010). Ley N° 29571. Código de Protección al Consumidor. Lima, Lima, Perú.

Congreso de la República (7 de diciembre de 2021). Comisión de Defensa del Consumidor y Organismos Reguladores de los Servicios Públicos. Recuperado de: https://www2.congreso.gob.pe/Sicr/ApoyComisiones/comision2011.nsf/03actacomxfec/D7F4804A16DDC649052587FE00798073/$FILE/2da.Ext_07.12.21.pdf

Cortés, S. (2024). Los cambios de criterio en protección del consumidor y el principio de predictibilidad, un vistazo al caso de los televisores. En Enfoque Derecho. Recuperado

de: https://enfoquederecho.com/los-cambios-de-criterio-en-proteccion-del-consumidor-y-el-principio-de-predictibilidad-un-vistazo-al-caso-de-los-televisores/

Cuesta, C., Ruesta, M., Tuesta, D., & Urbiola, P. (16 de Julio de 2015). La transformacion digital de la banca. [The digital transformation of banking]. Recuperado de https://url2.cl/IVC58

Federal Trade Comission (1974). Fair Credit Billing Act, 15 U.S.C. § 1601. Recuperado de: https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter41-subchapter1-partD&edition=prelim

Federal Trade Comission (1978). Electronic Fund Transfer Act, 15 U.S.C. § 1693. Recuperado de: https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter41-subchapter6&edition=prelim

Gobierno de Alemania [Bundesministerium der Justiz] (20 de diciembre de 2018) Zahlungsdiensteaufsichtsgesetz (ZAG). BGBl. I Nr. 62. Recuperado de: https://www.gesetze-im-internet.de/zag_2018/

Gobierno de Argentina (14 de noviembre de 1999). Ley 25.065, Boletín Oficial de la República Argentina. Recuperado de: https://www.argentina.gob.ar/normativa/nacional/ley-25065-55556

Gobierno de Chile (23 de abril de 2020). Ley de Fraudes, Ley 21.234. Diario Oficial de la República de Chile. Recuperado de: https://www.bcn.cl/leychile/navegar?i=1145840

Gobierno de Colombia (12 de octubre de 2011). Ley 1480, Diario Oficial No. 48.270. Recuperado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=44306

Gobierno de España (23 de noviembre 2018). Real Decreto-ley 19/2018, de servicios de pago y otras medidas urgentes en materia financiera, BOE núm. 283. Recuperado de: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16036#dd

Gobierno de México. Cargos no reconocidos en tarjeta de débito, se restituirán en dos días hábiles bancarios. (Revisado el 31 de mayo de 2024). Recuperado de: https://www.condusef.gob.mx/?p=contenido&idc=364&idcat=1

Gutierrez, S. (2017). Manual de supervisión de riesgos cibernéticos para juntas corporativas. [Cyber Risk Supervision Manual for Corporate Boards]. Obtenido de https://url2.cl/Bhl3c

INDECOPI (2021). Propuestas para la Protección del Consumidor en el Comercio Electrónico y la seguridad de producto. Recuperado de:

https://www.gob.pe/institucion/indecopi/informes-publicaciones/1783379-propuestas-para-la-proteccion-del-consumidor-en-el-comercio-electronico-y-la-seguridad-de-productos

Morón, J. (2017). Comentarios a la Ley del Procedimiento Administrativo General. Décimo segunda edición. Gaceta Jurídica.

Ramos, F. (2022). Factores de uso y adopción de las billeteras digitales en el Perú. En Newman Business Review, vol 8, núm.1, [pp.83-106].

Rojas, V. (2007). La Uniform Electronic Transactions Act de los Estados Unidos de América. En Revistas Jurídicas UNAM, núm. 119 [pp. 531 - 582] Recuperado de: https://www.scielo.org.mx/pdf/bmdc/v40n119/v40n119a7.pdf

Santana-Soriano, E. & Báez, K. (2022). Ciberespacio y Cibermundo: delimitaciones conceptuales desde el materialismo sistémico. En Ciencia y Sociedad, vol.47, núm.1, [pp.45-57]. Recuperado de: https://www.redalyc.org/journal/870/87070563004/html/

Segura, A. (2017). Ciberseguridad y Derecho Internacional. Revista Española de Derecho Internacional, vol. 69/2, [pp. 291-299]. Recuperado de: https://www.revista-redi.es/redi/article/view/675/665

Superintendencia de Banca, Seguros y AFP (30 de octubre de 2013). Resolución SBS N° 6523-2013. Reglamento de Tarjetas de Crédito y Débito. Recuperado de: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1089323

Superintendencia de Banca, Seguros y AFP (23 de febrero de 2021). Resolución SBS N° 504-2021. Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad […]. Recuperado de: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1277430

Tirado, J. (2021). Protección del consumidor. En Colección “Lo esencial del Derecho” N°53. Lima, Perú: Fondo Editorial PUCP.