El *Phishing* como Delito de Triple Impacto: Marcas, Datos Personales y Afectación del Patrimonio

Phishing as a Triple-Impact Crime: Trademarks, Personal Data and Assets

— Virginia Cervieri* y Carlos Pavón López** —

Resumen

El *phishing* es un delito cibernético que impacta significativamente en tres áreas críticas: las marcas, los datos personales y el patrimonio de los usuarios. Este artículo examina el daño a la reputación y presencia online de las empresas, la vulneración de datos personales de las víctimas, y el perjuicio económico sufrido por los usuarios de Internet. Se analiza cómo las empresas, al expandir su presencia online, se convierten en objetivos vulnerables para los *phishers*, quienes buscan obtener beneficios ilícitos mediante el engaño y la suplantación. La facilidad con la que los delincuentes pueden crear sitios web falsos y engañar a los usuarios para que revelen información confidencial plantea importantes desafíos legales y de seguridad . Se discuten las medidas preventivas y las normativas necesarias para proteger, tanto a las empresas, como a los consumidores en el entorno digital globalizado.

Palabras clave

Phishing, Marcas, Propiedad Intelectual, Cibercrimen, Datos Personales.

Abstract

Phishing is a cybercrime that significantly impacts three critical areas: brands, personal data, and users' wealth. This article examines the damage to companies' reputation and online presence, the breach of personal data of victims, and the economic harm suffered by Internet users. It analyzes how companies, by expanding their online presence, become vulnerable targets for phishers, who seek to obtain illicit benefits through deception and impersonation. The ease with which criminals can create fake websites and deceive users into revealing confidential information presents significant legal and security challenges. Preventive measures and regulations necessary to protect both businesses and consumers in the globalized digital environment are discussed.

Keywords

Phishing, Trademarks, Intellectual Property, Cybercrime, Personal data.

* Doctora en Derecho y Ciencias Sociales y Postgrado en Derecho Comercial, Universidad de la República. Magíster en Propiedad Intelectual. Especialista en derecho de marcas y antipiratería. Agente de Marcas. Socia directora de Cervieri Monsuárez. Presidente de la Cámara de Lucha contra la Piratería y el Contrabando. Presidente del Capítulo Uruguay de la Asociación Mundial de Juristas. Miembro fundador de la Comisión Permanente en defensa de los derechos de Propiedad Intelectual del Ministerio del Interior. Miembro del Comité del Equipo de Lucha contra la Falsificación y el Comercio Paralelo y del Subcomité de Destrucción Sostenible de MARQUES. Fundador de la Fundación Cervieri Monsuárez. Montevideo, Uruguay. E-mail: vcervieri@cmlawyers.com.uy.

** Abogado por la Universidad Nacional de Asunción (2018), Magíster en Propiedad Intelectual e Innovación por la Universidad de San Andrés, Buenos Aires (2021), profesor nivel inicial de la cátedra de Derechos Intelectuales e Industriales de la Facultad de Derecho y Ciencias Jurídicas y Diplomáticas de la Universidad Católica de Asunción, abogado del estudio jurídico Cervieri Monsuárez en su oficina de Asunción, Paraguay. E-mail: cpavon@cmlawyers.com.py presence, become vulnerable targets for phishers, who seek to make illicit profits through deception and impersonation. The ease with which criminals can create fake websites and trick users into revealing sensitive information poses significant legal and security challenges. Preventive measures and regulations needed to protect both businesses and consumers in the globalized digital environment are discussed.

Introducción

El *phishing* es un tipo de fraude cibernético por medio del cual, el atacante busca acceder a los "bienes credenciales" de una persona, para luego efectivizarlos en dinero. Según Kigerl (2017), por "bienes credenciales" se entiende cualquier información personal que pueda ser liquidada monetariamente, como datos de una tarjeta de crédito, información de acceso a cuentas bancarias, contraseñas de cuentas en redes sociales, entre otros.

El sistema se basa principalmente en la utilización de técnicas informáticas por medio de las cuales se logra engañar al usuario, de tal manera que él mismo ingrese a un sitio web que considera, en apariencia, confiable, y por ello ingrese sus "bienes credenciales" con la falsa representación de legitimidad del sitio web. Es allí donde se conjugan las marcas, los datos personales y la afectación del patrimonio del usuario.

Phishing significa en español "pescando", lo que describe coherentemente la técnica utilizada por los cibercriminales para cometer delitos informáticos. Los atacantes crean una falsa representación de un sitio web legítimo para el usuario, utilizando contenido protegido por derechos de propiedad intelectual de una corporación renombrada, de tal manera que, a primera vista, el usuario cree que está ingresando al sitio web oficial de dicha corporación, la cual puede ser desde una entidad financiera hasta un sitio de *e-commerce* de cualquier tipo de marca de productos o servicios.

En la intersección de los derechos afectados, se da una situación no menor en cuanto a la extraterritorialidad, característica de los ciberdelitos, y la territorialidad de la ley aplicable y jurisdicción competente en materia de observancia de los derechos afectados. Esta situación representa un importante desafío en cuanto a la armonización de las normas de cada Estado para hacer frente a los ciberdelitos y, con ello, lograr mejores resultados en la observancia de los derechos.

El término *phishing* fue acuñado en la década de 1990, durante los primeros días de Internet, cuando los atacantes comenzaron a utilizar técnicas de suplantación de identidad para robar contraseñas de usuarios de servicios en línea. A lo largo de los años, las técnicas de *phishing* han evolucionado significativamente, adaptándose a nuevas tecnologías y explotando las vulnerabilidades de los sistemas de seguridad. Actualmente, el *phishing* es una de las formas más comunes y efectivas de cibercrimen, afectando a millones de usuarios y empresas en todo el mundo.

En el contexto actual de ciberseguridad, comprender y combatir el *phishing* es crucial. Con la creciente digitalización de servicios y la dependencia de Internet para actividades cotidianas (desde la banca hasta las comunicaciones), las técnicas de *phishing* se han vuelto más sofisticadas y difíciles de detectar. Las empresas y los individuos deben estar constantemente vigilantes e informados sobre los riesgos asociados con el *phishing* para proteger sus datos y activos.

En los próximos apartados, profundizaremos en las particularidades del derecho marcario y el marco normativo aplicable; la gobernanza de Internet y las normas de comercio electrónico; la responsabilidad de los intermediarios de Internet; el régimen de delegación de nombres de dominio; y, la problemática del *phishing* y la intersección de los regímenes comentados. Con estas profundizaciones, el lector podrá notar la intersección entre dichos regímenes y cómo son abordados desde la perspectiva de la problemática del phishing. Finalmente, compartiremos algunas reflexiones sobre los mecanismos de prevención y combate a la problemática actual.

Derechos Marcarios

El derecho de marcas es una categoría de lo que la doctrina denomina propiedad industrial, junto con las patentes, diseños y modelos industriales, denominaciones de origen e indicaciones geográficas, etc. Por otra parte, tenemos a los derechos de autor y derechos conexos, que son denominados en algunos países como Propiedad Intelectual –principalmente en España—. Sin embargo, a efectos de este trabajo, denominaremos Propiedad Intelectual al conjunto de derechos de autor, derechos conexos y propiedad industrial, englobándolos en dicha denominación.

En materia de propiedad industrial existen dos tratados internacionales que cuentan con amplia adhesión por parte de los Estados. Por un lado, el Convenio de París (Acta de Estocolmo de 1967), que cuenta con la adhesión de 178 Estados (Organización Mundial de la Propiedad Intelectual – OMPI, 2024, *Tratados administrados por la OMPI)*, y, por el otro, el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC) que cuenta con la adhesión de 164 Estados (OMPI, 2024. *Colección de tratados de PI*). Estos instrumentos internacionales

garantizan una armonización mínima en materia de protección y observancia de los derechos de propiedad industrial en los países adheridos a los mismos, pudiendo diferir las respectivas legislaciones nacionales en cuestiones formales o procedimentales, pero manteniendo siempre un marco mínimo de protección acorde a dichos instrumentos.

Se considera que "podrá constituir una marca de fábrica o de comercio cualquier signo o combinación de signos que sean capaces de distinguir los bienes o servicios de una empresa de los de otras empresas" (Acuerdo sobre los ADPIC, Art. 15) [Texto modificado el 23 de enero de 2017]. Esta definición incluye a cualquier tipo de signo, incluyendo letras, números, figuras, colores, la combinación de ellos, figuras en 3D, sonidos, olores y, en general, cualquier signo capaz de ser fijado en un soporte material a los efectos de su registro.

El derecho marcario tiene como fin defender el activo intangible de un productor o comerciante, por un lado, y, por el otro, defender los intereses de los consumidores en cuanto al riesgo de confusión que puedan crear bienes y servicios que compiten en el mercado.

Pensemos a modo de ejemplo en los productos farmacológicos, alimenticios, o cosméticos, que por su naturaleza tienen una incidencia directa en la salud de los consumidores; por tanto, en cuanto un producto de esa naturaleza imite fraudulentamente o falsifique una marca legítima y perteneciente a un tercero, podría potencialmente dañar la salud de los mismos al confundirlos con el afán de obtener un beneficio patrimonial indebido, aprovechándose además del prestigio ajeno y colocando en el mercado productos sin la calidad garantizada por la marca legítima.

Como vemos, las infracciones marcarias afectan tanto al titular legítimo de la marca falsificada o adulterada, así como al consumidor o usuario. En ese sentido, es común que las infracciones marcarias estén relacionadas al contrabando, delitos tributarios, sanitarios, lavado de activos y asociación criminal.

En la mayoría de las legislaciones nacionales es usual que el derecho marcario se adquiera con el certificado de registro otorgado por el Estado, a través del organismo rector en materia de propiedad intelectual. En ese sentido, el registro de la marca atraviesa un proceso administrativo por el cual se analizan los requisitos formales y de fondo, y se establece un plazo para que terceros que podrían verse afectados por la marca solicitada puedan plantear oposiciones. Una vez cumplidos todos los requisitos legales, la marca es concedida mediante el correspondiente certificado de registro, por lo que, desde la fecha de concesión del registro, es que formalmente se adquiere el derecho de propiedad exclusivo sobre dicha marca con todas las facultades acordadas por la ley.

Debemos señalar que el registro es nacional, por lo que el derecho de propiedad otorgado por el Estado se extiende hasta el límite de sus fronteras. Así, en caso de que los productos o servicios sean comercializados en varios países, se deberá solicitar el registro de la marca en tantos países se comercialice y se pretenda obtener la protección marcaria, siguiendo los requisitos formales de cada legislación nacional, los cuales pueden variar en cada jurisdicción. Esta circunstancia difiere respecto al funcionamiento de Internet y del comercio electrónico en general, ya que, por la naturaleza de este, su alcance es global.

La relación entre las marcas y el *phishing* es particularmente problemática porque los phishers se aprovechan de la confianza que las marcas establecen con sus consumidores. La falsificación de una marca no solo daña la reputación de la empresa, sino que también puede poner en riesgo la seguridad y el bienestar de los consumidores que confían en la autenticidad de los productos y servicios ofrecidos bajo dicha marca. Este uso indebido de marcas legítimas para fines fraudulentos es una de las razones por las que la protección de marcas debe ser robusta y estar constantemente actualizada frente a las nuevas tácticas de los ciberdelincuentes.

Datos Personales

El *phishing* es un delito que compromete severamente la protección de los datos personales, afectando directamente los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). Estos derechos, reconocidos en numerosas legislaciones internacionales y nacionales sobre protección de datos, son fundamentales para la protección de la privacidad y la integridad de la información personal de los individuos.

Los derechos ARCO representan un conjunto de facultades que tienen los individuos sobre sus datos personales. El derecho de acceso permite a los individuos conocer qué datos personales están siendo tratados y la finalidad de dicho tratamiento. El derecho de rectificación otorga la capacidad de corregir datos inexactos o incompletos. El derecho

de cancelación permite solicitar la eliminación de datos personales cuando ya no sean necesarios para los fines para los que fueron recabados. Finalmente, el derecho de oposición permite a los individuos negarse al tratamiento de sus datos personales en determinadas circunstancias.

En el contexto del *phishing*, estos derechos se ven gravemente vulnerados. Los ataques de *phishing* suelen implicar la obtención no autorizada de datos personales, lo que viola el derecho de acceso, ya que las víctimas generalmente desconocen que sus datos están siendo recopilados y utilizados por terceros malintencionados. Además, una vez que los datos han sido robados, las víctimas pierden la capacidad de rectificar cualquier inexactitud o de cancelar el tratamiento de sus datos, ya que no tienen control sobre la información una vez que está en manos de los ciberdelincuentes.

La vulneración de los derechos ARCO a través del phishing tiene implicaciones legales significativas. En muchas jurisdicciones, la protección de los datos personales está respaldada por leyes estrictas que imponen obligaciones a los responsables del tratamiento de datos para asegurar la integridad y confidencialidad de la información personal. Estas leyes suelen incluir sanciones severas para aquellos que no protejan adecuadamente los datos personales.

El robo de datos personales mediante *phishing* puede llevar a las víctimas a emprender acciones legales contra las entidades responsables de la seguridad de sus datos, si se considera que estas no han implementado las medidas adecuadas para proteger la información. Esto puede resultar en demandas por daños y perjuicios, así como en sanciones administrativas impuestas por las autoridades de protección de datos.

Uno de los desafíos más complejos en la protección de los datos personales frente al *phishing* es la cuestión de la extraterritorialidad. Dado que el *phishing* es un delito que se lleva a cabo a través de Internet, los delincuentes pueden operar desde cualquier parte del mundo, lo que complica la aplicación de las leyes nacionales de protección de datos. Las víctimas y las autoridades de protección de datos se enfrentan a la difícil tarea de perseguir a los delincuentes en jurisdicciones extranjeras, donde las leyes y los recursos para combatir el cibercrimen pueden variar significativamente.

La cooperación internacional y la armonización de las leyes de protección de datos son esenciales para abordar estos desafíos. Iniciativas como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea han establecido estándares elevados de protección de datos y han incluido disposiciones para la cooperación internacional en la aplicación de la ley. Sin embargo, la implementación efectiva de estas normas a nivel global sigue siendo un desafío significativo.

El cumplimiento de las obligaciones legales de protección de datos personales es crucial para mitigar los riesgos asociados al *phishing*. Las entidades que tratan datos personales deben asegurarse de que están implementando medidas técnicas y organizativas adecuadas para proteger la información contra accesos no autorizados y otras formas de tratamiento ilegal. Esto incluye la adopción de tecnologías de seguridad avanzadas, como la encriptación y la autenticación multifactorial, así como la formación continua del personal en prácticas de ciberseguridad.

Además, las entidades deben ser transparentes en sus políticas de privacidad y proporcionar a los individuos mecanismos claros y accesibles para ejercer sus derechos ARCO. La capacidad de los individuos para acceder a sus datos, corregir inexactitudes, solicitar la eliminación de datos innecesarios y oponerse al tratamiento de sus datos es fundamental para la protección de su privacidad y para la confianza en el tratamiento de sus datos personales.

La intersección de la protección de datos personales con el *phishing* revela la necesidad de una regulación robusta y un enfoque proactivo en la gestión de la seguridad de la información. La capacidad de respuesta y la adaptación rápida a nuevas amenazas cibernéticas son esenciales para proteger los datos personales de los usuarios en un entorno digital cada vez más complejo y peligroso.

Patrimonio del Usuario

El *phishing* tiene un impacto directo en el patrimonio de los usuarios, afectando tanto su estabilidad financiera inmediata como su capacidad para llevar a cabo transacciones económicas de manera segura. Los ataques de *phishing* buscan obtener información financiera sensible, como números de tarjetas de crédito, datos de cuentas bancarias y credenciales de acceso, con el objetivo de realizar transacciones no autorizadas y transferir fondos a cuentas controladas por los delincuentes.

Los delincuentes pueden utilizar la información obtenida para vaciar cuentas bancarias, acumular

deudas en tarjetas de crédito robadas y realizar compras fraudulentas. Estos actos resultan en pérdidas financieras directas que pueden ser difíciles de recuperar. La naturaleza de las transacciones electrónicas hace que sea complicado rastrear y revertir las operaciones fraudulentas, dejando a las víctimas en una situación financiera precaria.

Además, el acceso a la información financiera permite a los atacantes realizar transferencias de fondos a cuentas en el extranjero, donde la recuperación del dinero se vuelve aún más difícil debido a las diferencias en las jurisdicciones legales y la cooperación internacional limitada. Este tipo de fraude no solo afecta a individuos, sino también a empresas que pueden ver comprometida la seguridad de sus transacciones y la confianza de sus clientes.

El *phishing* no solo resulta en pérdidas inmediatas, sino que también puede tener un impacto duradero en la estabilidad financiera de las víctimas. La pérdida de ahorros y el aumento de deudas pueden llevar a dificultades para obtener préstamos, hipotecas y otros servicios financieros en el futuro. La incertidumbre sobre la seguridad de los activos personales puede hacer que las víctimas sean más reacias a participar en actividades económicas, afectando su capacidad de planificación financiera a largo plazo.

La alteración de los historiales crediticios es otro efecto adverso del *phishing*. Cuando los atacantes utilizan la información personal para solicitar créditos y realizar compras a nombre de la víctima, esto puede generar un historial crediticio negativo que afectará la capacidad de la víctima para acceder a financiamiento en el futuro. La resolución de estas disputas crediticias puede ser un proceso largo y complicado, que requiere intervención legal y apoyo financiero.

El *phishing* no solo afecta a las víctimas directas, sino que también tiene implicaciones más amplias para el sistema financiero en su conjunto. La confianza es un componente esencial del ecosistema financiero, y cuando esta confianza se ve alterada, los efectos pueden ser de amplio alcance. La reticencia a realizar transacciones en línea y la desconfianza en las instituciones financieras pueden ralentizar la adopción de nuevas tecnologías y servicios, limitando el crecimiento y la innovación en el sector.

Las instituciones financieras, por su parte, deben enfrentar el desafío de restaurar la confianza de sus clientes después de un incidente de *phishing*. Esto puede requerir inversiones significativas en seguridad y medidas de protección de datos, así como esfuerzos de comunicación para asegurar a los clientes que sus activos están protegidos. La reputación de una institución financiera puede verse gravemente afectada por incidentes de *phishing*, lo que a su vez puede tener un impacto en su posición en el mercado y en su capacidad para atraer y retener clientes.

Por ello, el *phishing* tiene un impacto profundo y multifacético en el patrimonio de los usuarios, afectando tanto su estabilidad financiera inmediata como su confianza a largo plazo en el sistema financiero. Las pérdidas económicas directas, la alteración de los historiales crediticios y los efectos psicológicos y sociales son solo algunas de las consecuencias que enfrentan las víctimas de este tipo de fraude. La capacidad de las instituciones financieras para mitigar estos impactos y restaurar la confianza de los usuarios es crucial para la salud del ecosistema financiero en su conjunto.

Internet y Comercio Electrónico

La gobernanza de Internet no es ejercida en exclusividad por los Estados, siendo la propiedad intelectual uno de los derechos afectados, pero no el único. En una transacción de comercio electrónico se ven afectados al menos tres derechos: datos personales, regulación nacional del comercio electrónico y propiedad intelectual. Podrían verse afectados varios más, pero en general podemos encontrar estos tres derechos afectados en el cien por ciento de las transacciones electrónicas. Esto es así porque quien desee adquirir un bien desde una plataforma de comercio electrónico debe ineludiblemente compartir sus datos personales con la plataforma. Esta, a su vez, debe cumplir con las regulaciones impuestas por el país en donde se encuentran alojados sus *servidores* –o incluso por el mero hecho de ofertar productos en dicho territorio, aunque sus servidores no se encuentren alojados en ese territorio— y porque los productos ofertados en la plataforma requieren indefectiblemente de algún signo distintivo que los diferencie de otros.

En cuanto el derecho marcario se vea afectado en Internet, ya sea por la comercialización de productos que imitan la marca fraudulenta o directamente constituyen falsificaciones, será necesario contar con el registro de marca en el país donde se pretenda ejercer la observancia del derecho. *Ergo*, al aumentar la cantidad de países alcanzados por la plataforma de comercio electrónico, aumenta el riesgo del titular marcario a sufrir infracciones a su

marca, debiendo proceder a solicitar el registro de la misma en cada jurisdicción respectivamente.

El rápido crecimiento del comercio electrónico ha exacerbado estos riesgos, ya que cada vez más consumidores y empresas realizan transacciones a través de plataformas digitales. Esta expansión ha creado un entorno atractivo para los *phishers*, que buscan explotar las vulnerabilidades inherentes al ecosistema del comercio electrónico. Las empresas deben navegar por un complejo marco regulatorio que varía de un país a otro, mientras que los consumidores deben estar constantemente alertas ante posibles intentos de *phishing*.

Además, la interoperabilidad de los sistemas de pago y las plataformas de comercio electrónico ha añadido una capa adicional de complejidad. Las transacciones transfronterizas aumentan la dificultad de rastrear y prevenir el fraude, ya que los ciberdelincuentes pueden aprovechar las discrepancias en las regulaciones y la falta de coordinación entre las autoridades de diferentes países. Esta situación requiere un enfoque colaborativo a nivel internacional para desarrollar estrategias efectivas de prevención y respuesta al *phishing*.

Responsabilidad de los Intermediarios de Internet

La responsabilidad de los intermediarios de Internet ha sido un tema largamente debatido y, en la actualidad, lo sigue siendo. Algunos autores lo han definido en los siguientes términos:

> Por "intermediarios de Internet" nos referimos a aquellos prestadores de servicios de Internet que ofrece: acceso y conectividad a Internet; servicios de alojamiento de contenidos -caching y hosting-; motores de búsqueda; y, plataformas en línea, que permiten la publicación de contenido por los usuarios, tales como redes sociales, aquellas de publicación de noticias y opiniones, de *streaming* y de comercio electrónico (Bustos, Palazzi & Rivero, 2021, p.6).

El debate se ha centrado siempre en el tipo de responsabilidad aplicable a los intermediarios de Internet, ya que en general se encuentran en colisión varios derechos de igual jerarquía, como los derechos de propiedad intelectual, el derecho a la libre expresión, acceso a la información pública y un estándar sumamente relevante en el ámbito de Internet: la neutralidad de la red (Bustos, *et al.,* 2021, p. 117). Cabe mencionar que, lejos de acabar, los debates siguen a medida que el desarrollo y la innovación tecnológica avanzan, aunque a ritmos distintos. Sin embargo, el desafío sigue siendo el de "amalgamar" los derechos afectados, de manera que todos los titulares encuentren un mecanismo eficiente y eficaz que les permita realizar la observancia de sus derechos.

En ese contexto, países y bloques integrados, como la Unión Europea, han legislado la responsabilidad de los intermediarios de Internet en normas de comercio electrónico, como la célebre Directiva 2000/31/CE Del Parlamento Europeo y del Consejo del 8 de junio de 2000 sobre el comercio electrónico, la cual, en su sección cuarta, regula la responsabilidad de los prestadores de servicios intermediarios, adjudicándoles una inmunidad condicionada en cuanto los mismos actúen tomando medidas preventivas o ejecutivas al momento de tener conocimiento de la comisión de ilícitos a través de sus servicios. P ara ello, deberán contar con mecanismos eficaces que permitan a los titulares afectados realizar las denuncias correspondientes al intermediario de Internet.

En materia de propiedad intelectual, y más específicamente en lo relacionado a temas de derechos de autor y derechos conexos, se ha desarrollado la doctrina del puerto seguro o *safe harbour* (Liebowitz, 2018). En resumidas cuentas, la doctrina del puerto seguro plantea que el régimen de inmunidad condicionada o responsabilidad subjetiva utilizados por las normativas en materia de comercio electrónico, debe aplicarse en determinados casos, y solo en cuanto exista efectivamente un mecanismo eficaz por parte del intermediario de Internet para que un titular de derechos de autor pueda ejercer plenamente la observancia de sus derechos respecto a infracciones que ocurran en la plataforma. Existe cierto consenso en que el puerto seguro implica –en cierta medida— una limitación al derecho de autor, por lo que estas inmunidades a los intermediarios de Internet deben evitar un perjuicio injustificado a los titulares de derechos de autor, siguiendo, en cuanto sea posible, la regla de los tres pasos establecida en el artículo 9 del Convenio de Berna para la Protección de las Obras Literarias y Artísticas y en el artículo 13 de los Acuerdos sobre los ADPIC.

En general, la responsabilidad de los intermediarios de Internet se encuentra legislada en las leyes nacionales en materia de comercio electrónico, y es usual que las mismas incluyan una responsabilidad subjetiva o inmunidad condicionada en cuanto los mismos actúen con la debida diligencia para retirar contenidos infractores cuando sean notificados o avisados por parte de los titulares afectados. En

este punto, resulta importante señalar que la norma aplicable será la del país en donde el intermediario tenga su sede o donde se encuentre alojado el servidor.

Nombres de Dominio

Los nombres de dominio son caracteres alfanuméricos que identifican un IP (*Internet P rotocol*), que se constituye enteramente de caracteres numéricos, facilitando así la localización de sitios web. Estos nombres de dominio evitan que utilicemos largos conjuntos numéricos para navegar a través de Internet, ya sea, yendo de sitio en sitio o incluso enviando correos electrónicos (Reed, 2011). El sistema técnico es un poco más detallado y complejo, pero para los efectos del presente ensayo nos limitaremos a indicar el fin principal de los nombres de dominio, el cual, como mencionamos, es facilitar la experiencia del usuario a través de Internet.

Los nombres de dominio no son marcas, es decir, no se rigen por la legislación marcaria. Más bien, los mismos se rigen por políticas y reglas dispuestas por un organismo internacional privado y sin fines de lucro denominado *Corporación de Internet para la Asignación de Nombres y Números (ICANN* por sus siglas en inglés). Este organismo es el encargado de coordinar la delegación de nombres de dominios en todo el mundo, bajo el dominio de nivel superior genérico (*gTLD*) ".com" y los dominios de nivel superior código país (*ccTLD*) ".py, .uy, .bo, .pe, etc.". La delegación de nombres de dominios se realiza a través de registradores que, a su vez, tienen acuerdos con la *ICANN* con relación al cumplimiento de dichas políticas. Los nombres de dominio son otorgados en cuanto no sean idénticos a otro nombre de dominio previamente existente, aunque esa diferencia pueda radicar en un solo caracter. Asimismo, el principio que rige la delegación de nombres de dominio es el de "*first-come, first-served*", o traducido al español "el primero en llegar, el primero en ser servido" (ICANN, 2010).

La resolución de eventuales conflictos que surjan con relación a la delegación de nombres de dominio que puedan afectar derechos de terceros– principalmente marcarios— se rige por un instrumento denominado *Política Uniforme Para La Resolución De Conflictos En Materia De Nombres De Dominio (UDRP* por sus siglas en inglés). Este instrumento es aplicable a todo registrador y adquiriente de nombres de dominio a través de contratos de adhesión, a los cuales indefectiblemente se debe someter quien desee adquirir un nombre de dominio. En esencia, la *UDRP* somete a arbitraje cualquier conflicto derivado del registro y uso de mala fe de nombres de dominio a través de algunos de sus prestadores de servicios de resolución de disputas aprobados por la *ICANN* (ICANN, 2023), siendo probablemente el más conocido el *Centro de Arbitraje y Mediación de la OMPI* (https://www.wipo.int/amc/en/). Cabe resaltar que el demandante del procedimiento de arbitraje administrativo solo puede exigir la cancelación del nombre de dominio o la cesión del mismo a su favor, en cuanto pueda probar que el demandado ha registrado y usado el nombre de dominio en disputa de mala fe, conforme la *UDRP*.

Problemática del Phishing

Hemos mencionado que el phishing se trata de una técnica en la cual se engaña al usuario con falsas representaciones de sitios web confiables, a efectos de obtener sus "bienes credenciales". La intención final del *phisher* es obtener dinero con dichas credenciales, ya sea utilizando los datos de tarjetas de créditos, vendiendo los datos personales recolectados, o incluso utilizando dichos datos para escalar a un ilícito a través de la ingeniería social. Es probable que, en este punto del ensayo, el lector ya pueda presumir cómo interactúan el derecho marcario, los nombres de dominio, y la responsabilidad de los intermediarios de Internet en la problemática del *phishing*.

Desde el punto de vista de la problemática, el daño generado al titular de una marca es principalmente reputacional, representando inclusive un daño con derivaciones económicas. Al momento de enfrentar usos no autorizados de marcas, es imprescindible para el titular tomar las medidas legales en cuanto a la observancia de su derecho, sea contra locales formalmente constituidos o contra sitios web o plataformas en Internet. En cuanto al daño emergente, podemos mencionar que estas acciones representan un costo para el titular, quien debe incurrir en honorarios legales y gastos logísticos para luchar contra las infracciones, a lo cual se debe sumar el lucro cesante, en tanto el sitio atraiga clientela actual, y la pérdida de chance en cuanto pueda atraer clientes potenciales del titular marcario. Lo precitado no obsta a que se sumen otros rubros indemnizatorios atendiendo a las particularidades del daño, pero al menos tenemos un panorama general del daño causado por el *phishing* al titular de una marca.

Si lo analizamos desde la perspectiva del consumidor, debemos recordar que el derecho marca-

rio asimismo protege al consumidor en cuanto al riesgo de confusión que pudieran ocasionar signos distintivos que compiten en el mercado. Dependiendo del producto o servicio del que se trate, el cuidado respecto a evitar la confusión marcaria puede atenuarse o agudizarse, pero el principio de evitar cualquier tipo de confusión es una máxima del derecho de marcas. En ese orden de ideas, imaginemos un consumidor de productos cosméticos que es víctima de *phishing*; en la inteligencia del consumidor, el mismo es atraído a un sitio espúreo por la falsa representación de una marca famosa y confiable para el consumidor, quien es engañado entonces para compartir sus datos personales. Eventualmente, cuando la promesa no sea cumplida, o cuando el usuario tome conocimiento de que ha sido víctima de un delito cibernético, verá menguado su ánimo consumidor respecto a la marca utilizada para el *phishing* en su contra, consumándose así el daño a la reputación de la marca con efectos directos y tangibles.

En este punto, podemos dimensionar el daño causado por un delito de triple impacto: por un lado, al titular de una marca; por otra parte, al usuario consumidor; y, en tercera instancia, una afectación transversal, que es el patrimonio. Cualquier afectación a la reputación marcaria y a los datos personales deriva en un perjuicio patrimonial para las víctimas. Ya hemos mencionado cómo se vería afectado un titular marcario en cuanto al daño causado; sin embargo, el usuario infractor se encuentra igualmente –o incluso más— vulnerable respecto a la afectación de su patrimonio personal.

Aunque no es usual encontrar en nuestras legislaciones latinoamericanas una tipificación concreta del *phishing* como delito, nos encontramos en condiciones de sostener que, conforme la dogmática penal, estamos frente a un ilícito que cumple con los elementos objetivos y subjetivos del tipo penal de estafa. Debido a ello, varios países han incluido en sus respectivas normas penales los delitos informáticos, o como también lo denomina la doctrina, cometidos por medios informáticos.

Mecanismos de Prevención y Combate al Phishing

Hemos dicho que el *phishing* se basa en el engaño para obtener los bienes credenciales del usuario; por tanto, en cuanto la representación del engaño sea lo más similar posible a una situación legítima, esta tendrá mayor posibilidad de éxito. Por ello, las acciones preventivas deben darse en varios frentes: por un lado, el registro de las marcas tal y como son utilizadas y en las clases correspondientes a los bienes y servicios ofertados en el mercado; por otro , el registro de nombres de dominio en al menos los dominios de nivel superior genérico (*gTLD*) y en los de nivel superior código país (*ccTLD*) –en los países donde se tenga presencia actual o potencial—; y por último, pero no menos importante, respetar la imagen corporativa en los diseños y comunicación de la marca, de manera que el consumidor pueda encontrar elementos diferenciadores para identificar eventuales casos de *phishing*.

En cuanto a las acciones combativas, estas difieren según la estrategia decidida por el titular, pero podemos englobarlas principalmente en acciones legales, con base en la legislación marcaria y de comercio electrónico , sin desconocer la potencial aplicación de la legislación en materia de derecho de autor y de datos personales. Si bien no existe una armonización normativa en materia de protección de datos personales en nuestros países, usualmente las plataformas de servicios de *hosting* operan en países que cuentan con una protección adecuada en la materia, por lo que el cumplimiento se hace obligatorio a los efectos de evitar sanciones económicas.

En general, y como hemos mencionado en párrafos precedentes, los intermediarios de Internet, incluidos los servicios de *hosting*, se encuentran sujetos a regulaciones en materia de responsabilidad, por lo que, dependiendo de la normativa en materia de comercio electrónico del país donde estos se encuentren físicamente alojados, tendrán que dar cumplimiento a ciertos requisitos para mitigar su responsabilidad en casos de delitos por medios informáticos y acogerse a las previsiones del puerto seguro o *safe harbour*. Por ello , una acción eficaz suele ser realizar una denuncia a la plataforma de hosting donde se aloje el sitio web utilizado para el *phishing*, solicitando la baja inmediata del sitio en virtud de infracciones marcarias o de derechos de autor.

Conclusiones

Como delito de triple impacto, el *phishing* es una práctica en constante evolución y perfeccionamiento, por lo que requiere que las víctimas y titulares de marcas se mantengan informados y actualizados respecto a las medidas preventivas para evitar ser víctima de este flagelo.

Hemos visto que la complejidad de la gobernanza en Internet plantea desafíos importantes en mate-

ria de armonización de normas que hagan frente a los delitos cometidos por medios informáticos, en particular a los ilícitos en el entorno digital, de manera que las mismas logren disuadir a los infractores en la comisión del delito.

Notamos la relevancia de las normas en materia de comercio electrónico en cuanto a la imputación de responsabilidad a los intermediarios de Internet en casos de ilícitos cometidos a través de la utilización de sus servicios, y en la eficacia de dichas normas en cuanto a lograr resultados en el combate al *phishing* y otros ilícitos.

De igual manera, se ha dicho que tomar medidas preventivas en el registro de marcas y nombres de dominio, así como en las acciones de comunicación corporativa, ayudan a mitigar riesgos en favor de los titulares y consumidores, ya que la información es un arma de prevención importante en este tipo de ilícitos.

El *phishing* no es solo una amenaza actual, sino una que seguirá evolucionando a medida que la tecnología avanza. Los ciberdelincuentes continuarán desarrollando nuevas estrategias para engañar a las víctimas, lo que hace esencial que las empresas, los legisladores y los usuarios se mantengan proactivos en la adopción de medidas de seguridad. La colaboración internacional y la actualización constante de las normativas de ciberseguridad serán claves para reducir el impacto de estos ataques en el futuro.

Es imperativo que tanto las empresas como los individuos tomen un rol activo en la lucha contra el *phishing*. Las empresas deben invertir en tecnologías de seguridad avanzadas y en la formación continua de sus empleados, mientras que los usuarios deben estar informados y alertas ante posibles intentos de *phishing*. Solo a través de un esfuerzo conjunto podremos reducir significativamente el impacto de este tipo de cibercrimen y proteger nuestros datos y activos en el entorno digital.

Referencias

Bustos, G., Palazzi, P. y Rivero, S. (2021). *Responsabilidad de intermediarios de* Internet *en América Latina: Hacia una regulación inteligente de la economía digital [Archivo PDF].* https://shorturl.at/Cpy4p

Internet Corporation for Assigned Names and Numbers. (9 de febrero de 2010). *ICANN* Registry *Request Service [Archivo PDF]. https://www.icann.org/en/system/files/files/afilias-request-09feb10-en.pdf*

Internet Corporation for Assigned Names and Numbers. (s.f.). *List of Approved Dispute Resolution Service Providers. https://www.icann.org/resources/pages/providers-6d-2012-02-25-en*

Kigerl, A. (2017). Malicious Spam: The impact of prosecuting spammers on fraud and malware contained in email spam. En T. Saadawi & J. D. Colwell (Eds.), *Cyber Infrastructure Protection Volume III* (pp. 63–100). Strategic Studies Institute, US Army War College. http://www.jstor.org/stable/resrep11978.7

Liebowitz, S. (2018). *Economic analysis of safe harbour provisions.* [Archivo PDF]. https://www.cisac.org/es/servicios/informes-y-estudios/el-economic-analysis-safeharbour-provisions

Organización Mundial de la Propiedad Intelectual .(s.f.). *Tratados administrados por la OMPI*. https://www.wipo.int/wipolex/es/treaties/ShowResults?search_what=A&act_id=31

Organización Mundial de la Propiedad Intelectual .(s.f.). *Colección de tratados de PI. https://www.wipo.int/wipolex/es/treaties/parties/231*

Reed, S. R. (2011). Sensible Agnosticism: An Updated Approach To Domain-Name Trademark Infringement. *Duke Law Journal*, *61* (1), 211–250. http://www.jstor.org/stable/23034815