

LA EFICACIA DE LA APLICACIÓN DE LA PENA DE CIBERDELITOS PRACTICADOS MEDIANTE EL USO DE IDENTIDAD FALSA EN INTERNET*

*Andréa Arruda Vaz***

*Aléxia Ketlyn Soares dos Santos****

*Pedro de Oliveira Santos Junior*****

Resumen: El principal objetivo y propósito de este artículo científico es debatir sobre la ciberdelincuencia, más concretamente en relación con la identidad falsa para cometer delitos. En primer lugar se abordará el concepto principal de ciberdelincuencia y sus peculiaridades, así como su *modus operandi* y procedimiento de investigación. A continuación, se abordará el delito de falsedad de identidad en internet, sus características, sus penas y los medios utilizados para su represión. A continuación, se argumentará sobre la eficacia de las penas para los ciberdelitos y si son capaces de inhibir el delito, especialmente en relación con la falsa identidad, ya que la pena es baja y los delitos son habituales.

Palabras clave: ciberdelincuencia, ingeniería social, delito, falsa identidad, punibilidad.

* Fecha de recepción: 19 de noviembre de 2024. Fecha de aceptación: 27 de septiembre de 2025. Para citar el artículo: Arruda Vaz, Andréa; Soares dos Santos, Aléxia Ketlyn y de Oliveira Santos Junior, Pedro, "La eficacia de la aplicación de la pena de ciberdelitos practicados mediante el uso de identidad falsa en internet", *Revista Derecho Penal y Criminología*, vol. 47, n.º 123 (julio-diciembre de 2026), pp. 119-136.
DOI: <https://doi.org/10.18601/01210483.v47n123.06>

THE EFFICACY OF PENALTY ENFORCEMENT FOR CYBERCRIMES COMMITTED USING FALSE IDENTITY ON THE INTERNET

Abstract: This scientific article primarily aims to address cybercrime, specifically concerning the use of false identity to commit crimes. Firstly, the principal concept of cybercrime and its particularities will be discussed, along with its modus operandi and investigative procedures. Subsequently, this article will cover the crime of identity falsification on the internet, its characteristics, penalties, and the means used for its enforcement. Thus, it will explore the effectiveness of sentencing in cybercrime cases and whether such penalties are capable of deterring criminal acts, particularly in relation to false identity, given that its penalty is low and the crimes are frequent.

Keywords: cybercrime, social engineering, crime, false identity, punishment.

INTRODUCCIÓN

El tema que nos ocupa se establece en el ámbito del derecho penal, más concretamente en la lucha contra la comisión de delitos a través del uso de internet. En este

** Doctora en Derecho por el Programa de Posgrado Stricto Sensu en Derechos Fundamentales y Democracia del Centro Universitario Autónomo de Brasil - UniBrasil/PR, máster en Derecho por el Centro Universitario de Brasil - UniBrasil. Posgrado en Derecho Público, con énfasis en Derecho Administrativo por la Universidade Cândido Mendes. Posgrado en Derecho y Proceso Laboral por la Pontificia Universidad Católica de Paraná. Especialista en Educación y Metodologías de Enseñanza por Facear Araucária. Licenciada en Derecho por la Faculdade Dom Bosco. Directora de la Comisión de Derecho del Trabajo de la OAB/PR -Subsección Araucária-, período 2016-2018. Profesora invitada en los cursos de posgrado en Gestión Administrativa y Financiera y Gestión de Recursos Humanos en el centro universitario Uninter. Profesora invitada en el curso de posgrado en Derechos Humanos de la PUC/PR. Profesora invitada en el curso de posgrado en Derecho y Proceso Laboral en la Universidad Católica de Santa Catarina. Profesora invitada en el curso de posgrado en Derecho y Proceso Laboral de la Academia Brasileña de Derecho Constitucional. Profesora de las asignaturas de Historia del Derecho, Teoría General del Proceso, Derecho y Proceso del Trabajo y Derecho Constitucional en el centro universitario UniFesp/Uniensino. Abogada en las áreas de Derecho y Procedimiento Laboral, Derecho Colectivo del Trabajo, Derecho Constitucional, Derecho Civil, Derecho Penal y Derecho Administrativo, incluido el Derecho Administrativo Disciplinario. Autora de diversos artículos (en revistas nacionales e internacionales), capítulos de libros y del libro *Derecho fundamental de libertad sindical en Brasil y tratados de derechos humanos*. ORCID: 0000-0001-9177-2740. Correo electrónico: andrea@andreavaz.adv.br.

*** Licenciada del curso de Derecho en el Centro Universitario de Educación, Ciencia y Tecnología de Paraná - Uniensino. ORCID: 0009-0000-9482-063X. Correo: alexiaketylnsantos@gmail.com.

**** Graduado en Ciencias Jurídicas por la Universidad Tuiuti de Paraná. Posgrado en Derecho Penal por la Unicuritiba. Titular de Oliveira Santos Advogados. Ejercicio de la Abogacía Penal. Exdirector operativo de la Asociación Paranaense de Abogados Penalistas. Profesor de Derecho Penal en Facultades Anchieta, conferencista. ORCID: 0009-0005-0631-9519. Correo electrónico: posjr2002@yahoo.com.br.

sentido, la discusión que el artículo pondrá sobre la mesa es la eficacia de las penas impuestas cuando se es condenado por la comisión de un ciberdelito mediante el uso de una identidad falsa en internet. Así, la pregunta es: ¿Son suficientes las penas impuestas por este delito para inhibir su comisión? Si la pena es leve, ¿habría necesidad de ajustar la condena hasta el punto de que este delito dejara de ser rentable, inhibiendo la conducta delictiva?

Esta investigación se centrará específicamente en los ciberdelitos cometidos mediante el uso de identidades falsas exclusivamente en internet, teniendo en cuenta la expansión y democratización de los medios tecnológicos, que facilitan la actividad delictiva en la actualidad.

La justificación de este artículo es plantear requerimientos para tratar de reducir la recurrencia de delitos cometidos en internet mediante el uso de identidad falsa, ya que se observa un gran volumen de este tipo de delitos en la sociedad, lo cual hace habitual que las víctimas se quejen de este comportamiento.

El objetivo general de este trabajo es abordar la problemática de los delitos cometidos en internet, específicamente el uso de identidad falsa. Así, la pregunta que responder será si las penas aplicadas a este tipo de delitos serían suficientes para inhibir esta práctica delictiva, ya que, al tratarse de penas leves, se puede analizar que existe, de esta forma, una gran reincidencia en la realización de este delito. A continuación se estudiarán posibles medidas para evitar que los ciberdelitos cometidos en internet mediante el uso de identidad falsa se conviertan en algo tan habitual.

Partiendo del objetivo general de este artículo, sus principales objetivos serán: discutir el concepto de *ciberdelincuencia*, cómo funciona el delito de falsedad de identidad a través de internet, es decir, cómo se aplican y acercan los autores a las víctimas para llevar a cabo este delito, cómo se lleva a cabo el procedimiento de investigación para llegar a la persona que comete esta infracción penal y, por último, la aplicabilidad de la pena para castigar estos delitos, si son suficientes o no. La base metodológica del artículo será la investigación bibliográfica, basada en la lectura de libros, artículos, textos legales y jurisprudencia. La investigación se clasificará en cualitativa y cuantitativa.

Por lo tanto, este artículo comenzará discutiendo la práctica del cibercrimen en Brasil, conceptualizándolo y destacando sus diferencias con las conductas que sólo se consideran invasivas. A continuación, desarrollará el concepto y el propio delito de falsa identidad en internet, su penalización, sus medios y sus principales características. Por último, se abordará la eficacia de la aplicación de la pena para los ciberdelitos cometidos en Brasil y especialmente en lo que se refiere al delito de falsa identidad para la aplicación de estafas y otros delitos.

I. LA PRÁCTICA DE LA CIBERDELINCUENCIA EN BRASIL

En primer lugar, este artículo analizará el concepto primario de *ciberdelincuencia*, que, según Wendt, se utiliza para definir los delitos cometidos contra o a través de ordenadores. Es decir, dispositivos informáticos en general (Wendt, 2013; Jorge, 2013). Es posible entender que el cibercrimen involucra conductas que son consideradas invasivas y que sólo requieren un computador para ser practicadas, dividiéndose en cibercrimen propiamente dicho, que es un delito, y acciones que son consideradas sólo lesivas, eliminando así la punibilidad por no ser consideradas actos delictivos (Wendt, 2013; Jorge, 2013).

Wendt, en su libro, dice que

“Acciones lesivas atípicas” son aquellas conductas cometidas en/a través de la World Wide Web que causan algún inconveniente y/o daño a la víctima, pero no existe una previsión penal, es decir, el individuo causa algún problema a la víctima, pero no puede ser castigado en el ámbito penal debido a la inexistencia de una norma penal para ello (Wendt, 2013; Jorge, 2013).

La ciberdelincuencia también puede ser caracterizada y entendida cuando determinadas conductas, que se realizan a través de medios tecnológicos, son consideradas delitos. Así, el cibercrimen es la conducta utilizada a través de recursos digitales para llevar a cabo el crimen (Bomfati, 2020; Junior, 2020). Con esto, es posible darse cuenta de que incluso crímenes considerados convencionales serían factibles de ser cometidos en un ambiente virtual, debido a la facilidad y evolución en que se encuentra la población hoy en día.

Además, Bomfati y Junior afirman que hoy en día es posible encontrar ciertos tipos de delincuentes más sofisticados que, en lugar de colarse en tu cartera, introducen un simple virus en los ordenadores, capturan las contraseñas bancarias y retiran todo tu dinero del banco (Bomfati, 2020; Junior, 2020). Sin lugar a dudas, está claro que la población en general es vulnerable a este tipo de delitos virtuales, debido a la facilidad que se encuentra en este entorno.

Por ello, es importante destacar las clasificaciones de la ciberdelincuencia, que son: la ciberdelincuencia abierta y la ciberdelincuencia exclusiva. Cuando se trata de ciberdelincuencia abierta, cabe citar como ejemplos los delitos contra el honor, las amenazas, la pornografía infantil, la malversación, el robo por estafa, el racismo, etc.

Por otro lado, el pirateo informático, la interceptación telemática ilegal y los delitos contra las urnas electrónicas serían ejemplos de delitos exclusivamente cibernéticos. Según Cordeiro, los delitos más comunes cometidos en el entorno virtual serían la apropiación de datos, o incluso los casos de clonación de cuentas de redes sociales,

en los que los estafadores se hacen pasar por las víctimas para tomar los datos sensibles de las personas y luego exponerlos en las redes sociales (Cordeiro, 2022).

También hay que señalar que, cuando se trata de ciberdelincuencia, los delincuentes utilizan medios y estrategias avanzados para completar el acto malicioso. Wendt y Jorge traen a colación el concepto de *ingeniería social*, uno de los medios utilizados por los estafadores, que, según ellos,

Es la utilización de un conjunto de técnicas encaminadas a engañar a la víctima haciéndole creer la información facilitada y convenciéndola para que facilite datos personales en los que el delincuente tiene interés o para realizar alguna tarea y/o solicitud (Wendt, 2012; Jorge, 2012).

Como tal, está claro que estos delincuentes utilizan las emociones y la vulnerabilidad de las víctimas para llevar a cabo el acto delictivo. Sin embargo, es posible ver que, además de los medios utilizados anteriormente, también existe el término “phishing scam”, que significa pescar información de las personas, o mejor dicho, obtener información de forma simple. Wendt y Jorge citan que

Al principio, la palabra *phishing* se utilizaba para definir el fraude que consistía en enviar un correo electrónico no solicitado a la víctima, a la que se animaba a acceder a sitios *web* fraudulentos. Los sitios tenían como objetivo permitir el acceso a la información electrónica de la persona, como números de cuentas bancarias, números de tarjetas de crédito, contraseñas, correos electrónicos y otra información personal (Wendt, 2012; Jorge, 2012).

Por ello, es evidente la exposición e inteligencia que tienen los falsificadores para cometer ilícitos en las redes sociales, ya que en el mundo actual la fluidez en internet ha ido en aumento, así como la aptitud de las personas que lo manejan. Bertholdi indica que

El aumento significativo de la ciberdelincuencia en nuestro país tiene dos causas básicas: la primera está directamente relacionada con el hecho de que la *web* permite a los delincuentes tener libre acceso a un número significativo de víctimas, y la gran escalabilidad de esta actividad delictiva es innegable, especialmente en una nación que se preocupa poco por la educación básica sobre el uso de internet y la seguridad; luego están las técnicas utilizadas y los *crackers* reclutados para ocultar las actividades de los delincuentes, que son extremadamente complejas y rara vez encuentran resistencia en las frágiles estructuras de investigación y judiciales de Brasil (Bertholdi, 2020).

Está claro que las causas del aumento de la ciberdelincuencia están directamente relacionadas con la falta de información de la víctima, así como con la astucia y especialización de los delincuentes.

Siguiendo con el tema de la ciberdelincuencia, es necesario darse cuenta de que se rige por una legislación y conceptos específicos, por lo cual presenta diversas características y peculiaridades. Según Bomfati y Junior,

En cuanto a los delitos virtuales, aún estamos avanzando hacia una legislación específica, en la que existen varios conceptos a entender, como el delito virtual propio, impropio, mixto, mediato o indirecto, cuyas definiciones cambian en la medida en que el delincuente utilice tal o cual medio electrónico para realizar el hecho ilícito, o incluso utilice un medio informático para realizar un delito no informático, como el delito de hurto (Bomfati, 2020; Junior, 2020).

Por último, es importante y esencial discutir qué y cómo se lleva a cabo el proceso de investigación aplicado a la ciberdelincuencia. Cabe destacar que para una investigación completa es necesario que haya una fase inicial, una fase técnica y, por último, una fase consecuente, propiamente policial (Wendt y Jorge, 2012, p. 52). En este sentido, es importante destacar el siguiente supuesto, que Wendt y Jorge mencionan:

En la fase técnica de los delitos cometidos a través de internet se realizan y analizan las siguientes tareas y/o informaciones para localizar el ordenador que fue utilizado para la acción delictiva: análisis de la información narrada por la víctima y comprensión de lo ocurrido en internet; orientación a las víctimas para preservar el material probatorio del delito y su protección virtual; recogida inicial de pruebas en el entorno virtual; investigación inicial sobre los datos disponibles en la World Wide Web sobre probables autores, origen de correos electrónicos, registro y alojamiento de dominios; formalización de un informe o certificado de las pruebas recogidas e investigación preliminar; representación ante el Poder Judicial para emitir autorización judicial por infracciones de datos, conexión o acceso. También se pueden solicitar datos de registro a los proveedores de contenidos; analizar la información facilitada por los proveedores de conexión y/o de contenidos (Wendt, 2012; Jorge, 2012).

Así, de lo mencionado por los autores se desprende que todo comienza con el atestado policial y la denuncia de la víctima en una comisaría, con la necesidad de que la víctima conserve el material de apoyo a efectos de investigación. A continuación, los investigadores y el jefe de policía recogen y analizan las pruebas, y después se redacta un informe que se remite al poder judicial para que autorice la violación de datos y el acceso a estos.

A continuación, Wendt y Jorge hablan de la fase técnica, que según ellos es el momento en que se analiza la información recibida de los proveedores para ver si necesitan más datos. Se menciona el IP (Internet Protocol). Si es necesario, hay que hacer un nuevo informe al Poder Judicial. Por otro lado, si todo es correcto, una vez

identificado y localizado el ordenador conectado y que el delincuente ha accedido a internet, se pasa a la fase de campo propiamente dicha (Wendt, 2012; Jorge, 2012).

El delito de falsedad de identidad en internet, pena, medios y principales características

Este artículo se basará en el delito de falsedad de identidad practicado en internet, según los artículos 307 y 308 del Código Penal:

Art. 307. Atribuirse a sí mismo o a un tercero una identidad falsa con el fin de obtener una ventaja para sí mismo o para otros, o de causar daño a terceros: Pena - detención, de tres meses a un año, o multa, si el hecho no constituye un elemento de un delito más grave (Brasil, 1940).

Art. 308. Utilizar, como propio, pasaporte, carné de elector, carné de reserva o cualquier otro documento de identidad de otra persona, o darlo a otra persona para que utilice un documento de esta naturaleza, propio o de un tercero: Pena - detención, de cuatro meses a dos años, y multa, si el hecho no constituye un elemento de un delito más grave (Brasil, 1940).

El artículo 307 establece que la pena para este tipo de delito sería de privación de libertad de tres meses a un año, o multa si el hecho no constituye un elemento de mayor gravedad; es decir, del artículo anterior se desprende que la pena es inferior a un año y puede cambiarse por multa. Por lo tanto, para un individuo que cometa este tipo de delito sería expresamente pacífico, ya que podría cambiar la pena por una multa y volver a cometer el delito de otra manera.

Por todo ello, se entiende que la intención de quienes cometen el delito de falsedad de identidad es conseguir ventajas indebidas. Es decir, utilizar una identidad falsa para aplicar estafas a través de las redes sociales. Ya sea para extorsionar a las víctimas, difamarlas como si fueran otra persona, suplantar la identidad de familiares para obtener ventajas económicas, entre otras. Por otro lado, De Castro y Zaganelli afirman que la identidad falsa o “catfishing” se utilizaría para describir el acto de crear una identidad falsa o sustraerse de otra persona con el fin de engañar a individuos en línea (De Castro, 2022; Zaganelli, 2022).

Según Silva,

Cabe señalar que la creación de perfiles falsos en las redes sociales sólo se considera conducta delictiva si se basa en una persona real. En el caso de un perfil burdamente falso, en el que se utilicen fotos de objetos o paisajes, por ejemplo, no es necesario hablar de falsa identidad. Aquí tenemos la mera intención de preservar la identidad del usuario en las redes sociales (Silva, 2022).

Además, es necesario analizar algunos de los tipos de perfiles falsos que existen en el mundo virtual y cuáles pueden ser sus características, para que los usuarios puedan ser conscientes de los hechos. Hay que tener en cuenta, de entrada, que cada perfil creado de forma diferente tendrá unas motivaciones específicas para llegar a unos objetivos distintos. Arroyo presenta algunas características y diferentes tipos de perfiles. Según él,

Las principales características del perfil falso “clásico” son la falta de información básica como nombre de usuario, imagen de perfil o foto de portada, así como un bajo número de seguidores –o amigos– y la reciente creación del perfil (Arroyo, 2019).

En otras palabras, un perfil totalmente desprovisto de estipulaciones, con el fin de dificultar la identificación de la persona que hay detrás del usuario. Como resultado, un perfil de este tipo puede empezar a difamar a las personas y amenazarlas. También existe el perfil plagiador de identidad, que según Arroyo son falsificaciones de identidad que están presentes en las redes sociales. Sus principales características están relacionadas con copias originales de la información de las víctimas, como su nombre, foto, lugar de trabajo y ciudad (Arroyo, 2019).

También hay casos en los que se aplica una identidad falsa mediante documentos falsos para cometer el delito de malversación. En este caso, es importante analizar el caso concreto para tener en cuenta qué delito prevalecerá.

En este punto, se menciona el artículo 171 del Código Penal, más concretamente sus párrafos 2.º y 3.º, ya que ambos abordan específicamente el fraude, la utilización de una identidad falsa en internet para obtener ventajas ilícitas.

§ Apartado 2-A. La pena es de prisión de 4 (cuatro) a 8 (ocho) años y multa si el fraude se comete utilizando información proporcionada por la víctima o por un tercero engañado a través de redes sociales, contactos telefónicos o envío de correos electrónicos fraudulentos, o por cualquier otro medio fraudulento similar (Brasil, 1940).

§ Párrafo 2B. La pena prevista en el § 2-A de este artículo, teniendo en cuenta la importancia del resultado grave, se aumenta de 1/3 (un tercio) a 2/3 (dos tercios) si el delito se comete utilizando un servidor mantenido fuera del territorio nacional (Brasil, 1940).

§ Párrafo 3. La pena se aumenta en un tercio si el delito se comete en perjuicio de una entidad de derecho público o de un instituto de economía popular, de asistencia social o de beneficencia (Brasil 1940).

Así, en estos casos concretos se observa que las penas impuestas tienden a aumentar hasta en 1/3 o 2/3. Sin embargo, incluso con este agravante, se observa que el delito es habitual hasta el punto de considerarse “algo que vale la pena” para los delincuentes.

Para Steffens, Groth y Balbinot

El delito de falsedad de identidad admite tentativa, sin embargo, sólo en los casos en que la identidad se atribuye por escrito, debido a que el delito es plurisubsistente Si se produce verbalmente, no es posible que haya tentativa, ya que el delito es insubsistente (Steffens, 2019; Groth, 2019; Balbinot, 2019).

Dicho esto, en el escenario de la falsedad de identidad en el entorno digital, este delito es muy recurrente debido a que es completamente fácil de cometer, no requiere ningún esfuerzo. Una de las estafas más recurrentes tiene que ver con las redes sociales Instagram, Facebook y WhatsApp, donde los delincuentes se hacen pasar por amigos cercanos y familiares con el fin de obtener ventajas indebidas.

Por ejemplo: el individuo “X” encuentra un perfil oficial abierto en la plataforma Instagram con varias fotos. El falsificador aprovecha entonces la situación, toma fotos y crea otro perfil en Instagram, cambiando únicamente el tipo en el que está escrito el nombre de la persona. A continuación, el falsificador envía invitaciones a todos los amigos reales de la víctima, momento en el que comienza la estafa. Hay otros casos en los que el individuo crea maliciosamente un enlace dentro de estos perfiles falsos que lleva a páginas *web* de contenido sexual, dando a entender que la víctima es la verdadera propietaria. Lo mismo ocurre también en WhatsApp: el individuo envía mensajes a conocidos cercanos a las víctimas, cambiando únicamente el número. Comienza con historias sobre la necesidad de dinero para reparar teléfonos móviles y cosas por el estilo. Llegados a este punto, la persona, creyendo que realmente se trata de su amigo o familiar, acaba realizando varias transferencias bancarias a través de Pix.

En estos ejemplos, se puede observar que la creación del perfil falso fue con el fin de aplicar una estafa, es decir, la identidad falsa se convirtió en un delito penal; con el fin de cometer fraude y para difamar a las personas mediante enlaces a sitios para adultos. Así, la ley establece:

Art. 171. Obtener, para sí o para otros, ventaja ilícita, en perjuicio ajeno, induciendo o manteniendo a alguien en error, por artificio, ardid o cualquier otro medio fraudulento: Pena - prisión, de uno a cinco años, y multa, de quinientos mil réis a diez contos de réis (Brasil, 1940).

Art. 139. Difamar a alguien, imputándole un hecho que ofenda su reputación: Pena - detención, de tres meses a un año, y multa (Brasil, 1940).

En los casos ejemplificados anteriormente se observa que, además del hecho y delito de falsedad de identidad, el delincuente se estaría enfrentando a otras penas, como las recogidas en los artículos 171 y 139 del Código Penal.

II. LA EFICACIA DE LAS PENAS EN LAS CONDENAS POR CIBERDELINCUENCIA EN BRASIL

Llegados a este punto, este artículo abordará la aplicación de penas para los delitos informáticos. El derecho se entiende como instrumento para resolver conflictos en la sociedad, por lo cual es necesario mantenerse al día con los cambios a medida que cambia la humanidad, especialmente cuando se trata de internet y los delitos virtuales, que están en constante cambio.

De Castro y Zaganelli afirman que

El Derecho es un producto cultural y una herramienta de resolución de conflictos que debe estar en consonancia con la sociedad que regula. Por tanto, debe actualizarse en función de los cambios sociales. Sin embargo, esta no es la realidad práctica que se constata al analizar la relación entre el Derecho e Internet (De Castro, 2020; Zaganelli, 2020).

Así, el ordenamiento jurídico cuenta con tres leyes que se caracterizarían como las principales cuando se trata del entorno virtual: Ley n.º 12.695/2014, Ley n.º 12.737/2012 y Ley n.º 12.735/2012, todas con la intención de intentar inhibir las prácticas delictivas; sin embargo, esto no es lo que vemos en la práctica.

La Ley 12.737/2012, conocida como la Ley Carolina Dieckmann, fue la primera ley brasileña para tratar y castigar los delitos cibernéticos. En pocas palabras, esta ley fue creada después de que la actriz Ana Carolina sufriera el robo de fotos íntimas de su dispositivo a través de un hackeo a manos de delincuentes que comenzaron a extorsionarla, y luego publicaron dichas fotos (G1, 2012). Véase el artículo 154-A, *caput*, añadido al Código Penal:

Art. 154-A. Penetrar en dispositivo informático ajeno, conectado o no a una red informática, con el fin de obtener, alterar o destruir datos o informaciones sin autorización expresa o tácita del usuario del dispositivo, o instalar vulnerabilidades para obtener una ventaja ilícita: Pena - prisión, de 1 (uno) a 4 (cuatro) años, y multa (Brasil, 2021).

La Ley 12.695/2014, o ley Marco Civil da Internet, trata de la posibilidad de “construir derechos de los ciudadanos dentro de esta red, es decir, no se trata sólo de delitos de internet, sino de todo lo que necesita ser discutido y regulado en todas las áreas donde la tecnología de la información está presente” (Bomfati, 2020; Junior, 2020). Véase el artículo 1.º de la Ley 12.965/2014:

Esta ley establece principios, garantías, derechos y deberes para el uso de internet en Brasil y determina las directrices de actuación del Gobierno Federal, de los Estados, del Distrito Federal y de los municipios en relación a la materia (Brasil, 2014).

La Ley 12.735/2012, según su artículo 4, tipifica las conductas que se realicen conforme a la utilización de sistemas electrónicos, digitales o similares contra sistemas informáticos:

En los términos de la normativa, los órganos de policía judicial estructurarán sectores y equipos especializados en la lucha contra la actividad delictiva en redes informáticas, dispositivos de comunicación o sistemas informáticos (Brasil, 2012).

Por lo tanto, en este escenario evolutivo y preocupante, con nuevas formas de cometer delitos, existen grandes desafíos para los órganos de persecución penal, específicamente en Brasil, que deben planificar y prepararse para todos los tipos de problemas criminales encontrados en la ciberdelincuencia (Wendt, 2012; Jorge, 2012). Wendt y Jorge citan algunos de los desafíos que enfrentan las organizaciones criminales, tales como la legislación, la integración entre los ciberdelincuentes y diversos lugares, la formación de los agentes de policía y otros actores de la persecución penal, y la criptografía y la taquigrafía utilizada.

En cuanto a la legislación, los autores dejan claro que la mayoría de las actividades que causan daños o molestias a los usuarios pueden realizarse de forma típica. Sin embargo, para entender y tratar aquellos casos en los que no existe previsión legal de tipos penales específicos, se concluye que la conducta alegada no se considera delictiva por no existir previsión legal (Wendt, 2012; Jorge, 2012).

En otras palabras, nos damos cuenta de que aunque el acto cometido por los delincuentes cause un gran daño económico o incluso psicológico a las víctimas, si no existe una legislación penal expresa, acaban quedando impunes y volviéndolo a cometer.

En cuanto a la formación de los agentes de policía y otros actores de la persecución penal, los autores indican lo siguiente:

La falta de formación de los agentes de policía y de otros actores de la persecución penal, como el Ministerio Público y el Poder Judicial, representa un gran desafío, ya que puede impedir que los ciberdelincuentes sean castigados y, en consecuencia, causar impunidad. La formación debe ser realizada de forma continua por profesionales especializados, para que las fuerzas de seguridad puedan reprimir y controlar la evolución de estos delitos [...] (Wendt, 2012; Jorge, 2012).

En el caso de la integración entre ciberdelinquentes y diversas localizaciones, Wendt y Jorge afirman que “Los recursos permiten a los ciberdelinquentes, repartidos por diversas localizaciones, comunicarse y llevar a cabo acciones delictivas en asociación y de forma organizada” (Wendt, 2012; Jorge, 2012). Se ve enseguida que es muy fácil que los delinquentes se comuniquen entre sí para cometer delitos, lo cual dificulta la investigación.

Por lo tanto, es posible ver que, de acuerdo con Barreto, Kufa y Silva, gran parte de la dificultad encontrada en el combate al cibercrimen proviene de la propia naturaleza del ambiente en que parte del crimen es realizado, que es el ciberespacio. En otras palabras, para ellos, se trata de un espacio indefinido en el que los individuos realizan transacciones y se comunican (Barreto, 2022; Kufa, 2022; Silva, 2022). Continúan así:

La falta de recursos públicos para combatir la ciberdelincuencia es una situación común a todos los países, por no hablar de las contribuciones indispensables para crear un plan de prevención permanente de algunos de estos delitos. Esta deficiencia puede superarse en parte estableciendo asociaciones con el sector privado para ayudar en este empeño (Barreto, 2022; Kufa, 2022; Silva, 2022).

En otras palabras, podemos ver que la situación relativa a la ciberdelincuencia es bastante común no sólo en Brasil, sino en todo el mundo, por lo cual se necesitan cursos y más cualificaciones para crear carreras y prevención tanto para los autores como para las víctimas, con el fin de inhibir la ciberdelincuencia.

Con el propósito de satisfacer estas necesidades de investigación en el mundo cibernético, se presentó el Proyecto de Ley 5.202 de 2016. Fue creado con el fin de incluir los delitos cometidos contra o por medio de una computadora, conectada o no a una red, dispositivo de comunicación o sistema informatizado o incluso de telecomunicaciones, una vez que haya evidencia del trabajo de una asociación delictiva (Barreto, 2022; Kufa, 2022; Silva, 2022).

Por último, hablaremos del uso de la criptografía y la taquigrafía por parte de los delinquentes para evitar ser identificados. La conclusión es que esta tendencia es muy preocupante. El cifrado se utiliza para mezclar y codificar datos e información con el fin de garantizar que sólo el destinatario tenga acceso al contenido. La taquigrafía, por su parte, permite ocultar la información de interés dentro de un mensaje, es decir, ocultar vídeos, textos y audio (Wendt, 2022; Jorge, 2012).

La práctica del delito de falsedad de identidad y el poder punitivo de las penas vigentes en el ordenamiento jurídico actual

En relación con el delito de falsa identidad, en Brasil, precisamente, se ha analizado que su penalidad sería visiblemente baja, lo cual llevaría a la reincidencia. Por lo

tanto, este tema podría considerarse el eje de este trabajo, con el fin de discernir con mayor precisión el poder punitivo frente al delito de falsa identidad.

De Castro habla del carácter subsidiario del propio delito:

Dado que el “catfishing” permite a las personas ocultarse tras una identidad que no es la suya, a menudo se utiliza como medio para llevar a cabo otros delitos, como el fraude o la malversación. Es habitual que la víctima sea seducida para entablar una relación virtual y comience a confiar en su pareja, que entonces empieza a pedirle dinero y regalos o intenta realizar estafas (De Castro y Zaganelli, 2020).

Por lo tanto, cuando pensamos en la falsedad de identidad, nos damos cuenta de que el objetivo central se enmarca directamente en otro tipo de delito, ya que su finalidad principal es la obtención de un beneficio propio o ajeno. Por lo demás, veamos algo de jurisprudencia:

Recurso penal. Sentencia condenatoria. Delitos de malversación (art. 171, *caput*, del Código Penal) cometido dos veces y falsedad de identidad (art. 307 del Código Penal) cometido tres veces. recurso de la defensa: (1) solicitando la descalificación de los delitos de malversación por el delito de “hospedaje en hotel sin tener recursos para efectuar el pago”, previsto en el art. 176 del Código Penal. No se acepta. Para el delito previsto en el art. 176, el agente no debe tener recursos para efectuar el pago. En este caso, el acusado fingió los pagos utilizando recibos “pix” falsos. Intención específica de mantener a las víctimas en el error. (2) Aplicación, de oficio, del principio de conjunción entre los delitos de falsedad de identidad y malversación. Acusado que simuló tener una identidad falsa para cometer malversación, dos veces. Aplicación del precedente STJ 17. Delitos cometidos en el mismo contexto fáctico. Precedente. Adquisición. (3) Solicitud de aplicación de la atenuante de confesión espontánea. Concedida. El acusado confesó ante el tribunal la comisión de los delitos. Solicitud de compensación parcial con la agravante de reincidencia. Acusado multirreincidente. Reforma de la pena intermedia en relación con los delitos de malversación y falsedad de identidad, cometidos ante la autoridad policial para eludir la responsabilidad criminal. Reducción de la pena final, con reajuste del régimen de la pena inicial (semiabierto).

Recurso de casación conocido y parcialmente estimado. Honorarios fijados al acusado (SJPR - 3ª Sala Penal - 0005156-83.2022.8.16.0031 - Guarapuava - Ponente: Mario Nini Azzolini - J. 12.02.2023).

Visto esto, Duarte afirma que es posible visualizar el problema en torno a la creación de perfiles falsos, es decir, para ella, las plataformas intentan de diversas formas crear mecanismos que dificulten esta práctica delictiva y mantengan la calidad y

seguridad del servicio, sin embargo, existe una dificultad para rastrear a un usuario que crea un perfil falso (Duarte, 2021).

En resumen, cuando se examina y se estudia el término *identidad falsa*, se observa que los perfiles falsos en las redes sociales son diversos. Esto hace que a menudo sean difíciles de localizar. Arroyo afirma que “se ha constatado que existen diversos motivos para crear una cuenta no identificada en las redes sociales” (Arroyo, 2019).

El precedente STJ n.º 522 establece que “La conducta de atribuir una identidad falsa a una autoridad policial es típica, incluso en una situación de supuesta legítima defensa” (STJ 2015).

RECURSO INTERLOCUTORIO EN RECURSO ESPECIAL. USO DE DOCUMENTOS FALSOS. AUTODEFENSA. ATIPICIDAD. NO CONCURRENCIA. INHABILITACIÓN. IDENTIDAD FALSA. INHABILITACIÓN. Sobreseimiento. 1. Caso en que el acusado, interceptado por agentes de la policía militar cuando conducía un vehículo automotor, presentó una Licencia Nacional de Conducir falsa. 2. La absolución pretendida es inadmisibles, ya que este Superior Tribunal, en consonancia con el Supremo Tribunal Federal, entiende que tanto el uso de un documento falso como la atribución de una identidad falsa, aunque tengan como finalidad exclusiva la legítima defensa, constituyen un delito. 3. El “uso efectivo del documento objeto de la falsificación excluye la calificación de la conducta en el delito penal de falsificación”. La “utilización efectiva del documento objeto de la falsificación descarta la calificación de la conducta en la infracción penal de falsedad de identidad, prevista en el artículo 307 del Código Penal, que tiene carácter subsidiario” (Resp. 1.710.259/SP, Rel. ministro Jorge Mussi, Sala Quinta, juzgado el 11/9/2018, DJe 19/9/2018). 4. Recurso interlocutorio desestimado (AgRg no AResp n. 2.248.031/SP, relator ministro Reynaldo Soares da Fonseca, Sala Quinta, juzgado el 7/3/2023, DJe 13/3/2023).

Por lo tanto, al analizar el citado precedente es plausible entender que el delito de falsedad de identidad ante la policía, aunque se alegue en legítima defensa, será considerado típico. A pesar de esto, lo que se puede presentar es que el delito de falsa identidad, solo o incluso con otro delito, tiene una pena baja, porque al analizar el delito en sí, se juzgarán otras cuestiones. Entre otros, el artículo 59 del Código Penal.

Dicho esto, nos damos cuenta de que el proceso de investigación no es más que un proceso complejo para llegar al delincuente, teniendo que pasar por varios factores. Por lo tanto, cuando la policía tiene éxito en el proceso de investigación y llega al falsificador, su sentencia es indulgente, lo cual le permitirá cometer este delito de nuevo, necesitando sólo un ordenador con acceso a internet para empezar de nuevo.

Sin embargo, De Castro y Zaganelli dicen que

Brasil carece de legislación específica sobre el “catfishing”, aunque exista la necesidad de protección estatal. Por lo tanto, es esencial que las leyes brasileñas existentes se adapten para cubrir esta situación. Para ello, es posible darse cuenta de que la práctica analizada puede encuadrarse en el delito de falsa identidad (De Castro, 2020; Zaganelli, 2020).

Así, en vista de todo lo anterior, se puede concluir que las penas impuestas a este delito no serían suficientes para inhibir su práctica, por lo cual es factible ajustar la pena hasta el punto en que este delito ya no rinda frutos, inhibiendo o al menos reduciendo su práctica.

En otras palabras, sería necesario aplicar una legislación más estricta, con sanciones y calificativos más graves, para tratar de garantizar la paz social en la humanidad en relación con el uso de su identidad.

III. CONSIDERACIONES FINALES

Para resumir, este artículo comenzó conceptualizando lo que es la *ciberdelincuencia*, entendida como el delito cometido utilizando ordenadores conectados a una red de internet. Según este artículo, este delito también se caracteriza por comportamientos desviados aplicados por medios tecnológicos. También fue posible darse cuenta de que, además de los ciberdelitos mencionados anteriormente y enumerados aquí, existen de hecho conductas que, aunque perjudiciales para las víctimas, sólo serían consideradas “dañosas”, eliminando así la punibilidad.

A lo largo del texto se constata que todo esto está ocurriendo por el avance y especialización de los delincuentes en la aplicación de estafas y conductas consideradas ilegales en el mundo virtual. También se analiza que cuanto más se han desarrollado y evolucionado las redes sociales, más utilizan los delincuentes estrategias y medios cada vez más progresistas y creativos, penalmente hablando.

Así, en relación con el propio delito de falsedad de identidad, recogido en los artículos 307 y 308, ambos del Código Penal, se pudo comprobar que las causas relacionadas con el significativo aumento de la aplicación del delito estarían directamente vinculadas a la falta de información de la víctima, o, mejor dicho, a la dificultad que tendrían para comprender los mecanismos utilizados para cometer el delito, así como a la astucia de los delincuentes.

Es más, en este texto se han analizado varios tipos de perfiles que podrían considerarse falsos, siempre que se utilicen para medir y obtener ventajas ilícitas, y no sólo perfiles aleatorios.

Se puede concluir, por lo tanto, que los delitos virtuales son completamente furtivos, especialmente el delito de falsificación de identidad, que se entiende como un delito de medio que se utiliza para cometer otros delitos de fin. También nos damos cuenta de que aún existen grandes desafíos para los órganos de persecución penal brasileños, que necesitan una planificación más eficaz dirigida a la punición ejemplar de todos los tipos delictivos involucrados en la ciberdelincuencia.

La investigación también pudo analizar el hecho de que la legislación aún no está calificada para inhibir toda la gama de delitos cibernéticos, especialmente cuando se trata del uso de identidad falsa. Por lo tanto, es necesaria una mayor capacitación de la policía, el Ministerio Público y el Poder Judicial en este caso, con una legislación más estricta y calificada, ya que aún es notorio ver cuán grandes son los desafíos en el ambiente virtual para la correcta aplicación de la ley penal.

Y, por último, sería completamente importante que las víctimas conocieran mejor la ciberdelincuencia y los medios con los que se perpetra, comprobando siempre las fuentes de información y protegiéndose en la medida de lo posible, y buscando siempre ayuda si sospechan que algo malo puede estar ocurriendo o ya está ocurriendo.

BIBLIOGRAFÍA

Arroyo, Danilo Wohnrath *et al.* *La creación de perfiles falsos en las redes sociales Facebook y Twitter: motivaciones y tipos*. 2019. Disponible en <https://repositorio.ufsc.br/handle/123456789/203028> > Consultado el 07/05/2023 a las 15:49.

Barreto, Alesandro Gonçalves. Kufa, Karina. Silva, Marcelo Mesquita. *Cibercrimes, en Cibercrimes e seus reflexos no direito brasileiro*, 3.^a ed. São Paulo: Juspodivm, 2022.

Bertholdi, Juliana. Proceso y clasificación, en *Cibercrimen* [recurso electrónico]. Curitiba: Contentus, 2020. Disponible en <https://plataforma.bvirtual.com.br/Leitor/Publicacao/184412/pdf/0?code=S4hUDA7OBuYF8IrLtdUlfX6gUVZYh06NbMRMgtPxyb1Ouw/LMwseGWii417L8EDxQ+JC9D VWcmzrdmEmu8nTA.> > Accessed on 25/05/2023 at 23h41.

Bomfati, Cláudio Adriano. Junior, Armando Kolbe. Definiciones de Crimen, en *Cibercrimen*. Curitiba: Intersaberes, 2020. Disponible en <https://plataforma.bvirtual.com.br/Leitor/Publicacao/179734/pdf/0?code=AC/0drvJt9EusvViUiQZX6Iq548DLUrAvnCeRs3AhMYoirRRmaxAsxL01nHqpkm0hpTJ5N2zizpRzaiNb99/Yw=> > Accessed on 26/05/2023 at 14h23.

Brasil. Tribunal de Justicia de Paraná (3.^a Sala Penal). Recurso Penal - 0005156-83.2022.8.16.0031. Condena Sentencia. Rel.: juez Mario Nini Azzolini. Guarapuava, 12 de febrero de 2023. Disponible en <https://portal.tjpr.jus.br/jurisprudencia/j/410>

0000022167461/Ac%C3%B3rd%C3%A3o-0005156-83.2022.8.16.0031 > Consultado el 18/05/2023 a las 10:35.

Brasil. Decreto-ley 2.848, del 7 de diciembre de 1940. Código Penal. Disponible en https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm > Acceso el 02/04/2023 a las 13:05.

Brasil. Decreto-ley 12.373/2012. Ley Carolina Dieckmann. Disponible en https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm > Consultado el 01/05/2023 a las 14h11.

Brasil. Decreto-ley 12.695/2014. Marco de los derechos civiles en Internet. Disponible en https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm > Consultado el 11/05/2023 a las 14:12.

Brasil. Decreto-ley 12.735/2012. Ley Azevedo. Disponible en http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112735.htm > Consultado el 11/05/2023 a las 14:14.

Castro, Anaflavia Cera Daltro de; Zaganelli, Margareth Vetis. Catfishing: ¿delito de falsa identidad? *Revista de Estudos Jurídicos da UNESP*, vol. 24, n.º 40, 2020. Disponible en <https://ojs.franca.unesp.br/index.php/estudosjuridicosunesp/article/view/3099> > Consultado el 02/04/2023 a las 18h41.

Cordeiro, Bezerra, Luan, Victor. Ciberdelincuencia: por qué el derecho penal debe seguir el ritmo de los avances digitales. Disponible en <https://repositorio.animaeducacao.com.br/handle/ANIMA/29726> > Consultado el 03/05/2023 a las 22h04.

Duarte, Estefanía Martínez. Perfiles falsos en las redes sociales contemporáneas: un análisis de la responsabilidad penal y civil, 2021. Disponible en <https://dspace.mackenzie.br/handle/10899/31417?show=full> > Consultado el 25/05/2023 a las 19h43.

G1. Disponible en <https://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html> > Consultado el 03/06/2023 a las 17:29.

Silva, Hanna Karolina Santos da. Los principios de finalidad y necesidad como límites a la recogida de datos. 2022. Disponible en <https://repositorio.animaeducacao.com.br/handle/ANIMA/30623> > Consultado el 02/04/2023 a las 18h49.

Steffens, Alessandra; Groth, Nicolas Felipe; Balbinot, Rafael Sartori. Atribución de identidad falsa ante las autoridades policiales. *Anuario Pesquisa e Extensão Unoesp*, São Miguel do Oeste, v. 4, p. e23586-e23586, 2019. Disponible en <https://periodicos.unoesp.edu.br/apheusmo/article/view/23586> > Consultado el 12/05/2023 a las 13:34.

STJ. Precedente n.º 522, Sección Tercera, juzgado el 25/3/2015, DJe de 6/4/2015. Disponible en <https://scon.stj.jus.br/scon/pesquisar.jsp> > Consultado el 07/06/2022 a las 21h52.

STJ.T5. Recurso interlocutorio en recurso especial. 150047951.2018.8.26.0530. Magistrado Reynaldo Soares da Fonseca. Dje 13/03/2023. Disponible en https://processo.stj.jus.br/processo/pesquisa/?src=1.1.3&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&num_registro=202203615385 > Consultado el 07/06/2023 a las 22h14.

Wendt, Emerson. Jorge, Higor Vinícius Nogueira. Amenazas en la “World Wide Web”, en *Crimes Cibernéticos: ameaças e procedimentos de investigação*, 2.^a ed. Río de Janeiro: Brasport, 2013.