LA SUPLANTACIÓN PERSONAL A TRAVÉS DE MEDIOS VIRTUALES Y DIGITALES. [1]

El tipo penal de falsedad personal de la Ley 599 de 2000.

Adriana Lucia Loaiza Cadavid [2]
Edy Yuliana Orrego Osorio[3]
Hernán Darío Areiza Sánchez[4]

Resumen

En esta investigación se realizó un análisis acerca del delito de falsedad personal en Colombia, para ello establecieron cuáles son las causas que han generado el incremento de casos de suplantación personal a través de medios digitales y presenciales, se determinaron cuáles son los derechos que están siendo vulnerados, y los medios que se tienen para denunciar este delito.

Para esta investigación se analizaron los mecanismos de protección que existen en la actualidad para garantizar los derechos de los ciudadanos en relación con el manejo de los datos personales de manera individual y de las empresas que verifican, administran y califican los datos en Colombia y si la forma como se usan los datos de las personas en Colombia es la adecuada.

La opinión de las víctimas de dichos delitos fue fundamental para establecer que la ley es laxa con los delincuentes sino también ejerce un papel de verdugo con las víctimas de dichos delitos, puesto se determinó que el acompañamiento en la denuncia es mínimo y las respuestas son escasas a la hora de brindar soluciones eficaces a sus casos, además de que al final muchas víctimas deben asumir deudas que no son suyas.

Palabras clave: Datos personales, protección de datos, acceso a la información, suplantación personal, hábeas data.

1 Artículo para optar al título de abogados. Asesores temático y metodológico: Laura Victoria Cárdenas Rojas laura.cardenasro@amigo.edu.co y Jorge Enrique Barrera García jorge.barreraga@amigo.edu.co

2 Estudiante adscrita al programa de Derecho de la facultad de Derecho y Ciencias Políticas: Adriana Lucia Loaiza Cadavid 2: Adriana.loaizaad@amigo.edu.co
3 Estudiante adscrita al programa de Derecho de la facultad de Derecho y Ciencias Políticas: Edy Yuliana Orrego Osorio3: edy.orregoos@amigo.edu.co
4 Estudiante adscrito al programa de Derecho de la facultad de Derecho y Ciencias Políticas: Hernán Darío Areiza Sánchez4:hernan,areizasa@amigo.edu.co

Inicio de la investigación: 2021. Finalización de la investigación: 2022

Abstract

In this research an analysis was made about the crime of personal falsehood in Colombia, for this purpose it was established which are the causes that have generated the increase of cases of personal impersonation through digital and face-to-face means, it was determined which are the rights that are being violated, and the means that are available to denounce this crime.

For this research, the protection mechanisms that currently exist to guarantee the rights of citizens in relation to the handling of personal data individually and of the companies that verify, manage and qualify the data in Colombia were analyzed, and whether the way in which people's data is used in Colombia is adequate.

The opinion of the victims of such crimes was fundamental to establish that the law is lax with criminals but also plays the role of executioner with the victims of such crimes, since it was determined that the accompaniment in the complaint is minimal and the responses are scarce when it comes to providing effective solutions to their cases, in addition to the fact that in the end many victims must assume debts that are not theirs.

Keywords: Personal data, data protection, access to information, personal impersonation, and habeas data.

Introducción

Clasificar los delitos en el marco de la virtualidad ha sido tan complejo como penalizarlos. Por eso, este artículo de investigación pone su acento en el origen del acto delictivo que se ha incrementado escandalosamente en los últimos años en Colombia.

Hablar simplemente de suplantación, es fijar la atención en la punta del iceberg del problema, pues la fase más ostentosa no ha resultado contundente debido a los pocos recursos investigativos y a la actualidad de las leyes que regulan los delitos informáticos. Sin embargo, resulta útil el estudio del caso dada la incurrencia sucesiva en el país, pues es posible evidenciarla a través de personas víctimas de este flagelo.

Entre tanto, la suplantación personal es un acto que lleva a una persona a hacerse pasar por otra, ya sea de forma física o digital, con propósito de acceder a información personal o empresarial de manera fraudulenta. Esta ilegalidad ha aumentado en la era digital pues es un medio donde interactúan millones de personas de forma voluntaria u obligada. La voluntad se refleja en las redes sociales, donde se publican fotografías, estados de ánimo, lugares que se frecuentan, historias personales, y la información obligada se otorga a la hora de usar entidades financieras, de salud, de trabajo, entre otras. En el momento en que esa información circula en la nube, se corre el riesgo de ser víctima de fraudes, o bien, en el caso de los delincuentes, se tiene la oportunidad de acceder a todo.

Por eso, la policía o autoridad encargada, pone a disposición de la ciudadanía la posibilidad de denunciar delitos informáticos, que se clasificarán más adelante en la investigación.

La suplantación de identidad, según datos de la Dijín, creció 409% el año pasado, en plena pandemia del covid-19. El reporte reveló que mientras en 2019 hubo alrededor de 300 casos de este tipo, en 2020 la cifra se disparó a 1.527 reportes"

Así pues, es notorio que durante la pandemia la virtualidad se impuso y "mediante el Decreto 749 del 28 de mayo de 2020, el Gobierno Nacional ordenó el Aislamiento Preventivo Obligatorio en todo el territorio colombiano"(Presidencia de la república, oficina de prensa, 2020).

Este aislamiento preventivo, propició el trabajo, el estudio y el ocio en diferentes modalidades de la virtualidad. Surgieron aplicaciones, plataformas, motores de búsqueda y

todo tipo de recursos que permitieran la comunicación entre las personas. Y no se puede eludir la responsabilidad que todos tienen a la hora de entregar y recibir datos.
De ahí la importancia de conocer las causas y las diferentes modalidades de los delitos, con el fin de acudir a la ley para denunciarlos, pero sobre todo, conocerlos.

Este artículo de investigación se desarrolla teniendo claridad en los objetivos propuestos, teniendo en cuenta testimonios de personas víctimas de suplantación de identidad y estafa y haciendo un análisis de la poca bibliografía encontrada.

Los avances tecnológicos, la globalización de la informática , la propagación del coronavirus Covid 19 y las medidas de confinamiento emitidas por el gobierno nacional decreto 476 del 25 de marzo de 2020, han llevado a que empresas privadas como bancos y empresas de telecomunicaciones utilicen todos los recursos tecnológicos que tienen a su disposición, para que las personas puedan acceder de manera rápida y fácil a ellos y a sus servicios, sin embargo, este auge de la informática que busca que todas las personas tengan la información en tiempo real, ha hecho que personas que tienen conocimiento en informática utilicen técnicas para hurtar u obtener información personal, información financiera de empresas o hasta intervienen las políticas de las entidades bancarias para el beneficio propio.

A medida que el uso de internet se ha extendido, ha aumentado el riesgo de su uso inadecuado. Los delincuentes cibernéticos recorren la virtualidad y realizan incursiones fraudulentas cada vez más frecuentes y variadas, como el acceso sin autorización a sistemas de información, piratería informática, fraude financiero, sabotaje informático y pornografía infantil, entre otros. Pese a la dificultad para descubrirlos, varios países han dispuesto un sistema judicial especializado que permite procesarlos y castigarlos. A ese grupo de países se unió Colombia en 2009. (Ojeda Pérez, et al., 2010).

Las conductas que más afectan a las personas en Colombia son el hurto por medio informático que se encuentra consagrado en el artículo 269A: acceso abusivo a un sistema informático y siguientes de la ley 1273 de 2009, que modificó el código penal, creando un nuevo bien jurídico tutelado “de la protección de la informática y de los datos”, llevando esta conducta al “delito de falsedad personal”, (artículo 296 de la ley 599 del 2000). El (artículo 296 de la ley 599 de 2000), define como falsedad personal aquella situación que

para beneficio propio o daño en otra persona, “suplante, atribuya o sustituya nombre, edad, estado civil, o calidad que pueda tener efectos jurídicos, incurrirá en multa, siempre que la conducta no constituya otro delito”(pág. 53).

Según lo anterior, se puede deducir que de los delitos mencionados nace la suplantación de identidad, toda vez que al navegar en redes sociales o en internet, se da clic en enlaces de dudosa procedencia y es allí donde se da el robo de información sensible, al recibir llamadas telefónicas y se otorgue información financiera, personal o empresarial para dicho caso.

Para abordar el tema de seguridad de datos personales, se debe relacionar con el manejo de identificaciones que se transfieren en los motores de búsqueda, cuyos alcances con la información de toda índole, deben ser normalizados y que finalmente se apliquen los derechos de protección de datos. De este modo se garantizaría el control con la conexión en la web. Como fue mencionado por Marqueo Ramírez (2016).

> Así como la afectación “significativa” que supone a los derechos fundamentales de respeto a la vida privada y de protección de datos personales, la posibilidad de acceder a información estructurada sobre una persona física a partir de la búsqueda en Internet por su nombre (Pág 77).

Como fenómeno de la pandemia se encuentra que estadísticamente aumenta el número de casos de suplantación personal con respecto al 2019. Para el 2020, año en que inició la pandemia del Covid 19 se refleja que la suplantación personal creció en un 35.8% equivalente a 4.353 casos en 2020 comparado con los 951 casos reportados para el año 2019. (Acosta Argote, 2021).

Es importante tener en cuenta que la suplantación de la identidad también está tipificada como delito, porque viola la intimidad personal, para proteger a los ciudadanos se han encaminado acciones para la prevención de los delitos informáticos, la suplantación de identidad y espionaje informático, dichas herramientas son conocidas como Tratamiento de datos (Suarez Sánchez, 2016).

Metodología

Para el desarrollo de este artículo de investigación se aplicará un enfoque cualitativo, donde se trabaja con estadísticas, gráficos, bases de datos y estudios previos que se han generado en los últimos años en la Fiscalía General de la Nación, la Policía Nacional de Colombia y la Superintendencia Financiera.

También, donde se analiza la situación vivida por víctimas, a través de sus casos de suplantación personal, fraude en internet

En cuanto al análisis se debe cumplir con el objetivo de establecer qué leyes reglamentan este delito de falsedad personal en Colombia y algunos países, la opinión de diferentes magistrados sobre el tema y lo que se ha decido en la Corte Suprema de Justicia sobre las tutelas de vulneración de los Derechos que se ven afectados por la suplantación personal.

Dicha investigación, tendrá un enfoque dogmático, porque se estudiará la norma jurídica, se analizará la eficacia del ordenamiento jurídico y si se ajusta a la nueva realidad social de la informática.

En esta investigación como lo menciona Tantaleán Odar, (2016)

> Aquí se estudia a las estructuras del derecho objetivo –o sea la norma jurídica y el ordenamiento normativo jurídico- un estudio dogmático se basa, esencialmente, en la legislación y la doctrina como fuentes del derecho objetivo, y eventualmente comprendería algún precedente vinculante, en tanto, tiene similar fundamento y efectos que la legislación (pág. 4).

Es decir que el enfoque dogmático jurídico es teórico, porque se describe , interpreta , analiza la norma jurídica, cuestionando y haciendo supuestos, sin desconocer las limitaciones que hacen según los contextos sociales para así llegar a contribuir con la efectividad del ordenamiento jurídico.

Desarrollo

Desde hace mucho tiempo se viene hablando de falsedad como un delito que consiste en la alteración o simulación de la verdad con efectos relevantes, hechos en documentos públicos o privados, en monedas en timbres o en marcas. La Real Academia de la Lengua RAE, define la falsedad como: "falta de la verdad o autenticidad. Falta de conformidad entre las palabras, las ideas y las cosas" (S.F.).

La falsedad personal se convirtió en un delito que se encuentra tipificado en el Código Penal Colombiano**,** la ley 599 de 2000, en su artículo 296 de Julio de 2000 asegura:

> El que con el fin de obtener un provecho para sí o para otro, o causar daño, sustituya o suplante a una persona o se atribuya nombre, edad, estado civil, o calidad que pueda tener efectos jurídicos, incurrirá en multa, siempre que la conducta no constituya otro delito (pág 53).

Uno de los más grandes ventajas para la falsedad personal es la falta de precaución que los ciudadanos tienen con sus datos personales, muchas veces se observa cómo las personas entregan datos personales en llamadas telefónicas sin confirmación de quiénes están solicitando estos datos, así como la falta de cuidado al aceptar cookies en las páginas de internet y otros medios digitales que son los más propicios para la suplantación personal.

Cuando se habla de medios digitales, se entiende que son espacios en los que se generan diversos estilos de comunicación e intercambio de información de contenido digital como las páginas web, redes sociales, archivos digitales y bases de datos entre personas.

El artículo 15 de la (Constitución Política de Colombia, 1991, pág 15), refiere que "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar".

Sin embargo, en muchas situaciones los gobiernos pueden hacer uso de los datos de sus ciudadanos, puede ser para enviar información de interés de toda su ciudadanía o para hacer campañas políticas tratando de hacer un cambio en la intención del voto. Es bien sabido que no siempre la información que le llega a las personas es información verídica, la mayoría de las veces la información de las personas puede ser manipulada.

En 2014 se realizó la Cumbre Mundial de la Sociedad de la Información, que tenía como objetivo "reducir la brecha digital existente entre los países en desarrollo y los países desarrollados mediante un mayor acceso a servicios modernos de TIC" (Zhao , 2011, Parr. 3). Aun así, no siempre el acceso a las Tics es bueno para las personas, como lo afirma la Corte constitucional en la Ley 1341 de 2009 "el Estado velará por la adecuada protección de los derechos de los usuarios de las Tecnologías de la Información y de las Comunicaciones" (pág. 2).

A pesar de la protección de datos que ofrece la rama legislativa del poder público en Colombia para el uso de herramientas tecnológicas por parte de los ciudadanos, son estos los que deben cuidar su dignidad humana, pues los delitos informáticos son cada vez más frecuentes. Y es que disponer toda la confianza a la hora de proveer datos es un descuido por parte de los usuarios. Toda ley, aunque esté amparada por el gobierno, sólo se ejecuta cuando la infracción es un hecho, esto es, que la protección de la información es también una responsabilidad ciudadana. No es posible que cada oportunidad de acceder a un recurso informático sea también un acto de ingenuidad. Esto para mencionar algunos casos, como los mensajes de texto recibidos en el celular donde ofrecen trabajo bien remunerados, premios, o contenido provocador. Cosas que se salen de la realidad, pero generan una ilusión inconsciente que se desenvuelve en el error de abrir enlaces con fines maliciosos.

También, se pueden mencionar múltiples casos de extorsión por medio de las redes sociales, ya sea suplantación de identidad donde envían mensajes de auxilio y ponen en alerta al usuario, solicitando dinero para resolver un problema vital o por la publicación de documentos equivalentes a fotografías, videos que comportan la intimidad de una persona. Además de las veces que los delincuentes se identifican como funcionarios del banco y, con propuestas de descuentos o compensaciones por buena conducta en el historial crediticio, terminan obteniendo hasta los números de clave y de seguridad.

Cierto es que las entidades financieras todo el tiempo recalcan y promueven campañas sobre seguridad de la información, pues en estos casos no sólo se tipifican robos de datos, sino de dinero. De ahí, que la responsabilidad bancaria teorice que "La información es el activo más importante de empresas y personas, por lo tanto, se genera todo tipo de responsabilidades" (Realpe, S.F. Párr 13).

La recomendación es siempre tratar de tener contraseñas seguras, cambiarlas constantemente y adoptar una cultura preventiva para evitar que la información personal, privada y bancaria salga de las personas, así evitando suplantaciones de identidad, extorsiones o delitos informáticos.

Con las clasificaciones de delitos informáticos comunes, se evidencian los nuevos riesgos de las diferentes poblaciones, lo que lleva al gobierno a elaborar leyes y normas que describan los procedimientos a seguir con el propósito de buscar la manera adecuada del tratamiento de la información que se suministra para abastecer bases de datos empresariales, bancarias, editoriales, entre tantas que conducen a la necesidad de afinar y perfeccionar las disposiciones legales que incluyan las necesidades individuales que surgen en una sociedad cada vez más sistematizada y automatizada.

En la última década, en Colombia se han emitido leyes que regulan el problema de manera particular y general, con el fin de proteger los datos personales con el desempeño único de sancionar los delitos y adaptar condiciones precisas y ordenamientos en el marco legal. En consecuencia, las empresas públicas y privadas que acopian y tramitan los datos personales están con el compromiso de resguardarlos de un uso clandestino y garantizar los derechos señalados en la Ley 599 de 2000, con fundamento en la Constitución Política de Colombia. Pues para tener una planeación positiva sobre la prevención de delitos financieros y tributarios, es indispensable conocer las leyes.

Es así como entra en vigencia la Ley 1581 de 2012 que tiene como objetivo principal "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos" (pág 1.). No solo es importante que los ciudadanos velen por el cuidado de sus datos personales, también es importante que las empresas tanto públicas y privadas prioricen en la necesidad de hacer cumplir la normativa de protección de datos, sean conscientes de sus deberes dentro del procesamiento de los datos personales y que garanticen la transparencia en el proceso de recolección, procesamiento y tratamiento de la información.

Como lo determina Ortiz Rodríguez, 2016

> El término falsificación de documentos aparece, por primera vez, en La Lex Cornelia Testamentaria y Num María cuyas disposiciones penaron algunas frecuentes falsedades en testamentos y monedas. Posteriormente esas disposiciones se extendieron a otros documentos jurídicos y la ley se denominó Lex Cornelia de Falsis. EI Fuero Juzgó y sancionó la falsificación de escritos y su uso en juicio. EI Código de las siete partidas especificó diversas modalidades de la falsificación en documentos cometidos por notarios públicos, escribanos del Rey, de la ciudad o de las villas y por particulares. En España y a partir de 1822 los códigos penales empezaron a sistematizar las diversas clases de falsedad (pág.1).

Según lo anterior, se puede decir que la falsedad de documentos se viene estudiando desde décadas atrás, inicialmente se daba esta falsedad en documentos que se presentaban en juicio, es decir que eran documentos públicos y que no cualquier persona del común podía falsificar.

En Colombia, bajo la denominación "delitos contra la fe pública", el Código Penal de 1890 consagra los delitos de falsificación de documentos de crédito, falsedades en documentos oficiales y públicos, y falsedades en documentos privados. Mientras tanto en el Código Penal vigente se establecen diversos tipos de falsedad en documentos públicos, oficiales, títulos valores, eclesiásticos que pueden producir efectos en el estado civil de las personas. Se distinguen en dicho código, la falsedad material, ideológica, intelectual, la personal y la falsedad por uso. El código penal anterior tipifica este delito como delito contra la fe pública. En el nuevo código hablamos de que es falsedad personal lo cual implica suplantar o sustituir a otro, lo cual es hacer aparecer a ese otro como autor de un documento, pero también hacerse pasar por ese otro, en este caso el autor del delito se presenta físicamente fingiendo ser otro. Se trata pues de una suplantación física, sin embargo, para la implantación o sustitución, salvo el caso de homónimos, es absolutamente necesario atribuirse nombre falso. Atribuirse al estado civil, calidad, profesión, oficio, edad o condición lo cual es mentir sobre la identidad, el estado o las cualidades de una persona con el fin de causar daño.

Según el planteamiento de Rojas Bejarano (2014)

> Colombia ha evolucionado en materia de protección de datos en los últimos años con la implementación de nuevas normas que tienen como fin salvaguardar los derechos y deberes fundamentales, así como los procedimientos y recursos para la protección de estos, a partir de la jurisprudencia constitucional, se consideró el derecho de Hábeas como un derecho fundamental autónomo, distinguible de otras garantías como la intimidad y el buen nombre. No obstante, a la luz de los estándares internacionales para su efectiva protección requiere estrategias que, de manera armónica, garanticen su seguridad jurídica (pág. 107).

Este es un proceso que va evolucionando en materia de protección de datos que ha vulnerado varios derechos, pero que hoy es protagonista en normas que se pueden aplicar para garantizar su cumplimiento, uno de ellos es el derecho al comparendo y la invocación del Habeas Data.

En la actualidad se habla de este delito que cuenta con mucho auge por la tecnología que se ha implementado para suplantar pero también para proteger a las personas, este está tipificado en la ley 599 de 2000 en su Artículo 296 que nos define el delito como

> El que con fin de obtener provecho para sí o para otro, o causar daño, sustituya o suplante a una persona o se atribuya, nombre, edad, estado civil o calidad que pueda tener efecto jurídicos, incurrirá en multa, si su conducta no constituye otro delito(pág 53).

Se le ha otorgado al ciudadano medios seguros y rápidos para hacer peticiones de revisión de sus casos cuando se ve afectado en las centrales de riesgos, uno de estos medios es poder acercarse a la central de riesgo para interponer una queja, y la entidad deberá contestar en máximo 15 días, si por este medio no es posible solucionarlo la Superintendencia de Industria y Comercio (SIC) está en la capacidad de ayudar al ciudadano y sancionar la entidad que incurra en el error, se tiene como ente que puede ayudar a mitigar los daños a la Fiscalía General de la Nación y denunciar la falsedad Personal, la cual puede ser escrita u oral.

En la actualidad existe la Ley estatutaria 1581 de 2012 para la protección de los datos personales, dicha ley tiene por objeto

> Desarrollar el objeto constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas, en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información consagrada en el artículo 20 de la misma (pág 1).

En la actualidad la SIC tiene una clasificación de los datos personales que se deben tener y que entran en la protección del marco de la ley.

Dato Público: Es el dato que según la ley o la constitución es considerado como un dato público. Son datos afines a estado civil, profesión u oficio.

Dato Semiprivado: Es el dato que no tiene naturaleza íntima, su divulgación puede interesar solo a su titular o a cierto sector, personas o comunidad en general.

Dato Privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato Sensible: Es el dato que afecta la intimidad del titular, su uso indebido puede generar discriminación.

Siguiendo lo planteado por Peña Valenzuela (2021)

> La autorización para el recaudo y tratamiento de datos personales se ha convertido poco a poco en un deber ser de las empresas y entidades que han involucrado este documento en su día a día. La autorización debe ser expresa o por actos inequívocos y su alcance debe estar vinculado a la finalidad o propósito que va a tener el procesamiento de la información (Parr 4).

Las empresas tanto públicas como privadas deben reconocer que también son actores fundamentales en la protección de datos tanto de sus usuarios internos y externos, como de la información producida por su misma organización. Una efectiva sociedad de la información se construye teniendo equilibrio entre la protección de los datos tanto de las personas naturales como de las empresas.

Ante el incremento de los delitos informáticos y la suplantación de la identidad, es importante reconocer que ahora dichos delitos son mucho más enmarañados y las empresas pueden ser cada vez más vulnerables.

La protección de datos la vulnerabilidad de estos no es solo un tema que atañe a Colombia, es un tema a nivel global, en 2003 surge la Red Iberoamericana de Protección de Datos integrado por representantes de sectores públicos y privados con la misma problemática de violación de datos, suplantación personal y fraude electrónico que Colombia, dichos actores desarrollan iniciativas y proyectos que van encaminados en la protección de datos. La Red estándares de protección de datos que "buscan ser el modelo de referencia para la regulación futura en la región del derecho de protección de datos, así como para la revisión de las normas ya existentes para su actualización conforme a sus parámetros" (Peña Valenzuela, 2021, parr 9).

Colombia ha tipificado en la ley 1273 de 2009 los delitos informáticos más comunes, sin embargo no todas las personas los conocen, y su desconocimiento ha permitido la proliferación de los mismos. "En Colombia los delitos informáticos son los accesos de manera ilícita o no autorizada a los datos e información que están resguardados en formatos digitales" (World Legal Corporation, 2021, parr 2).

El código penal establece cuales son los delitos informáticos más comunes en Colombia, y de los cuales la ciudadanía requiere mayor protección e información para así evitar que los ciudadanos sean víctimas de dichos delitos. La ley 1273 de 2009 define dichos delitos.

Acceso abusivo a un sistema informático

Según el artículo 269A: El acceso abusivo a un sistema de información es el "acceso a un sistema protegido o no" siendo estos correos electrónico, redes sociales, bases de datos, o cualquier otra plataforma con o sin protección, quien cometa dicho delito "incurrirá en una pena de prisión de 48 a 96 meses y una multa económica de 100 a 1000 SMLV".

Obstaculización ilegítima de sistema informático o red de telecomunicación

Este delito dificulta el acceso, lentifica la ejecución de los comandos, suspende los servicios, impide la apertura de las páginas web, envía correos spam, niega la información, desvía las búsquedas y permite los virus con el fin de dañar la segmentación de los datos. El Articulo 269B infiere que quien cometa este delito "incurrirá en una pena de prisión de 48 a 96 meses y en una multa económica de 100 a 1000 SMLV, siempre que la conducta no constituya delito sancionado con una pena mayor"

Interceptación de datos informáticos

Este delito adultera las claves de acceso a los sistemas, quien trate de acceder a estos con las contraseñas conocidas le será imposible visualizar la información contenida, pues las claves de acceso han sido cambiadas. El articulo 269C promulga que quien cometa este delito "incurrirá en pena de prisión de 36 a 72 meses".

Daño Informático

Cuando hablamos de daño informático hablamos de falsificación de documentos electrónicos, robo de identidad, phreaking, fraudes electrónicos y pornografía infantil. Para lo cual el artículo 269D define "El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos" quien cometa este delito "incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 SMLV".

Uno de los delitos informáticos que más se conocen y para dañar las empresas es el uso de Softwares maliciosos. Un software malicioso es cualquier aplicativo, programado para dañar un sistema operativo. De este modo pueden robar datos personales de un dispositivo, reducir la velocidad de un computador y enviar correos electrónicos falsos desde su cuenta de correo electrónico sin su conocimiento. Los tipos de software malicioso más usados son:

Virus: Programa nocivo que puede copiarse a sí mismo e infectar a un dispositivo electrónico.

Gusano: Programa informático dañino que envía duplicados de sí mismo a otros dispositivos mediante una red.

Software espía: Software ilegal que colecciona información de los usuarios sin que se dé cuenta.

Adware: Software que imita, muestra o descarga automáticamente anuncios publicitarios en un dispositivo.

Troyano: Programa informático que al instalarse destruye el sistema de un dispositivo y roba su información.

Para el software malicioso el articulo 269E infiere que quien cometa este delito" incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 SMLV".

Violación de datos personales

Cuando se habla de este delito se habla de violación a datos confidenciales o sensibles, o a la acción de hacer uso de los datos de las personas poniéndolos como disponibles y violando la integridad de estos, dicha acción puede poner en riesgo los derechos y libertad de las personas. El articulo 269F promulga que quien viole los datos personales de otra persona "incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 SMLV".

Suplantación de sitios web para capturar datos personales

La suplantación de sitios se hace a través de la clonación de páginas de entidad bancarias o correos electrónicos con el fin de hacer que los consumidores virtuales sigan enlaces que los lleva a entregar sus datos personales consiguiendo con esto ser estafados. El articulo 269G promulga que quien suplante sitios web "incurrirá en pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 SMLV".

El Código Penal y su ley 1273 de 2009 contempla en su capítulo 2 otros importantes delitos informáticos

Hurto por medios informáticos y semejantes

Este se define como una descarga o instalación de aplicaciones o software espía para el robo de información, el acceso ilegal a sistemas informáticos y la clonación de tarjetas débito y crédito. El artículo 269I promulga que quien cometa este delito "recibirá la pena señalada en el 240" del mismo código penal, dicho artículo señala que "La pena será de cinco (5) a doce (12) años de prisión cuando el hurto se cometiere sobre elementos destinados a comunicaciones telefónicas, telegráficas, informáticas, telemáticas y satelitales".

Transferencia no consentida de activos

Se fundamenta como un fraude donde el delincuente ejecuta transferencias contables y automáticas de cualquier activo o valor, no autorizada y no contemplada por su titular en

daño de un tercero. Esto se posibilita cuando se comenten todos los delitos ya mencionados. El artículo 269J promulga que quien cometa dicho delito

> Incurrirá en pena de prisión de 48 a 120 meses y en multa de 200 a 1.500 SMLV. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

En cuanto a los datos personales, la ley estatutaria 1581 de 2012 hace referencia a que toda información que se encuentra ligada a una persona y con la cual pueda identificarse. Hablamos de su documento de identidad, lugar de nacimiento, estado civil, edad, lugar de residencia, recorrido académico, laboral o profesional. Se establece también como dato personal sensible estado de salud, características físicas ideología, sexualidad y otros aspectos. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos.

La Superintendencia de Industria y Comercio SIC (S.F.), establece que en Colombia

> Los datos personales conforman la información necesaria para que una persona pueda interactuar con otras o con una o más empresas y/o entidades para que sea plenamente individualizada del resto de la sociedad, haciendo posible la generación de flujos de información que contribuyen con el crecimiento económico y el mejoramiento de bienes y servicios. Así, por ejemplo, cuando hacemos una solicitud de crédito ante una entidad financiera, se requiere diligenciar formularios con nuestra información personal, o cuando realizamos una compra y para realizar la factura de venta solicitan datos como el número de documento de identidad, correo electrónico, dirección y teléfono de contacto, entre otros (Parr 3).

Podemos hablar también de la falsedad material que puede ocurrir cuando alguien enmienda, tacha, borra, suprime o de cualquier manera altera su texto constatable en forma material, es decir si altera el contenido material del documento, es falsedad material impropia, si se elabora íntegramente el documento privado.(CSJ SP, 29 nov. 2000, rad. 13231).

Mientras que la falsedad ideológica tiene lugar cuando el particular consigna en el documento privado hechos o circunstancias ajenas a la realidad, es decir, cuando falta a su deber de verdad sobre un aspecto que comporta quebrantamiento de relaciones sociales con efectos jurídicos (CSJ SP, 30 abr. 2008, rad. 23159).

A pesar de la normativa existente y vigente, de las múltiples campañas que se tienen en radio, televisión y medios escritos para evitar el fraude electrónico y la suplantación personal y a pesar de los múltiples esfuerzos de la policía y su departamento de delitos informáticos en prevenir a las personas sobre el fraude, los ciudadanos siguen siendo descuidados con sus datos, con las páginas que visitan y con la entrega de sus datos personales y bancarios en páginas de dudosa procedencia y llamadas extorsivas.

Es importante recalcar que todas las personas tienen derecho a conocer, actualizar, rectificar y retirar todo tipo de información que las empresas públicas o privadas hayan recogido sobre ellas y reposen en bases de datos.

Para la protección de ese derecho la Corte Constitucional mediante Sentencia C-1011 estudia la Ley 1266 de 2008, con la cual los ciudadanos disponen del Habeas Data para la protección de sus datos, y el derecho a toda información. Dicha ley establece que

> Se aplicará sin perjuicio de normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público (pág 1).

Aunque la ley cubre un gran espectro para la protección de los ciudadanos tiene como excepción las bases de datos estatales, tales como las de la Fuerza Pública y las del Departamento Administrativo de Seguridad DAS, las cuales se usan para garantizar la seguridad nacional.

Sin embargo el alcance de la corrupción ha tocado también esta Ley, haciendo que el DAS utilice la excepción de la norma haciendo infiltraciones a las comunicaciones telefónicas, correos electrónicos y mensajes de texto para hacer seguimiento e inteligencia a periodistas y personajes de la vida política con el fin de obtener información y manipularla al antojo de los intereses gubernamentales.

Sin embargo no solo la ley es mal utilizada por los servicios de inteligencia del gobiernos, muchas personas han sido estafadas o han visto su dinero desaparecer de los bancos gracias a empleados corruptos que entregan información bancaria de sus usuarios a bandas delincuenciales. La Ley 1266 en su artículo 4, establece principios para el manejo de la información, donde el primer principio toca directamente la privacidad de los datos de los usuarios por parte de los bancos. Reiteramos en esta investigación que el desconocimiento de la norma permite que los datos de las personas sean vulnerados y las empresas no hagan un correcto uso de ellos.

Los principios establecidos en el artículo 4 de la Ley 1266 de 20008 que se convierten en parte fundamental de la Ley y que deberían ser conocidos y aprendidos por los ciudadanos son.

Principio de Veracidad: "La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error"

Principio de finalidad: Los datos entregados por las personas deben obedecer a un fin que debe ser claro para la persona que la entregue**. "**La finalidad debe informársele al titular de la información previa o al momento con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto".

Principio de circulación restringida: los datos personales no tienen ningún tipo de accesibilidad, "salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados".

Principio de temporalidad de la información: "La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos".

Principio de interpretación integral de derechos constitucionales: "Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables". Esta ley establece que se ampararan los derechos de Hábeas data, buen nombre, honra, intimidad e información.

Principio de seguridad: La información contenida en los registros que alcanza la ley así como el resultado de consultas se deberá manejar con bajo todos los protocolos de seguridad existentes garantizando la que los registros estén seguros y "evitando su adulteración, pérdida, consulta o uso no autorizado".

Principio de confidencialidad: Las personas naturales o jurídicas que intercedan en la administración y uso de datos personales y que no estén clasificados como datos públicos están obligados a garantizar la reserva de dicha información.

Como lo encontramos en la realización de esta investigación, muchas de las personas que han sido suplantadas, se han enterado de que alguien al interior de alguna entidad ha hecho un mal uso de su información personal.

En la realización de esta investigación encontramos a una persona que fue víctima de un desfalco en el banco por culpa de un mal uso de su información privada financiera, según la víctima

> Fui al banco, pedí un extracto de mi cuenta de ahorros y lo guardé en la casa, más o menos 2 meses después volví al banco a retirar un dinero que necesitaba y sabía y que tenía según el extracto que había pedido anteriormente y me di cuenta de que alguien había sacado todo el dinero de mi cuenta, puse el denuncio en la fiscalía, contraté a un abogado y ahí me enteré que una persona que trabajaba en el banco y tenía acceso a los estados de cuenta había ayudado a una banda de delincuentes a retirar el dinero de mi cuenta (Areiza Sánchez, comunicación personal. Mayo 2022).

La víctima contó que antes de la pandemia cada que necesitaba hacer una diligencia bancaria le pedían su huella para que el banco pudiera hacer la verificación de su identidad y así evitar que se suplantara su identidad, en cambio con la llegada de la pandemia, y como muchos lo vivimos a duras penas revisaban bien la foto de la cedula para saber si coincidía o no con la persona que entrega la cédula.

La persona entrevistada cuenta que afortunadamente el banco le devolvió su dinero, sin embargo otras personas pasan por el calvario de no solo ser suplantadas y el temor que esto puede generar sino que también quedan con una deuda con algún almacén o con el propio estado, planteado por García Santiago (2021)

> Los controles de seguridad han sido dejados un poco de lado a la hora de diseñar el acceso ciudadano a trámites y soluciones virtuales. Muestra de ello son las denuncias publicadas en medios de comunicación, donde diversos clientes de entidades bancarias revelan cómo delincuentes les suplantan la identidad y sustraen dinero de sus cuentas sin su consentimiento. También piden créditos u otros productos financieros en cualquier ciudad del país sin que nadie se percate a tiempo de la estafa (parr 2).

Las personas que notifican haber sido suplantadas dicen que no saben que es más difícil, si recibir la noticia de la suplantación, darse cuenta de la deuda que tienen o hacer todo el proceso de denuncia. Para García Santiago "Lo más preocupante es que no son casos aislados…Los delincuentes aprovechan la debilidad de los sistemas informáticos o el desconocimiento de los usuarios para sustraer información" (2021, parr 3).

Se radicó en el congreso hace muy pocos días, un proyecto de ley que promueve la protección a los ciudadanos de suplantación personal en entornos digitales, el representante Duvalier Sánchez, ponente del proyecto en entrevista con el Diario El País (2022), informa que con este proyecto se busca que "a las víctimas se les suspendan los cobros de cartera y se les eliminen los reportes en las centrales de riesgo por las deudas que tengan debido a los productos o servicios que fueron adquiridos sin su consentimiento" (parr 3). Dicho proyecto deberá pasar 4 debates en el congreso antes de convertirse en ley y partir de ese momento podrá ser aplicado y entrara en vigencia.

La persona que ha sido suplantada tendrá 30 días para poner la denuncia ante la Fiscalía, una vez sea notificado a la entidad que su cliente ha sido víctima de fraude, la entidad deberá detener cualquier tipo de cobro por cuota, mora, y la víctima deberá ser retirada de centrales de riesgo.

Las entidades comerciales deberían mejorar en sus protocolos de seguridad, sobre todo en los protocolos de seguridad digital, a muchas personas les han realizado compras por medio de suplantación de identidad, la revista Semana, entrevisto a Camilo Zea fundador de la empresa Pronus. Según Zea en Semana (2022), indica que "Los robots permiten analizar las características biométricas de la persona y compararlas con el documento de identidad que presenta, para luego contrastarlo contra bases de datos y así saber si los

papeles son legítimos"(Parr 5). Para Zea se pueden presentar más errores teniendo protocolos de verificación de identidad a ojo humano que con elementos biométricos.

No se trata de satanizar el comercio electrónico, pero si es importante ser un poco más desconfiado de las páginas web y de las compras que se pueden hacer en ellas, sino de asesorarse mejor y evitar dar información importante en páginas web. Revisar las cookies que se van a aceptar, y no seguir enlaces sospechosos pueden ayudarle a evitar ser víctima de suplantación de identidad, sin embargo los delincuentes son bastante inteligentes y siempre logran su cometido. En entrevista con la Revista Semana (2021) el Coronel Julián Buitrago del centro cibernético de la Dirección de Investigación Criminal, Dijín, "los criminales cibernéticos logran estafar a las personas, robarse sus datos personales, extraer la información de los sitios bancarios y luego desaparecer sin dejar rastro" (parr 1).

En entrevista para RTVC noticias, Valentina Gómez, una de las muchas víctimas de suplantación de identidad y estafa en internet cuenta como se vio afectada por los delincuentes informáticos en Bogotá Valentina Gómez Acosta es una de las tantas víctimas de suplantación.

> Ella es una de las cientos de víctimas de suplantación de identidad, a la que inescrupulosos le han robado su identidad para estafar a su nombre. En su caso, al menos a 12 personas a través de reconocidas plataformas de comercio electrónico. De no ser por mensajes que recibió a través de sus cuentas de redes sociales, Valentina no se habría enterado jamás de que algunos delincuentes estaban vendiendo y comprando equipos tecnológicos a su nombre.

En el caso de Valentina se ven reflejados dos escenarios; las acciones malintencionadas de los delincuentes que usan la información para cometer fraude y al mismo tiempo, las virtudes de la informática, que permitieron que los conocidos se pudieran comunicar con ella para percatarla de lo que estaba pasando. Ante esto, se intuye que no se trata de dejar de utilizar los medios para evitar el delito, sino que se debe interactuar con cautela. Según la versión de Valentina, los delincuentes estaban vendiendo productos a su nombre, tenían su foto y su documento de identidad para parecer confiables.

Para evitar la suplantación se debe tener en cuenta la importancia de hacer un cambio periódico de contraseñas en cuentas de ahorro, correos electrónicos y redes sociales, así

como la actualización y continua verificación de su historial crediticio. Esto le ayudará a estar alerta ante cualquier cambio, también es muy importante para sus cuentas de ahorros tener activos los servicios de alertas y notificaciones, así como establecer un monto mínimo de compras, esto debería ser suficiente para evitar cualquier tipo de estafa.

No solo son las personas naturales las que se ven estafadas o dañadas en su reputación como en el caso de Valentina, también muchas empresas se ven dañadas en su buen nombre por los estafadores digitales, tal es el caso de la empresa Mercado Libre, a quienes por cuenta de los delincuentes cibernéticos se han visto gravemente afectados en su nombre y en sus ventas, en entrevista con Portafolio(2019), el director de la región Andina de Mercado Libre Jaime Ramírez, recomienda a quienes visitan su portal verificar tanto la reputación del vendedor como la descripción de los productos.

Para nadie es un secreto que desde las mismas cárceles se siguen cometiendo muchos delitos, entre estos delitos de fraude digital o extorsión, el plagio de cuentas constituye las mismas acciones delictivas más realizadas dentro de los penales. David Salazar, periodista del periódico La crónica del Quindío (2022), analiza la situación que se presenta desde las cárceles, lugares que incuban la operación de extorsiones, estafas y robo a la población por medio de llamadas o mensajes de texto en las que amedrentan, angustian o ilusionan a las víctimas. Para no caer en esta trampa

> se recomienda no aceptar solicitudes de amistad por parte de personas extrañas y denunciar ante la línea 123 de la Policía cuando lleguen mensajes de texto extraños como aquel que da cuenta de un supuesto premio de un sorteo en el que la víctima nunca se inscribió, generalmente este mensaje hace referencia a la entrega de un vehículo nuevo o a dinero en efectivo, por supuestos concursos que, en realidad, usurpan el nombre de empresas reconocidas a nivel nacional o internacional para captar la atención de las posibles víctimas (parr 6).

Los tan populares Call Center son un foco de delincuencia cibernética. En otro testimonio publicado por El Tiempo (2021), se conoció como los estafadores, brindan servicios y productos ficticios a través de este tipo de empresas

> Hicieron una primera llamada un día cualquiera, se presentaron a nombre de la franquicia de (...) que efectivamente es la tarjeta de crédito que manejo. Me dijeron que por mi buen manejo crediticio me había hecho beneficiaria de un paquete de servicios a un precio muy económico, narra Clara", aduciendo que quedó endeudada y que mes a mes le hacen un descuento de sus ingresos por un producto que nunca llegó a sus manos (parr 3).

Desde el call center del que llamaron a Clara, manipularon la información, hicieron la compra del paquete de salud y Clara hoy paga mensualmente una cuota de más de $50000 al banco.

No solo las personas de a pie son víctimas de estafas digitales, la reconocida periodista Jessica de La Peña, también pasó por la dura e incómoda experiencia de enterarse de que había sido víctima de robo cibernético y sus cuentas habían sido vaciadas “Me despierto a las 5:30 am y me encuentro con que se metieron a mi portal de Davivienda y me desocuparon mis cuentas. Incluso hasta me dejaron sobregirada. Todo lo hicieron durante la noche y madrugada mientras dormía” (twitter, 2021).

Y es que las personas jurídicas no están menos expuestas a estos delitos y es difícil controlar toda la información que se globaliza en el instante mismo en que se abre una página web "En Colombia el 83% de las compañías carecen de protocolos de respuesta a la violación de políticas de seguridad informática"(Portafolio, 2019, Parr 1)

Para Santiago Pinzón, vicepresidente de Transformación Digital de la Asociación Nacional de Empresarios de Colombia (Andi), en materia de prevención los empresarios todavía tienen un terreno muy importante por desarrollar, pues además es un tema que pasa por la cultura empresarial.

Sin embargo, y aunque mucho se habla del tema de la suplantación personal desde las propias víctimas, poco se ha investigado y poco se ha publicado, pero otra falencia se encuentra en el proceso de hacer la denuncia, y es que ya todos sabemos que la suplantación personal es un delito tipificado en el Código Penal, pero muy pocos sabemos cómo o donde hacer la denuncia. Díaz Gamboa, 2022 para Asuntos Legales explica, “se deben modificar las claves de las cuentas adscritas a sus dispositivos, para evitar futuras

suplantaciones. Posteriormente, se debe acudir a la Fiscalía o Policía Nacional para interponer la respectiva denuncia por el delito de falsedad personal" (parr 6).

Lo cierto es que no solamente Colombia está sufriendo por la suplantación de identidad, países como Perú también se encuentran en el proceso de tipificarlo como delito en su código Penal, pero hasta el momento de esta investigación, es el único país que considera la suplantación personal como un daño moral

> Desde el 21 de octubre del año 2013 existe la Ley Nº 30096 que regula los delitos informáticos, siendo el artículo 9 de dicha ley que tipifica el delito de suplantación de identidad como el delito en que una persona puede suplantar la identidad de una persona jurídica o natural ocasionando un perjuicio material o moral (Aldecoa Jiménez, 2020, pág 10).

Aldecoa Jiménez (2020) no sataniza los avances tecnológicos pero hace una sugerencia bastante importante "Así como estas nuevas tecnologías y transformación digital es evolutiva, constantemente las normas y los organismos reguladores deben ir a la par con esta evolución" (pág. 10).

Las cifras de suplantación personal en el Perú son casi tan impresionantes como las de Colombia, en este país el delito de suplantación personal en internet para el año 2021 aumentó en un 92,9% con respecto a las denuncias interpuestas en el 2020 datos entregados al diario El Peruano (2022), por parte de la Policía Nacional del Perú indican que "La modalidad de suplantación de identidad ocupa el segundo lugar en la lista de delitos cibernéticos. Este delito pasó de registrar 935 denuncias en el 2020, hasta un total de 2.666 para el 2021" (Parr 7).

Aunque el panorama es bastante alarmante, las cifras y la falta de una legislación más dura no ayuden, existen países donde la situación es muchísimo peor de la que nosotros estamos presenciando, nuestro vecino país Venezuela, según el portal Valora Analitik (2021), quienes no solo tienen una alta tasa de denuncias pro suplantación personal sin que también son el país de Latinoamérica donde más se cometió el delito de robo de datos por internet a través de correos electrónicos, descargas de aplicaciones y violación de contraseñas. (Mejor conocido como phishing). "Los piratas electrónicos buscan que un individuo descargue malware o dé información personal a través del correo electrónico o el

teléfono, explotando su miedo, ansiedad, curiosidad y confianza" (Valora Analitik, 2021, parr 4), recomienda a las personas:

> Evite descargar programas y apps gratuitos de sitios inseguros en tus dispositivos electrónicos.
>
> Cree claves robustas distintas para cada cuenta, evitando que tengan relación con tus datos personales, tales como fechas de nacimiento, teléfonos o nombres.
>
> Conserve sus documentos personales, físicos y electrónicos, así como sus contraseñas, en lugares seguros.
>
> Destruya documentos con información personal, financiera o sensitiva, así como tarjetas bancarias vencidas.
>
> Evite abrir correos electrónicos de origen sospechoso que soliciten información personal o financiera.

Para el caso de Argentina el panorama es muchísimo más preocupante, dado que este país ni siquiera contempla la suplantación de identidad como delito,

> La suplantación de identidad digital no es un delito en la Argentina… Existen una serie de conductas que efectivamente no se encuentran tipificadas en el Código Penal ni en leyes complementarias. Me refiero al robo, sustitución o usurpación de identidad digital… esa conducta no constituye delito, en tanto y en cuanto se trataría de un acto preparatorio de otro delito (Pilnik, 2021).

Uno de los países que históricamente conocemos por la dureza de su legislación y la aplicación de sus leyes sin contemplaciones es Estados Unidos, estos no escaparon del delito de fraude personal y robo de identidad.

Dicha situación, al igual que en Latinoamérica aumentó con la emergencia sanitaria del Covid 19, La Comisión Federal de Comercio indicó que en 2021 recibieron 1.4 millones de denuncias por robo de identidad en el año 2020. Gressin 2021 citada en Owaida 2021 asegura que

> Las denuncias por robo de identidad a la FTC coinciden con la caída del empleo a nivel nacional. Después de que el gobierno otorgó subsidios a las personas que quedaron sin trabajo por la pandemia, los ciberdelincuentes se anotaron para recibir estas ayudas utilizando información personal de otras personas (parr 3).

Según Owaida 2021 "Los ciberdelincuentes utilizaron el robo de identidad como un medio para obtener acceso a los pagos de estímulo federal emitidos por el Servicio de Impuestos Internos de los EEUU, incluso los ciberdelincuentes cometen fraude con la devolución de los impuestos" (parr 6).

España no sale bien librado del delito de suplantación personal, y su legislación es muy clara. Puede ser casi el único país que entiende el delito de robo de identidad o usurpación como un delito carcelable. El artículo 401 del Código Penal Español refiere: "el que usurpare el estado civil de otro será castigado con la pena de prisión de seis a tres años" (Código Penal Español, 2015).

Según Marín y Oquendo, 2021 "En España en 2019 hubo alrededor de 300 casos, en 2020 la cifra se disparó a 1.527 reportes. España es el país de la Unión Europea en el que se registran más suplantaciones de identidad, según la Oficina Europea de Estadísticas"(Parr 4).

La Unión europea protege a todos sus ciudadanos

> La Directiva protege el derecho fundamental de los ciudadanos a la protección de sus datos cuando los utilicen las autoridades policiales y judiciales a efectos de aplicación de la ley. Más concretamente, la Directiva garantizará que se protejan adecuadamente los datos personales de víctimas, testigos y sospechosos de delitos, además de facilitar la cooperación transfronteriza en la lucha contra la delincuencia y el terrorismo (Comisión Europea, S.F. Parr 7).

Para el caso de EEUU, recientemente están empezando a aplicar estrategias y leyes para el tratamiento y protección de los datos de los usuarios. En el estado de California, en 2020 comenzó a regir la Ley de protección al consumidor. "Se trata de la primera legislación en Estados Unidos que da a los consumidores control sobre cómo se usa su información

personal en línea, del mismo modo que el Reglamento General de Protección de Datos" (Renter Barcelona, 2020. Parr 3).

No todo está perdido, el despliegue de La regulación general de protección de datos (GDPR) por sus siglas en inglés

> Está teniendo un impacto en las empresas de todo el mundo, gracias a su alcance legislativo más allá de las fronteras de la UE. Pero las empresas también tienen que contentarse con la nueva legislación sobre privacidad de datos en los Estados Unidos, el Reino Unido, China y muchos otros países. Algunas leyes están inspiradas en el GDPR, mientras que otras adoptan un enfoque único que satisface las necesidades de su país (Stranieri, 2019, parr 1).

En cuanto a políticas claras en la protección de datos a los ciudadanos y al consumidor, Colombia es un país adelantado en el tema, aun así no escapa al delito del fraude digital. Sin embargo es importante rescatar la ventaja que lleva en materia de protección de datos y leyes que sancionan el fraude digital y la manipulación indebida de datos personales sobre otros países como Estados Unidos por ejemplo.

Paradójicamente, siendo Colombia uno de los países con más aumento de fraude digital, y teniendo en el último año un aumento importante en ese delito, se celebró en Medellín La II Jornada STIC Capítulo Colombia, presente en este evento estuvo el entonces Ministro de Defensa Diego Molano quien aseguró que el Ministerio de Defensa busca fortalecer las capacidades de la fuerza pública para proteger la seguridad nacional, incluyendo el Ciberespacio. (Red de gobierno electrónico de América Latina y el Caribe, 2022). No hay que olvidar que solo para el año 2021, se habían recibido 48.831 denuncias y se habían bloqueado 150.000 sitios con contenido malicioso (Salazar, 2022).

El estado colombiano ha venido trabajando en cabeza de la Registraduría Nacional del Estado Civil en diseñar estrategias que eviten la suplantación y el uso indebido de los documentos. Una de estas estrategias es la nueva, poco conocida pero eficaz Cédula Digital, esta será de carácter gratuito para quienes la expidan por primera vez. Uno de los beneficios más importantes que tendrá la nueva cédula digital es como lo expresa la misma Registraduría Nacional del Estado Civil, con la nueva cédula digital la ciudadanía contará

con “la imposibilidad de falsificación o adulteración, la identificación y autenticación biométrica, la imposibilidad de suplantación o usurpación de identidad, la protección de datos personales y el ingreso sin pasaporte a todos los países miembros de la Comunidad Andina” (Registraduría Nacional del Estado Civil, 2022, parr 9).

Según palabras del registrador Alexander Vega “esto ayudará a prevenir el crimen, protegerá los datos personales de los ciudadanos, mejorará su calidad de vida y será amigable con el medioambiente” (Vega en El Tiempo, 2022, parr 6). La duda que surgirá en muchos ciudadanos usuarios de cédula digital es ¿qué pasa con su nueva cédula en caso de pérdida o robo del celular?, a esto responde la registraduría “si pierde su celular y en él tenía su cédula digital, debe reportar su pérdida para inhabilitarla; podrá estar seguro de que nadie la utilizará” (El Tiempo, 2022, parr 17).

La vigencia de la cédula digital será de 10 años, y deberá ser actualizada basada en los cambios y actualizaciones de sistemas biométricos.

Como medida de protección ante la falsedad personal, también se ha venido trabajando en el sistema biométrico de reconocimiento de huella dactilar

> Por ser considerado como un método seguro y efectivo en controles de acceso de entrada y salida, autorizar operaciones sensibles, evitar acceso a zonas restringidas y establecer plena identidad, esto gracias a que es única en cada ser humano y con el pasar del tiempo, los avances tecnológicos será nuestra firma digital (Maya Vargas, 2013, pág 26).

El sistema biométrico no es un sistema infalible hablando de seguridad. Es un sistema que tiene múltiples vulnerabilidades comparado con otros sistemas de control de acceso. Este tipo de vulnerabilidades pueden ser saneadas realizando una auditoría de control pertinente y a tiempo, podría evitarse la suplantación o infiltración de los sistemas que causaría una pérdida de recursos tangibles e intangibles importantes para el correcto funcionamiento empresarial (Maya Vargas, 2013).

La implementación de equipos biométricos para la seguridad de los datos, requiere de un alto presupuesto, pero también requiere un arduo trabajo para duplicar la seguridad de la información,

> Los datos pueden capturarse durante la transmisión a la base de datos central y pueden replicarse, de manera fraudulenta, en otra transacción. El resultado es que una persona puede perder el control de sus propios datos, presentando grandes riesgos en términos de privacidad las autoridades de protección de los datos parecen preferir las soluciones que cuentan con dispositivos de datos descentralizados (Thales Group, S. F. Parr 58).

Las herramientas biométricas no son del todo seguras, en muchos casos los delincuentes se valen de plastilina, polvos magnéticos o silicona líquida pueden tomar una copia de la huella dactilar y hacer un uso indebido de ella.

Joel Martin Visurraga Agüero, perito dactiloscópico reconocido especialista en biometría, invitado por el diario El Comercio de Perú (2021), da pautas para la protección de las huellas digitales y evitar que por medio de estas sea víctima de fraude que no son solo útiles en escenarios de Perú sino también a nivel internacional. El experto recomienda:

> Que la huella dactilar no sea el único mecanismo de ingreso a tus aplicaciones más importantes. Es mejor solo aceptar, registrar y pasar la identificación biométrica en establecimientos y entidades de suma confianza. No tener huella dactilar digitalizada en el celular, ya que el equipo puede perderse o sufrir un robo, lo que hace más probable aún que la huella caiga en manos de algún delincuente. Si identificas alteraciones en los lectores de huella no los utilices (parr 5).

Conclusiones

Con esta investigación se concluye que el flagelo de la suplantación de identidad no es solo para Colombia sino que es un delito internacional.

La parte más preocupante de esta investigación se deriva en que así como en Colombia, el resto de países que fueron mencionados aquí tienen una legislación y una caracterización del delito insuficiente para dicho crimen, aunque la mayoría de estos tengan en sus códigos penales la tipificación de delito para la suplantación de identidad las penas o castigos son mínimos para quienes cometen dicho delito.

Con los avances tecnológicos, los castigos para los delincuentes de delitos informáticos deberían volverse una prioridad para la justicia de los países que aunque tienen este delito tipificado siguen viendo en aumento las denuncias de víctimas de este tipo de delitos.

Es importante que los ciudadanos tomen conciencia de la importancia del cuidado de sus datos.

Se concluye así mismo la importancia de establecer y promocionar el cuidado de los datos entre los ciudadanos para evitar el delito de suplantación. Logramos identificar que la mayoría de las personas que han sido víctimas de este delito están desinformadas acerca de la vulnerabilidad de sus datos.

Se concluye además que nunca los esfuerzos en la protección de datos serán suficientes, existe una insuficiente cultura de la verificación de páginas web, cambio de contraseñas y uso de contraseñas seguras, así como la falta de conciencia y responsabilidad en la verificación de estados de cuenta e historiales crediticios.

Referencias.

Acosta Argote, C. (12 de abril de 2021). Delito de suplantación de identidad aumentó 409% en 2020 debido a la pandemia. *Asuntos Legales*. https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-2020-debido-a-la-pandemia-3151651

Aldecoa Jiménez, M. d. R. (2020). El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019. https://hdl.handle.net/20.500.12692/61838

Código Penal. [CP]. Artículo 240. 2009 (Colombia). Legis Editores. https://xperta.legis.co/visor/legcol/legcol_7599204254d4f034e0430a010151f034/coleccion-de-legislacion-colombiana/ley-1273-de-enero-5-de-2009---ley-1273-de-2009

Código Penal Español. [CPE]. Artículo 401 del Código Penal. 2015 (España). https://www.conceptosjuridicos.com/codigo-penal-articulo-401/

Código de Procedimiento Penal. [CPP]. 599 .Articulo 296. 24 de julio de 2000 (Colombia). Legis Editores. https://xperta.legis.co/visor/penalpro/penalpro_bf1a5f53632649f42e38891665e21476688nf9/codigo-penal-y-de-procedimiento-penal-basico/capitulo-unico

Comisión Europea. (2018). *La protección de datos en la UE: The General Data Protection Regulation (GDPR), the Data Protection Law Enforcement Directive and other rules concerning the protection of personal data*. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es

Constitución Política de Colombia. [Const]. Artículo 15. Julio 7 de 1991 (Colombia). Legis editores.

Congreso de la República de Colombia (Enero 05, 2009). Ley 1273 de 2009 “de la protección de la información y de los datos”. D.O. 47223.Legis Editores. https://xperta-legis-

co.luisamigo.proxybk.com/visor/legcol/legcol_bf11a8a7d3c88cc486fb007e4b8b70c1a6enf9/

Corte Suprema de Justicia. Sala Penal. NO CASAR la sentencia ameritada (Fernando Enrique Arboleda Ripoll; 28 junio 2000). https://app.vlex.com/#vid/691878689

Corte Suprema de Justicia. Sala Penal. NO CASAR la sentencia impugnada (María del Rosario González de Lemus; 30 Abril 2008). https://app.vlex.com/#vid/43756275

De la Peña, J. [@Jessie_dlp]. (7 octubre de 2021). [Tweet]. Twitter. https://twitter.com/Jessie_Dlp?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor

Díaz Gamboa, S. (mayo 2022). ¿Sabe lo qué debe hacer en caso de que sea víctima del delito de suplantación de identidad? *Asuntos legales*. https://www.asuntoslegales.com.co/consumidor/que-debe-hacer-en-caso-de-ser-victima-del-delito-de-suplantacion-de-identidad-3357134#:~:text=Uno%20de%20estos%20es%20la,ilegal%20de%20personas%20o%20empresas.

El Comercio, (Diciembre 2021). ¿Cómo proteger mi huella dactilar y evitar una suplantación de identidad? *El comercio. Perú*. https://elcomercio.pe/casa-y-mas/ideas-y-diseno/tecnologia-como-proteger-mi-huella-dactilar-y-evitar-una-suplantacion-de-identidad-nndc-noticia/?ref=ecr

El país. (Octubre de 2022). Radican en el Congreso proyecto de ley para proteger a víctimas de suplantación digital. *Redacción política. Diario El País*. https://www.elpais.com.co/politica/radican-en-el-congreso-proyecto-de-ley-para-proteger-a-victimas-de-suplantacion-digital.html

El Peruano, (Septiembre 2022). Denuncias por delitos informáticos se incrementaron en más del 90% en el Perú. . https://www.elperuano.pe/noticia/188048-denuncias-por-delitos-informaticos-se-incrementaron-en-mas-del-90-en-el-peru#:~:text=Esto%20significa%20que%203%20de,mil%20666%20para%20el%202021.

El Tiempo. (2021). El testimonio de una víctima de estafadores a través de 'call center'. https://www.eltiempo.com/justicia/delitos/estafa-testimonio-de-victima-que-robaron-a-traves-de-call-center-595708

El Tiempo. (2022). *Cédula digital: ¿quién la debe tramitar y desde cuándo?*. https://www.eltiempo.com/politica/gobierno/cedula-digital-todo-lo-que-necesita-saber-para-hacer-el-cambio-699707

García Santiago, H.J. (2021). Qué responsabilidad le atañe al banco cuando suplantan su identidad. *Portafolio*. https://www.eltiempo.com/bogota/suplantacion-que-hacer-si-alguien-suplanto-mi-identidad-y-tengo-una-deuda-657242

Ley 1341 de 2009 .Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC. 2009. DO. N°47426.

Ley 1266 de 2008 Por la cual se dictan las disposiciones generales del hábeas data. DO. N°47.219. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488#:~:text=HABEAS%20DATA&text=Dicta%20las%20disposiciones%20generales%20del,la%20proveniente%20de%20terceros%20pa%C3%ADses.

Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 2012. DO. N°48587. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

Maqueo Ramírez, M. S. (2016). Análisis comparativo de las resoluciones emitidas por el tribunal de justicia de la unión europea y el instituto federal de acceso y protección de datos respecto del motor de búsqueda gestionado por Google y la protección de datos personales. *Boletín Mexicano de Derecho Comparado*, *49*(145), 75-100. https://doi.org/10.22201/iij.24484873e.2016.145.4992

Marín, E. & Oquendo, C. (2021). *Suplantación de identidad a través de Internet: comparativa entre España y Colombia*. Confilegal. https://confilegal.com/20210924-opinion-suplantacion-de-identidad-a-traves-de-internet-comparativa-entre-espana-y-colombia/

Maya Vargas, A. (2013). S*istema biométrico de reconocimiento de huella dactilar en control de acceso de entrada y salida* [Tesis de Especialización en Administración de la seguridad, Universidad Militar Nueva Granada].https://core.ac.uk/download/pdf/143449128.pdf

Ojeda Pérez, J. E., Rincón Rodríguez, F., Arias Flórez, M. E., y Daza Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad*, 11(28), 41-66. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Ortiz Rodríguez, A. (1980). La falsedad en documentos en el nuevo código penal. *Nuevo Foro Penal*, 8, 11. https://heinonline.org/HOL/LandingPage?handle=hein.journals/nuefopnl8&div=5&id=&page=

Owaida, A. (Febrero 2021). *El robo de identidad aumentó durante la pandemia*. *We Live Security*. https://www.welivesecurity.com/la-es/2021/02/04/el-robo-de-identidad-aumento-durante-la-pandemia/#:~:text=La%20Comisi%C3%B3n%20Federal%20de%20Comercio,el%20doble%20que%20en%202019.

Peña Valenzuela, D. (2021). La protección de datos personales: entre lo público y lo privado. *Blog de derecho de los negocios*. https://dernegocios.uexternado.edu.co/la-proteccion-de-datos-personales-entre-lo-publico-y-lo-privado/

Pilnik, F. (Diciembre 2021). *Comentarios sobre la suplantación de identidad digital* . *Ministerio de Justicia y derechos humanos. Argentina.* http://www.saij.gob.ar/franco-pilnik-comentarios-sobre-suplantacion-identidad-digital-dacf210223-2021-12-16/123456789-0abc-defg3220-12fcanirtcod?&o=0&f=Total%7CFecha%7CEstado%20de%20Vigencia%7CTema/Derecho%20civil/persona%20humana/identificaci%F3n%20de%20las%20personas/documentos%20de%20identidad%7COrganismo%5B5%2C1%5D%7CAutor%5B5%2C1%5D%7CJurisdicci%F3n%5B5%2C1%5D%7CTribunal%5B5%2C1%5D%7

CPublicaci%F3n%5B5%2C1%5D%7CColecci%F3n%20tem%E1tica%5B5%2C1%5D%7CTipo%20de%20Documento&t=307

Presidencia de la República de Colombia. (28 de mayo de 2020). Gobierno Nacional expide el Decreto 749, mediante el cual ordena el Aislamiento Preventivo Obligatorio en el país a partir del 1° de junio. *Oficina de prensa*, https://id.presidencia.gov.co/Paginas/prensa/2020/Gobierno-Nacional-expide-Decreto-749-mediante-el-cual-ordena-Aislamiento-Preventivo-Obligatorio-en-el-pais-a-partir-200528.aspx#:~:text=Mediante%20el%20Decreto%20749%20del,Sanitaria%20por%20causa%20del%20coronavirus

Portafolio, (Enero de 2019). El secuestro de información desangra a las empresas del país. https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729

Portafolio, (Mayo de 2019). Así son las estafas al comprar y vender productos por internet. . https://www.portafolio.co/economia/finanzas/asi-son-las-estafas-al-comprar-y-vender-productos-por-internet-529139

RCTV Noticias, (Noviembre de 2021). La historia de joven víctima de suplantación de identidad. . https://www.rtvcnoticias.com/historia-joven-victima-suplantacion-identidad

Real Academia de la Lengua. RAE. (S.F). Diccionario de la lengua española: *Definición de Falsedad*. Real Academia Española. https://dle.rae.es/falsedad?m=form

Realpe, G. (S.F.). Los tipos de responsabilidad por el mal manejo de datos en los delitos informáticos y en la protección de datos personales. https://www.cloudseguro.co/responsabilidad/

Red de gobierno electrónico de América Latina y el Caribe. (Marzo 17 de 2022). *II Jornada STIC. Capítulo Colombia*. https://www.redgealc.org/contenido-general/noticias/ii-jornada-stic-capitulo-colombia/

Registraduría Nacional del Estado Civil. (2022). *A partir de hoy, comienza la masificación de la cédula digital en nuestro país*. Registradora Nacional del Estado Civil. Oficina de prensa. https://www.registraduria.gov.co/A-partir-de-hoy-comienza-la-masificacion-de-la-cedula-digital-en-nuestro-pais.html#:~:text=Recordemos%20que%20los%20principales%20beneficios,el%20ingreso%20sin%20pasaporte%20a

Renter Barcelona, A. M. (2020). *La primera ley de privacidad en línea de EE.UU. entra en vigor en California*. . https://www.lavanguardia.com/vida/20200105/472713380363/california-estados-unidos-privacidad-consumidor-e-commerce-comercio-electronico.html

Rojas Bejarano, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum Jus: revista especializada en sociología jurídica y política*, 8(1), 107-139. https://app-vlex-com.luisamigo.proxybk.com/#search/jurisdiction:CO/datos+personales/WW/vid/786997809

Salazar, D. (marzo 22 de 2022). Plagio de cuentas, el delito informático más común en el Quindío. *La crónica del Quindío*. https://www.cronicadelquindio.com/noticias/judicial/plagio-de-cuentas-el-delito-informatico-mas-comun-en-el-quindio

Semana. (Diciembre de 2021). Delitos cibernéticos ascendieron un 17 % en Colombia durante 2021. *Redacción Nacion. Revista Semana. https://www.semana.com/tecnologia/articulo/delitos-ciberneticos-ascendieron-un-17-por-ciento-en-colombia-durante-2021/202116/*

Semana. (Enero de 2022). Suplantación de identidad, un flagelo que está al alza. *Redacción Delitos. Revista Semana*. https://www.semana.com/economia/macroeconomia/articulo/suplantacion-de-identidad-un-flagelo-que-esta-al-alza/202214/

Stranieri, S. (2019). *Leyes globales de privacidad de datos: USA, UE, China y más*. . https://www.ipswitch.com/es/blog/leyes-globales-de-privacidad-de-datos-usa-ue-china-y-mas

Suarez Sánchez, A. (2016). *Manual de delito informático en Colombia: Análisis dogmático de la ley 1273 de 2009*. Universidad Externado de Colombia. https://www-digitaliapublishing-com.luisamigo.proxybk.com/a/68720

Superintendencia de Industria y Comercio. SIC. (S.F). *Sobre el régimen general de Protección de Datos Personales*. https://www.sic.gov.co/informacion-sobre-la-proteccion-de-datos-personales

Tantaleán Odar, R. M. (2016). Tipología de las investigaciones jurídicas. *Derecho y cambio social*, 13(43), PP. 2-37. https://dialnet.unirioja.es/servlet/articulo?código=5456267

Thales Group, (S.F). Biometría para identificación y autenticación. https://www.thalesgroup.com/es/countries/americas/latin-america/dis/gobierno/inspiracion/biometria

Valora Analitik. (Agosto, 2021). *Colombia, cuarto en América más amenazado por robo de identidad*. https://www.valoraanalitik.com/2021/08/20/colombia-cuarto-en-america-mas-amenazado-por-robo-de-identidad/

World Legal Corporation. (2021). Delitos informáticos en Colombia. *World Legal Corporation*. https://www.worldlegalcorp.com/blog/delitos-informaticos-en-colombia/

Zhao, H. (2011). La Cumbre Mundial sobre la Sociedad de la Información y la brecha de la banda ancha: obstáculos y soluciones. https://www.un.org/es/chronicle/article/la-cumbre-mundial-sobre-la-sociedad-de-la-informacion-yla-brecha-de-la-banda-ancha-obstaculos-y