72

Fecha de presentación: junio, 2022
Fecha de aceptación: agosto, 2022
Fecha de publicación: noviembre, 2022

# REGULACIÓN GLOBAL

## PARA EVITAR LA SUPLANTACIÓN DE IDENTIDAD DIGITAL

## GLOBAL REGULATION TO PREVENT DIGITAL IDENTITY THEFT

Pamilys Milagros Moreno Arvelo[1]
E-mail: uq.pamilysmoreno@uniandes.edu.ec
ORCID: https://orcid.org/0000-0001-8913-4352
Cesar Elías Paucar Paucar[1]
E-mail: uq.cesarpaucar@uniandes.edu.ec
ORCID: https://orcid.org/0000-0003-2624-0427
Cinthia Mariela Cajas Parraga[1]
E-mail: uq.cinthiacajas@uniandes.edu.ec
ORCID: https://orcid.org/0000-0003-2644-0074
[1] Universidad Regional Autónoma de los Andes¬ Quevedo. Uniandes

Cita sugerida (APA, séptima edición)

Moreno Arvelo, P. M., Paucar Paucar, C. E., Cajas Parraga, C. M., (2022). Regulación global para evitar la suplantación de identidad digital. *Revista Universidad y Sociedad*, 14(6), 690-696.

RESUMEN

El siguiente trabajo trata sobre la suplantación de identidad digital, siendo tratado como una realidad del desarrollo de la tecnología. Lo que busca esta investigación es realizar un análisis de la suplantación digital que lleve a una propuesta de regulación jurídica para garantizar el derecho humano a la identidad. Los métodos aplicados en la investigación fueron el sintético y el inductivo, siendo utilizada como instrumento la entrevista, misma que se hizo a expertos en el área del derecho tecnológico y penal. Se llegó a la conclusión de que en algunos Estados es más desarrollada que en otras la regulatoria de la suplantación de identidad, es necesario una regulación global ante esta problemática, a través de tratados internacionales que ayuden a la solución sobre este tema.

Palabras clave: Identidad digital, suplantación de identidad, regulación jurídica, derecho humano a la identidad.

ABSTRACT

The following work deals with digital identity theft, being treated as a reality of the development of technology. The purpose of this research is to perform an analysis of digital impersonation that leads to a proposal of legal regulation to guarantee the human right to identity. The methods applied in the research were synthetic and inductive, being used as an instrument the interview, which was made to experts in the area of technological and criminal law. It was concluded that in some States the regulation of identity theft is more developed than in others, it is necessary a global regulation of this problem, through international treaties that help to solve this issue.

Keywords: digital identity, identity theft, legal regulation, human right to identity.

## INTRODUCCIÓN

La identidad humana es el conjunto de características que diferencian a una persona de otra, formada por rasgos que le son propio y de la interacción humana, que evoluciona con el tiempo. Este concepto de identidad se ha ampliado a la identidad digital, producida por los datos suministrados por la persona, las acciones realizadas dentro del mundo digital y las inferidas por terceras personas de las acciones ejecutadas por el individuo.

La identidad es un derecho humano fundamental recogido en la mayoría de los textos constitucionales, como un derecho que el Estado debe garantizar; la Declaración Universal de los Derechos Humanos, en sus artículos 6 y 12, se refieren al derecho de la personalidad y a la privacidad. La identidad es parte del ser de la persona, de sus rasgos que lo individualizan del resto de los miembros de la sociedad. Sin embargo, no todos los individuos gozan de este derecho, por lo cual sigue siendo un punto por realizar dentro de los objetivos de desarrollo sostenible para el 2030 (Naciones Unidas, 2016). En cuanto a la identidad digital, no se ha configurado como derecho, se ha discutido, sobre el derecho a la privacidad en el mundo digital, pero no se ha configurado la identidad digital como derecho, así lo precisa (Sullivan, 2018) quien sostiene la necesidad de su reconocimiento.

La identidad puede ser estática o dinámica, la identificación estática significa el almacenamiento en un registro público, para distinguir a una persona del resto; mientras, la identidad dinámica, viene dada, por las interacciones que realiza una persona dentro del entorno digital.

En la "sociedad digital" la identidad estática y la identidad dinámica se interrelacionan en las bases de datos, en las redes sociales y en los distintos sistemas de información, la identidad de las personas es esencial para que las personas puedan acceder a servicios y realizar distintas actividades con relevancia jurídica como son: el comercio electrónico, los negocios electrónicos, el gobierno electrónico, la educación digital y el desenvolvimiento de la persona humana en la "sociedad digital" (Núñez, 2016).

El desarrollo de nuevas tecnologías y la interacción que las personas realizan en medios virtuales, en los cuales se almacena información personal, es cada vez mayor y natural, al punto que como afirma (Área, 2011) han alcanzado tal grado de penetración y omnipresencia en nuestra vida que sin ellas carecemos de identidad y presencia social. Tenemos una identidad reconocible y bien definida en la vida real, pero nuestra identidad como sujeto será incompleta si carecemos de visibilidad en los mundos de comunicación virtuales.

Se han realizado estudios e intentos de implementar a gran escala y con alto nivel de privacidad la identidad digital para uso público en las relaciones con el Estado, ejemplo es el caso de India, que posee una población muy numerosa, y para quien la identidad digital se presenta como una oportunidad y garantía del Estado (Mir et al., 2020).

La identidad digital es el resultado de los cambios y desarrollo tecnológicos actuales, que, a producidos efectos positivos como las compras en línea, el voto electrónico, la suscripción de documentos mediante firma digital, los contratos inteligentes; sin embargo, las plataformas de identidad digital pueden producir resultados no deseados o degenerativos (Masiero & Arvidsson, 2021). Tal situación plantea la necesidad de protección y privacidad de dichos datos, siendo necesaria una regulación jurídica al respecto; sin embargo, careciendo el mundo digital de fronteras, dificulta el ámbito de regulación por parte del Estado. La necesidad de la regulación jurídica radica ante los problemas presentados por suplantación de identidad digital, que conlleva a la sustracción de dinero de cuentas bancarias, deterioro de la reputación personal, entre otros delitos.

La suplantación de identidad implica que una persona actuando dolosamente, sustituye a otra persona en el mundo digital, usando las contraseñas de acceso de la persona, ingreso no autorizado a perfiles, creación de perfiles falsos, generando daños económicos o del buen nombre del titular de la identidad digital. Quien suplanta la identidad, puede utilizar información subida a la red por el propio suplantado, como fotografías, datos de identificación, estado civil, residencia, números telefónicos, entre otros, ya que, al subir una información a internet, se pierde el control sobre esos datos, los cuales pueden ser distribuidos rápidamente. Paralelamente, a la suplantación de identidad está el derecho a la privacidad, el cual se ve vulnerado con publicaciones no autorizadas que exceden la libertad de información, ya que viola el derecho a la intimidad, así como los casos de publicaciones falsas o descontextualizadas.

Todo lo expresado anteriormente, lleva a la interrogante de ¿Cómo regular jurídicamente la suplantación de identidad digital? De allí que la investigación se planteó como objetivo realizar un análisis de la suplantación de digital que conlleve a una propuesta de regulación jurídica que garantice el derecho a la identidad y a la protección y privacidad de los datos almacenados en el mundo digital. Para ello, se partió de la fundamentación teórica del concepto identidad digital, pasando por el diagnóstico de la regulación jurídica de la identidad digital, y finalmente, el desarrollo de la propuesta de regulación jurídica.

Se empleó un enfoque cualitativo, de alcance propositivo, siendo los métodos utilizados el analítico sintético y el inductivo, como instrumento se usó la entrevista a una muestra de expertos en el área del derecho informático y penal, tanto de experiencia académica como práctica en el ejercicio de la función jurisdiccional. Respecto a las consideraciones éticas de la investigación, se obtuvo el consentimiento de los entrevistados, y se les planteó los objetivos de la investigación, participando consciente y libremente, pudiendo expresar libremente sus ideas y con la libertad de poder finalizar la entrevista si así lo consideraban, por lo que se reitera su participación libre sin fraude o coacción.

## DESARROLLO

## MATERIALES Y MÉTODOS

La investigación se realizó con un enfoque cualitativo, que permitió profundizar el objeto de estudio en los elementos característicos del mismo, apoyándose en los métodos analíticos sintético e inductivo, para descomponer la categoría identidad digital desde su manifestación en la realidad que llevó a una propuesta general de regulación jurídica del fenómeno investigado. La investigación es bibliográfica de tipo documental y de campo, por consiguiente, un diseño experimental. Se utilizaron las técnicas del análisis de contenido de las unidades de análisis, y la entrevista a una muestra de expertos, que fue la forma como se recolectaron los datos.

Para la selección de los expertos se tomó en consideración la experticia en el área penal y/o derecho informático, tanto académica como práctica en el ejercicio de funciones jurisdiccionales. El instrumento para la entrevista fue la guía de entrevista estructurada, ya que se respetó la cantidad, tipo y orden de las preguntas a todos los expertos; las preguntas fueron abiertas, pudiendo los entrevistados responder libremente de acuerdo a su experiencia y conocimiento.

Las preguntas realizadas exploraron la categoría regulación jurídica, ya que, con ellas, se procuraba diagnosticar la situación jurídica de la suplantación de identidad y las propuestas para su regulación desde la mirada de los expertos. Las preguntas fueron: ¿Existe en su país el delito de suplantación de identidad digital?, ¿Considera que es necesario establecer el delito de suplantación de identidad digital?, ¿Cuáles serían los elementos que configurarían el delito de identidad digital? Según su opinión, ¿cuáles serían las pruebas para este tipo de delito?, ¿Cuál mecanismo jurídico, considera el más idóneo para garantizar el derecho a la identidad personal?, ¿Es suficiente la tipificación del delito de suplantación de identidad digital por cada Estado, o considera que debe regularse de una manera global?

Para garantizar la confiabilidad y validez de los datos se acudió a la triangulación: Teórica, metodológica y de fuentes, confrontando diversas fuentes, teoría sobre el tema y utilizando diversos métodos dentro de la investigación, estableciendo las correspondientes distancias epistémicas.

Los datos obtenidos de las entrevistas fueron tabulados utilizando el análisis de contenido, identificación de unidades de análisis, se procedió a lectura de la transcripción de las respuestas dadas por los entrevistados, tomando en cuenta el objetivo e identificando los puntos en común y diferencia entre los expertos, y así obtener los datos relevantes hasta alcanzar la saturación.

## RESULTADOS

Los expertos coinciden en la poca o nula regulación del delito de suplantación de identidad digital por parte de los Estados, considerando la necesidad de su tipificación ante el auge de las tecnologías y el uso en las múltiples actividades de la vida cotidiana. Y debido a que, en materia de delitos no se puede aplicar la analogía, es impretermitible una perfecta adecuación entre la conducta desplegada por el sujeto y el tipo penal previsto en la norma. De allí, que se requiera el apoyo transdisciplinario de la informática forense y la criminología para realizar configurar desde la teoría del delito el delito de suplantación de identidad digital. Siendo los principales elementos de este delito, los señalados en la figura 1.

El cambio y desarrollo socioeconómico y tecnológico han compartido el fenómeno concomitante de una importante internacionalización del delito; la frecuencia de los delitos propiamente transnacionales y otros delitos de carácter puramente internacional, en gran variedad de formas, han aumentado. En las últimas décadas, la delincuencia transnacional se ha intensificado hasta alcanzar niveles difícilmente imaginables, circunstancias propiciadas y facilitadas por los medios modernos de comunicación, viajes a velocidades ultrasónicas con precios accesibles, la transferencia de bienes, servicios y fondos a nivel internacional.

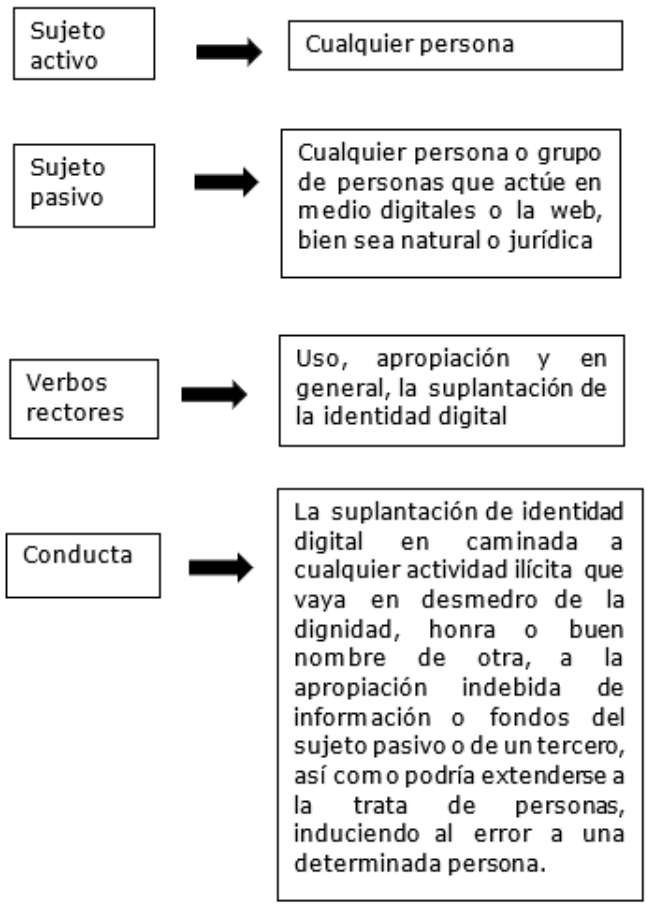


Figura 1. Elementos para configurar el delito de suplantación de identidad digital.

En cuanto los elementos probatorios, consideran que debería hacerse uso de la auditoría forense, sin embargo, esta solo identifica el dispositivo usado para cometer el delito, pero no a la persona quien lo comete, por lo que sería necesario la asignación por parte del Estado de una identificación digital a cada ciudadano, para el acceso a cualquier dispositivo electrónico que lo individualice y lo responsabilice de sus acciones. Estas acciones serian con el objetivo de proteger el derecho a la identidad.

Los expertos opinan que la suplantación de identidad digital es un delito transnacional debe regularse de manera global, así se evita que los delincuentes puedan evadir la responsabilidad en un estado donde el delito no esté tipificado. Además, que los sujetos envueltos en el delito, puede residir en Estados distintos, siendo necesaria la regulación global, como los delitos de narcotráfico, trata de personas o ambientales.

De la revisión documental, se obtuvo estadísticas del Banco Interamericano de Desarrollo, (Chomczyk, 2020), sobre regulación de blockchain e identidad digital en América Latina, específicamente, en Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela. No encontrándose en los países objeto de la investigación, regulación normativa eficiente sobre "identidad, posesión de datos, mecanismo de acreditación, validez legal de la documentación digital, redes ***blockchain***, firmas digitales, contratos inteligentes y criptoactivos, entre otros" (Chomczyk, 2020).

En el caso de la Unión Europea, es amplia la regulación comunitaria que limita el uso de la información personal obtenida por parte de las empresas, tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, leyes de spam, cookies, solicitud de autorización de usuario para la sustracción de datos, el derecho al olvido, este último objeto de interpretación por la corte europea de Derechos Humanos.

Ya en la década de 1980, en un entorno muy diferente al actual, la Organización para la Cooperación y el Desarrollo Económico (OCDE) redactó ciertas directrices sobre la protección de la privacidad y los flujos transfronterizos de datos personales… Los principios de privacidad de la OCDE constituyen, hoy por hoy, a nivel internacional, un marco de privacidad comúnmente utilizado, lo que se refleja en las actuales leyes de privacidad y protección de datos o en los principales programas de prácticas y principios de privacidad adicionales (Telefónica, 2013).

Algunos de estos principios son de: limitación a la recopilación, calidad de los datos, especificación de propósito, limitación de uso, medidas de seguridad, apertura y responsabilidad.

En líneas generales, estos principios establecen, por un lado, las condiciones de recogidas de datos justas, legales, con un límite y la necesidad de consentimiento por parte del titular de los datos personales, la persona de quien se recogen. A su vez, determinan la obligatoriedad por parte de los responsables del tratamiento de los datos a especificar el uso de estos en todo momento, prohibiendo un uso diferente al especificado y más concretamente, su divulgación. Además, la persona objeto de interés tendrá derecho a comprobar sus datos y la identidad del controlador, pudiendo en un momento dado pedir su eliminación o modificación (Telefónica, 2013).

## DISCUSIÓN

Los datos obtenidos de las entrevistas y la revisión documental coinciden en la necesidad de tipificar el delito

de suplantación de identidad digital, como mecanismo de protección del Estado al Derecho de Identidad de la persona, el cual concentra la personalidad misma del ser humano. Debido al desarrollo tecnológico que ha permitido la globalización, esta realidad de identidad digital, se convierte en un tema transnacional, es decir, que, si bien involucra al Estado, lo sobre pasa al ámbito internacional, siendo necesaria una regulación de carácter global, como los temas de narcotráfico, trata de personas, problemas ambientales, entre otros. Como afirma (Champo, 2006) el derecho penal estatal que conocemos hasta ahora no es capaz de enfrentar por no estar concebido para una globalización del delito (internacionalización), el cual muestra nuevas formas y modalidades delictivas que afectan directa y simultáneamente a varios Estados, o, mejor dicho, a varias personas de diferentes Estados.

La regulación jurídica de la identidad digital podría partir del soft law, es decir, de la declaración de principio y recomendaciones que progresivamente serian adoptadas por los Estados, hasta finalmente convertirse en hard law, a través de tratados internacionales, este debido al hecho, que no todos los Estados se encuentran en el mismo nivel de desarrollo normativo en este tema, además de encontrarse dentro de sistemas jurídicos diversos.

La regulación de los datos de las personas por parte de las leyes debe ser clara, como afirma (Berduschi, 2019) "deben determinar con suficiente claridad su ámbito de aplicación, las garantías que ponen en lugar en el almacenamiento de datos, duración, uso, destrucción y acceso de terceros, así como las garantías contra arbitrariedad y abusos".

Es necesaria la comprensión de este tipo de conducta para su correcta tipificación y sanción, lo cual puede ser realizado con el apoyo de criminólogos, que analices al sujeto activo y pasivo de este tipo de delito, así como la forma de ejecutar la acción delictiva.

Son múltiples los delitos informáticos, por ello, se debe precisar en los elementos del delito, ya que en la suplantación de identidad digital hay apropiación, uso, más que manipulación o alteración de datos, por otra parte, hay quienes asemejan el término suplantación con el de robo de identidad, sin embargo, el robo supone apropiación de bienes; o es asemejada a la estafa, sin embargo, esta supone manipulación psicológica para producir en la víctima una falsa apreciación de la realidad, en cambio, en la suplantación de identidad digital, no necesariamente se produce un daño económico, puede ser a su honra o buen nombre. Estas asimilaciones de los delitos informáticos a los tipos penales tradicionales, es lo que ha llevado a una referencia impropia.

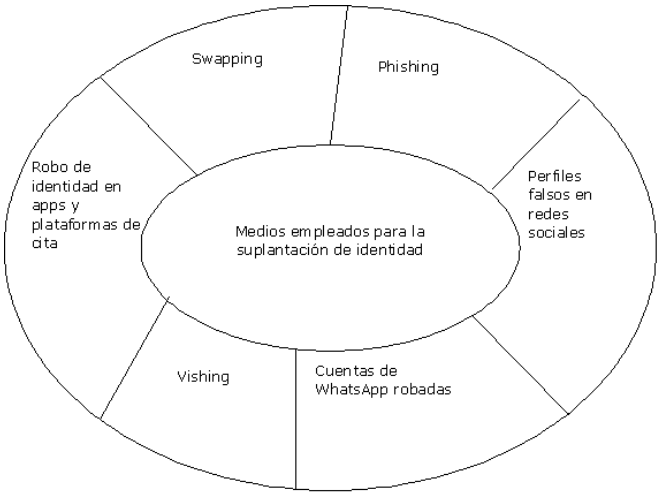


Figura 2. Medios empleados para la suplantación de identidad

El phishing obtiene los datos de la persona mediante un correo aparentemente confiable que solicita el ingreso a un link, en el cual se produce la sustracción de información, que posteriormente es usada para suplantar la identidad. Mientras que, los perfiles falsos en redes sociales inducen al error a la persona que cree estar comunicándose con una persona conocida y le suministra datos personales.

Las cuentas de WhatsApp robadas son usadas por los delincuentes para enviar mensajes a los contactos de la víctima y obtener información de ellos. De igual manera, puede ocurrir con las apps de citas.

El vishing es la obtención de información por medio de llamadas telefónicas, haciendo creer a la víctima que se trata de la entidad bancaria o de una institución conocida. Por su parte, el swapping o tarjetas de sim clonadas, ocurre cuando se burlan los controles de seguridad de las empresas telefónicas y se obtiene un duplicado de la tarjeta sim de un individuo, accediendo de esta forma a los datos personales almacenados.

Los aspectos que podría considerar la regulación de la identidad digital están:

- Elementos del delito de suplantación de identidad digital.
- La jurisdicción para juzgar los delitos de suplantación de identidad, dado que los sujetos pueden pertenecer a Estados diferentes.
- Facultades o poderes del Estado en el manejo de los datos privados de las personas en la red para la persecución de delitos de cualquier índole.

- Uso de los datos por las empresas.
- Consentimiento consciente, informado y expreso por parte de los usuarios antes de obtener sus datos.
- Alcance del Derecho al olvido.
- La identidad digital de los menores de edad y personas con discapacidad, tanto su uso como protección.

Todos estos elementos deben recogerse en la configuración de este delito de carácter transnacional, compartiéndose las características esgrimidas por (Saénz, 2020) sobre delitos transnacionales, a saber:

1. El bien o interés jurídico afectado a través de estos delitos afecta los derechos humanos de la comunidad internacional y, por ende, la relación sociopolítica entre los países que la integran.

2. El sujeto activo está conformado por organizaciones criminales de carácter internacional o, en su defecto, por sujetos que pertenecen a este tipo de organizaciones.

3. La acción ilícita realizada por el victimario guarda relación con la organización criminal a la cual pertenece.

4. Existe una estructura organizativa en la que se jerarquizan las actividades en atención al grupo de poder al cual pertenece dentro de la organización (p. 145).

Igualmente, es necesario desarrollar un registro de identidad digital, que permita a los usuarios actuar con responsabilidad y seguridad dentro de la red, tanto en sus relaciones privadas como públicas, es decir, al momento de negociar, participar en redes sociales, enviar información, así como ciudadano a través del voto electrónico, requerimientos a la administración pública, entre otros. Esto, necesitaría de un consenso de los Estados que procure establecer las pautas y requerimiento para tal registro, de manera que se logre precautelar el derecho a la identidad de todas las personas, ahora en un ámbito digital.

Sobre la identidad global, ejemplifican el caso de Estonia, quien desarrolló la residencia electrónica, se trata de un sistema de identidad transnacional que permite a los individuos no residentes del país participar en la sociedad como ciudadanos digitales, en consecuencia, poder hacer uso de los servicios electrónicos de Estonia y así subsanar las brechas generadas por el poco desarrollo de gobierno electrónico de sus Estados de origen. Otro ejemplo es Suiza con el Swiss id, como identidad digital única para sus ciudadanos para la realización de operaciones en internet.

Además, del castigo por la suplantación de identidad, es necesaria la prevención de este tipo de conductas, que a medida que se desarrolla la tecnología, se incrementan las formas de fraude. De acuerdo a (Vanitha & Akila, 2020) la tecnología biométrica es una solución para la seguridad en la nube, y así evitar suplantación de identidad, a través de un sistema de autenticación biométrico apropiado, ya que involucra La biometría utiliza múltiples atributos que involucran tanto a los físicos como rasgos de comportamiento humanos para su identificación. El reconocimiento facial, de huellas dactilares, escaneo de iris y retina, vena de la palma, geometría de la mano y reconocimiento de voz pertenece a las características fisiológicas y la firma, las pulsaciones de teclas son características conductuales. Hay quienes sugieren la combinación de tecnología biométrica y criptografía. La tabla 1. Presenta algunos mecanismos de prevención de la suplantación de identidad.

Tabla 1. Mecanismos de prevención de la suplantación de identidad

| Mecanismo de protección | Característica |
|---|---|
| Contraseñas seguras | Evitar el uso de información personal, combinar letras mayúsculas y minúsculas, así como números |
| Ignorar correos electrónicos de phishing | No abrir correos electrónicos no confiables y evitar hacer clic en los enlaces y descarga de archivos adjuntos sin investigar adecuadamente el correo |
| Privacidad en las redes sociales | Mantener los perfiles privados, aceptando solo a personas conocidas |
| Limitar el uso de wifi público | Los wifis públicos hacen más vulnerable la apropiación de datos personales por parte de delincuentes |
| Navegación segura en internet | Hay muchos programas maliciosos ejecutados durante la navegación por Internet para recopilar información. Siempre se debe acceder y explorar sitios web seguros y confiables con marca verde segura https que encripta los datos entre el navegador del cliente y los sitios web |

| | |
|---|---|
| Banca segura | Verificar regularmente la cuenta bancaria y la tarjeta de crédito. Usar teclado virtual proporcionado por los bancos para iniciar sesión en la banca en línea en lugar de usar el teclado del dispositivo |
| Actualizaciones del sistema y seguridad | Las vulnerabilidades pueden ser de sistema operativo, aplicación o malware, para proteger de estas vulnerabilidades se requiere actualizar regularmente el sistema operativo, la aplicación y software antivirus con las últimas actualizaciones |
| Uso seguro de dispositivos móviles | Usar PIN o contraseña segura para dispositivos móviles, conectar y configurar los dispositivos móviles a los sistemas de seguridad proporcionada por el proveedor que proporciona muchas características de seguridad para asegurar los dispositivos, como la instalación de borrado remoto, la ubicación del dispositivo. Detección y alertas de seguridad en dispositivo perdido. |

## CONCLUSIONES

La suplantación de identidad es una conducta contraria a al respeto de la dignidad y derecho de la persona al libre desarrollo de su personalidad. El Estado debe velar por la protección y garantizar el ejercicio del derecho a la identidad, que, en los últimos tiempos, gracias al desarrollo de las tecnologías, abarca la identidad digital.

Europa presenta un desarrollo en la regulación de la identidad digital, mientras que América Latina, tiene poca regulación del tema. Esta diversidad de tratamiento jurídico ayuda que los actores de este tipo de conducta busquen los Estados más laxos en la materia. Lo anterior hace necesaria una regulación global, ya que se trata de una actividad transnacional que va más allá del Estado, por cuál, se debe encuadrar la suplantación de identidad dentro de la teoría del delito, considerando a los sujetos pasivo y activo, la acción que se desarrolla y las posibles sanciones, que tiendan a castigar este tipo de actividad, así como su prevención, para precautelar el bien jurídico de la honra, buen nombre y derechos económicos de las personas. Igualmente, se evidencia la necesidad de configurar un registro global de identidad digital, que permita el acceso al mundo digital de manera individualizada y con responsabilidad.

## REFERENCIAS BIBLIOGRÁFICAS


Area, M. (2011). Tic, identidad digital y educación. Cuatro reflexiones. Reencuentro. Análisis de Problemas Universitarios, (62), 97-99. https://www.redalyc.org/pdf/340/34021066012.pdf

Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2), 1-6.

Champo, N. (2006). El derecho penal frente a la globalización. Boletín mexicano de derecho comparado, 39(116), 405-428.

Chomczyk, A. (2020) Regulación de blockchain e identidad digital en América Latina/el futuro de la identidad digital. Banco Interamericano de Desarrollo https://publications.iadb.org/es/regulacion-de-blockchain-e-identidad-digital-en-america-latina

Masiero, S., & Arvidsson, V. (2021). Degenerative outcomes of digital identity platforms for development. Information Systems Journal, 31(6), 903-928. https://onlinelibrary.wiley.com/doi/epdf/10.1111/isj.12351

Mir, U. B., Kar, A. K., Dwivedi, Y. K., Gupta, M. P., & Sharma, R. S. (2020). Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. Government Information Quarterly, 37(2), 101442. https://www.sciencedirect.com/science/article/abs/pii/S0740624X19303557

Naciones Unidas. (2016). Objetivos y metas del desarrollo sostenible. Naciones Unidas. https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/

Núñez, J. (2016). Derecho de identidad digital en internet. (Tesis de doctorado de la Universidad Nacional Mayor de San Marcos). http://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/6252/N%c3%banez_pj.pdf?sequence=2&isAllowed=y

Sáenz, J. E. (2020). Enfoque jurídico penal de los delitos transnacionales según la legislación penal panameña. Revista Metropolitana de Ciencias Aplicadas, 3(3), 141-148.

Sullivan, C. (2018). Digital identity–From emergent legal concept to new reality. Computer Law & Security Review, 34(4), 723-731. https://www.sciencedirect.com/science/article/abs/pii/S0267364918302024

Telefónica, F. (2013). Identidad Digital: El nuevo usuario en el mundo digital. Barcelona: Editorial Ariel. https://revistas.unae.edu.ec/index.php/runae/article/view/148

Vanitha, V. & Akila, D. (2020) Carmel, V. V., & Akila, D. (2020). A survey on biometric authentication systems in cloud to combat identity theft. J Crit Rev, 7(3), 540-547. https://www.researchgate.net/profile/Akila-D/publication/339974479_Journal_of_Critical_Reviews_A_SURVEY_ON_BIOMETRIC_AUTHENTICATION_SYSTEMS_IN_CLOUD_TO_COMBAT_IDENTITY_THEFT/links/5e70a0e0299bf15867b755a7/Journal-of-Critical-Reviews-A-SURVEY-ON-BIOMETRIC-AUTHENTICATION-SYSTEMS-IN-CLOUD-TO-COMBAT-IDENTITY-THEFT.pdf