DOI: https://doi.org/10.56712/latam.v4i2.862

Sim swapping como variante del delito de la violación a la intimidad e integrante de otras infracciones penales

Sim Swapping as a variant of the crime of privacy violation and a part of other criminal offenses

María Rosa Nugra Morocho
nugramariarosa@gmail.com
https://orcid.org/0009-0002-3155-7744
Universidad Católica de Cuenca
Cuenca – Ecuador

Sofía Alejandra Maldonado Archila
Sofiarchmald@gmail.com
https://orcid.org/0009-0009-8016-9714
Universidad Católica de Cuenca
Cuenca – Ecuador

Jaime Alberto Pacheco Solano
jaimepachecos@hotmail.com
https://orcid.org/0009-0004-5080-8582
Universidad Católica de Cuenca
Cuenca – Ecuador

Marcel Eugenio Villavicencio Quinde
markvillavi@hotmail.com
https://orcid.org/0009-0006-7751-7712
Universidad Católica de Cuenca
Cuenca – Ecuador

Artículo recibido: 04 de julio de 2023. Aceptado para publicación: 21 de julio de 2023.
Conflicto de intereses: Ninguno que declarar

Resumen

El SIM Swapping es un delito informático que radica en la suplantación de la tarjeta SIM, lo cual permite acceder a la información que las víctimas contienen en sus teléfonos móviles, donde contienen datos referentes a bancas virtuales, cuentas de redes sociales, fotografías, etcétera. El objetivo de esta investigación es el de identificar al SIM Swapping como variante del delito de la violación a la intimidad, y además, como integrante de otras infracciones penales que se encuentra tipificadas en el Código Orgánico Integral Penal del Ecuador. Principalmente, hemos de enfocarnos en responder a la siguiente interrogante: ¿dicha falta de tipificación del SIM Swapping dentro del COIP, vulnera la seguridad jurídica de los ciudadanos? Para ello, se ha realizado una investigación cualitativa de alcance analítico y descriptivo, recabando el sustento teórico en la respectiva revisión de referencias bibliográficas y doctrina relacionada al presente tema. Además, se ha realizado un exhaustivo análisis con respecto al concurso de infracciones que derivan de este delito informático, con el objetivo de dar a conocer la magnitud y el alcance del mismo, dando a exponer el riesgo al que nos encontramos, esperando que se le brinde la debida atención desde una perspectiva legal, puesto que los delitos informáticos, a pesar de ser concurrentes en la actualidad, aún han sido expuestos lo suficiente, informando a los ciudadanos como prevenir ser víctimas de estos actos y los medios legales por los que pueden optar para su protección.

Palabras clave: sim swapping, delitos informáticos, seguridad jurídica, concurso de infracciones

Abstract

SIM Swapping is a computer crime that lies in the impersonation of the SIM card, allows gaccess to the information contained in the victim's telephone, such as virtual banking, social networking, and photographs. The objective of this investigation is to identify SIM Swapping as a variant of the crime of violation of privacy and a member of other criminal offenses that are typified in the Comprehensive Organic Criminal Code of Ecuador. Mainly, we must focus on answering the following question: does the lack of typification of SIM Swapping within the COIP violate the legal security of citizens? For this, qualitative research of analytical and descriptive scope has been carried out while gathering the theoretical support in the respective review of bibliographic references and doctrine related to this topic. In addition, an exhaustive analysis has been performed out regarding the infringement contest that derives from this computer crime. Our aim is to publicize the magnitude and expose the risk that we find ourselves in while hoping that it will give due attention from a legal perspective. We hope to sufficiently expose these computer crimes and inform citizens how to prevent being victims of these acts and their legal means of protection.

Keywords: sim swapping, computer crimes, legal certainty, infringement competition

Como citar: Nugra Morocho, M. R., Maldonado Archila, S. A., Pacheco Solano, J. A., & Villavicencio Quinde, M. E. (2023). Sim Swapping como variante del delito de la violación a la intimidad e integrante de otras infracciones penales. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades 4(2), 3655–3670. https://doi.org/10.56712/latam.v4i2.862*

INTRODUCCIÓN

El SIM SWAPPING, como fuente de varios delitos informáticos, según la "Guía para prevenir el robo de identidad", elaborada por el Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales, manifiesta que: "Es la apropiación de la identidad de una persona, para hacerse pasar por ella, asumir su identidad frente a terceros públicos o privados, a fin de obtener ciertos recursos o beneficios a su nombre". [1]

Este delito es también conocido como SIM Splitting o SIM jacking, es un fraude de telecomunicaciones entendido como una forma de ingeniería social. (Jendruszak, 2022). Consiste en duplicar la tarjeta SIM o chip, con el fin de suplantar la identidad de las víctimas, y a través de esto lograr un acceso a todo tipo de información, sin embargo, comúnmente es utilizado para el acceso a cuentas bancarias que se encuentran ligadas al número telefónico, lo que conlleva a un fraude financiero, razón por la cual los bancos tienen el mayor interés en explicar este delito y maneras de prevención. (Hacienda: Secretaría de Hacienda y Crédito Público, 2023)

El análisis que proponemos en esta investigación es identificar el concurso ideal de infracciones que se derivan del SIM SWAPPING, enfocándonos principalmente en la violación a la intimidad, delito que se encuentra tipificado en el Artículo 178 del Código Orgánico Integral Penal. Si bien se menciona la información contenida en soportes informáticos[2] como medio para cometer el delito, aquello no desglosa cuáles son las conductas que se derivan del mismo. Entre ellas tenemos: acceso a cuentas bancarias, fraude bancario, de identidad o telefónico, acceso a las redes, robo de datos, acceso no autorizado a sistemas informáticos, violación a la privacidad, estafa, acoso y extorsión, ocasionando no solamente un daño patrimonial, sino también moral.

Estos delitos informáticos ya forman parte de una problemática delincuencial en nuestro país que aún no goza del interés legal adecuado y necesario convirtiéndose en un delito atípico, atentando contra la seguridad jurídica mencionada en el Art. 82 de la Constitución de la República, la cual manifiesta que: "El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes.". [3]

Con el desarrollo de esta investigación, tenemos como objetivo dirigir la atención a esta nueva modalidad de crimen y como la ausencia de esta figura dentro de la legislación ecuatoriana puede incidir en consecuencias negativas para la seguridad jurídica y violación de la intimidad de los ciudadanos. Para ello hemos realizado una investigación de carácter cualitativo, aplicando la metodología analítica, informativa y descriptiva.

METODOLOGÍA

La metodología que hemos utilizado para el desarrollo del presente artículo es la cualitativa, la cual es también conocida como interpretativa, fenomenológica o etnográfica. Para la realización del mismo, deben seguirse ciertas fases, siendo la del planteamiento del problema, revisión de la literatura, recolección de datos, análisis de datos y finalmente, el reporte de resultados. Sin embargo, esto también puede observarse desde la agrupación de cuatro fases: preparatoria, trabajo de campo, fase analítica y fase informativa (Piza Burgos, Amaiquema Márquez, & Beltrán Baquerizo, 2019). Fases que hemos cumplido a cabalidad para el desarrollo de esta investigación.

---

[1] 1 (Instituto Federal de Telecomunicaciones)

[2] (Código Orgánico Integral Penal)

[3] (Constitución de la República del Ecuador, 2008)

Como investigadoras nuestro papel dentro de esta investigación fue la de recopilar mediante fuentes bibliográficas, toda aquella información que fuera pertinente con respecto a la problemática de nuestro interés, tomando en cuenta doctrina, jurisprudencia e inclusive legislaciones de otros países con el fin de comparar y poder formar un criterio analítico sobre el tema. Esto con el objetivo también de poder sintetizar de una forma clara y precisa toda esta información, para que la lectura y la comprensión de este artículo sea sencillo y ameno para el lector.

Por tanto, la información que hemos utilizado goza de credibilidad, validez y fiabilidad, y gracias al análisis desarrollado en base a la misma, podemos dar a conocer más acerca de este delito informático el SIM Swapping, y cuáles son sus apariciones dentro de la esfera jurídica del derecho penal ecuatoriano.

RESULTADOS Y DISCUSIÓN

A partir de la respectiva investigación realizada sobre el SIM Swapping, y ante la inquietud por nuestra parte con respecto a la duda de cómo se encuentra regulado este delito dentro de nuestra normativa jurídica, hemos partido de ciertos puntos para el análisis del mismo. Inicialmente, debemos conocer cuáles son las generalidades de este delito y cuáles son sus fases de ejecución, puesto que esto nos ayudará en gran medida a la comprensión de su alcance y peligrosidad.

En virtud del interés de esta investigación, hemos desarrollado un análisis del SIM Swapping desde la perspectiva penal del ordenamiento jurídico ecuatoriano, de los bienes jurídicos afectados, legislación comparada de Estados Unidos, Chile y Colombia; los fundamentos jurídicos para su tipificación, el concurso de infracciones que surgen a partir del mismo, el SIM Swapping como integrante de otras infracciones penales en el Código Orgánico Integral Penal y finalmente el análisis a partir de la siguiente interrogante: ¿la falta de tipificación del SIM Swapping vulnera la seguridad jurídica de los ciudadanos?

Generalidades del SIM Swapping

Para que este delito sea llevado a cabo se requieren de varias etapas. Inicialmente identifican a la víctima, a quienes previamente ya han investigado y recaudado la información necesaria. Posteriormente, interceden en la compañía telefónica de la víctima para así, mediante el convencimiento, solicitar a un representante la transferencia del número telefónico a una nueva tarjeta SIM, excusándose por supuesto daño o pérdida. Una vez que la solicitud es aceptada, restablece las contraseñas de sus cuentas de interés para poder acceder libremente a estas. Es especialmente peligroso, ya que pueden recibir códigos que permitan iniciar sesión en tus redes sociales, bancos o incluso cuentas de comercio electrónico. (Jendruszak, 2022)

Debemos hacer énfasis en que la tarjeta SIM es un componente de gran valor y sumamente delicado de nuestros teléfonos móviles, ya que es a través de este que podemos acceder a la red y navegar en ella, realizar llamadas, enviar o recibir mensajes; pero lo más importante, es que esto vendría a ser nuestro medio de identificación para recibir mensajes de texto que se encuentran destinados únicamente a nosotros por la razón de estar vinculadas a nuestras cuentas personales. (Fernández, 2022)

No está de más explicar que la tarjeta SIM es un “módulo de identidad del suscriptor”, siendo esta pequeña tarjeta extraíble que cuenta con un chip único y que se encuentra asociada a nuestra cuenta móvil. Al extraerla de nuestro teléfono y colocarla en uno nuevo, tanto nuestro número como nuestros datos se traspasan al nuevo teléfono. Lo mismo sucede en el caso de duplicarlas. (Ministerio del Interior y Seguridad Pública, 2021)

La manera en la cual se lleva a cabo el SIM Swapping realmente es a través de una operación sencilla, ya que en varias de las ocasiones bastan con una simple llamada para que esta se materialice. Lo único con lo que deben contar con anterioridad es con la información personal del usuario para poder identificarse ante el telefónico operador. Una vez cuentan con acceso a la cuenta telefónica, inician el fraude. (Cyber Intelligence Team, 2022)

Fases de ejecución del SIM SWAPPING

La primera fase es la de extracción de datos personales. Se basa en recopilar toda la información esencial de la víctima, ya que esta será la utilizada para hacerse pasar por ella ante la compañía telefónica. Deben contar con información básica sobre sus nombres completos, número de su documento de identificación personal y fecha de nacimiento, ya que esta suele ser la información con la que cuentan las empresas telefónicas y con las que se podría "asegurar" la identidad.

Esta información la podemos recopilar de dos maneras: Robo selectivo de SIM (centran su interés en cuentas de redes sociales de gran alcance) o fuerza bruta (prueban con varios números hasta que les toca uno que les sea conveniente) (Jendruszak, 2022). Una vez que hayan elegido a la víctima, pueden obtener los datos a través de métodos como filtraciones de datos, redes sociales, aplicaciones maliciosas, compras realizadas en internet, correos electrónicos, vía WhatsApp, a través de enlaces falsos, o solicitando directamente esta información, normalmente haciéndose pasar por otras empresas (Ministerio del Interior y Seguridad Pública, 2021) (Intercambio de SIM O SIM Swapping: una estafa de teléfono móvil, 2021).

Sin importar cuál de las dos modalidades elijan, se realizan pasos similares. Por ejemplo, deben investigar la información básica del titular, se hacen pasar por la víctima ante la empresa telefónica, solicitan que el número antiguo sea transferido a una nueva SIM, para finalmente recibir mensajes que permitan entrar a las cuentas personales y sustraer todo tipo de información personal de la víctima. (Jendruszak, 2022)

La segunda fase es la de uso de información. Puede adoptar distintas formas, lo cual dependerá de los fines que busque la víctima, atendiendo a si busca obtener un beneficio económico o únicamente perjudicar a la víctima moralmente; o bien pueden ser ambas alternativas en conjunto. Entre esas formas tenemos: suplantación o fraude de identidad, fraude bancario, violación a la intimidad, acoso, estafa, extorsión e instigación al suicidio (Albors, 2020). Sin embargo, hondaremos más acerca de este concurso de infracciones más adelante, analizado desde una perspectiva del ordenamiento jurídico del Ecuador.

Bienes jurídicos afectados por el SIM Swapping

Un bien jurídico es un objeto de protección o tutela dentro de un marco legal, promoviendo que se proteja su integridad y correcto desarrollo. El principal interés del Estado es proteger dichos bienes ya que es la ley quien debe otorgar una correcta protección mediante normas que prohíban con amenazar las acciones que menoscaben estos intereses vitales dentro de una comunidad para el correcto desenvolvimiento de los individuos dentro de la misma. (Kierszenbaum, 2009)

Como bien hemos analizado, son varios los delitos que surgen del SIM Swapping, y por ende, son afectados varios bienes jurídicos, y entre ellos están: la privacidad, la identidad, la propiedad, el derecho al honor, la intimidad personal y familiar y a la propia imagen, el patrimonio y la integridad personal; lo cual abarca tanto la física, como la psíquica, moral y sexual.

Por ejemplo, la Corte Constitucional en el Caso No. 456-20-JP, analizó el caso de una estudiante que reenvío fotografías íntimas de una compañera de colegio, incurriendo en la práctica del

sexting[4]. Dicha actividad se ha relacionado fuertemente con problemas psicológicos y conllevando consecuencias negativas para las víctimas, afectando principalmente a las mujeres. Entre estas afectaciones podrían darse el acoso, la extorsión, intentos de suicidio, ciberacoso, etcétera.[5]

Podemos identificar entonces que en un solo acto pueden verse vulnerados varios bienes jurídicos. Como lo es en el presente caso, se vio afectado el derecho al honor, a la intimidad personal y a su integridad, afectando en consecuencia moral, sexual y psicológicamente a la víctima, lo cual es aún más grave si tomamos en cuenta que se trata de una adolescente que se vio atacada dentro de su centro educativo.

Análisis del SIM Swapping desde la perspectiva penal del ordenamiento jurídico ecuatoriano

Es necesario para esta investigación que partamos del análisis del Artículo 178 del Código Orgánico Integral Penal, el cual nos habla de la violación a la intimidad. Para ello, hemos de citar el presente artículo:

La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años (…)[6]

Hemos de hacer énfasis en la mención de la información contenida en soportes informáticos. Para ello debemos aclarar, ¿qué son los soportes informáticos? Son todos aquellos dispositivos mediante los cuales podremos almacenar información en un formato electrónico, y que, por lo tanto, estos son de fácil transportación. Entre ellos tenemos los discos duros, unidades USB, tarjetas SIM, ordenadores portátiles, smartphones, etcétera. (Universidad de Cádiz, 2018)

Si bien podemos considerar que se hace una referencia sobreentendida al SIM Swapping, es necesario que este sea mencionado de manera independiente debido a que este delito informático desglosa otra serie de delitos, siendo en este punto donde surge un concurso de infracciones. Además, esta clase de delitos cada vez suelen ser más comunes y es necesario un enfoque legal hacia estos, para que en consecuencia los ciudadanos tengan un mayor conocimiento y puedan ya sea prevenirlos, o acudir ante la ley cuando sean víctimas de ellos.

Es mencionado de igual forma las acciones de acceder, interceptar, difundir o publicar esta información personal, no obstante, no se menciona con qué objetivo es realizado, el cual como podremos identificar en el transcurso de esta investigación, pueden ser de distinta índole, Por ejemplo, puede darse el objetivo de extorsionar con el fin de obtener un beneficio económico por parte de la víctima; o bien puede ser meramente un interés en acosar y violentar psicológicamente a la víctima ocasionando un daño meramente moral.

Por estas razones es necesario que se identifique individualmente al SIM Swapping, para que así podamos conocer el alcance y la magnitud de este delito, que va mucho más allá del de la violación a la intimidad de una persona.

[4] El *sexting* es el acto de enviar contenido sexual a través de dispositivos tecnológicos, en el cual pueden verse implicados niños, adolescentes o adultos, suponiendo entonces un riesgo para los implicados de que este contenido sea exhibido y viralizado sin su consentimiento. (Sierra, 2018)

[5] (La justicia restaurativa y el derecho al debido proceso en contextos educativos. , 2021)

[6] (Código Orgánico Integral Penal)

Fundamentos jurídicos para la tipificación del SIM SWAPPING

En primer lugar, es importante hablar acerca del principio de legalidad, siendo este un principio fundamental que será aplicado cuando no exista el debido apego a la legalidad por parte del Estado, el cual es también conocido como el principio de juridicidad. Es decir, se aplicará en los casos donde los actos realizados por los poderes públicos se encuentren en contraste con la ley, actos no autorizados legalmente o los no regulados completamente por la ley, acarreando invalidez. (Islas Montes, 2009)

Dicho principio se encuentra regulado en el debido proceso dentro del Artículo 76 numeral 3 de la Constitución de la República, indicando lo siguiente:

Nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal, administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la ley. Solo se podrá juzgar a una persona ante un juez o autoridad competente y con observancia del trámite propio de cada procedimiento.[7]

Es pertinente realizar un análisis del delito SIM Swapping en relación al principio de legalidad, puesto que al existir este vacío dentro del ordenamiento jurídico penal, da lugar a la vulneración de la seguridad jurídica de los ciudadanos al no brindar una protección legal a las víctimas de estos crímenes, que no cuenten con una norma que explique claramente cuáles son las circunstancias de este delito y del alcance de este al no considerarse un delito no pudiendo entonces ser procesado ni sancionado la persona que lo comete. Para la protección del principio de legalidad se aplica la prohibición de la analogía y la interpretación extensiva.

Con respecto a la prohibición de la analogía e interpretación extensiva, esto se encuentra tipificado en el Artículo 13 numeral 3 del Código Orgánico Integral Penal, donde se manifiesta lo siguiente: "Queda prohibida la utilización de la analogía para crear infracciones penales, ampliar los límites de los presupuestos legales que permiten la aplicación de una sanción o medida cautelar o para establecer excepciones o restricciones de derechos."[8]

Por otra parte, la interpretación extensiva es aquello que conlleva una intelección amplia de la norma, extendiendo el alcance a la máxima cantidad de supuestos posibles, dando lugar a varias interpretaciones legales, pero dentro del sentido de la norma. No obstante, si este es excedido, llega a incurrir en la analogía. Aclaramos que la analogía no debe ser considerada una modalidad de interpretación puesto que se da cuando el intérprete se ha alejado totalmente de la norma analizada, recayendo entonces en una ausencia de norma. (Cevallos López, Pupo Kairuz, Calderón Ramíez, & Ponce Ruiz, 2020)

En este punto podemos concluir que las autoridades no podrán sancionar en base a una interpretación amplia de la ley para tratar conductas que no se encuentren previa y expresamente tipificadas en la ley. Si bien se deduce que ciertas actitudes no son moralmente aceptables y ocasionan un perjuicio a la sociedad, no podrán ser objeto de persecución penal, ocasionando así una limitación para el sistema de justicia penal al momento de procesar y sancionar conductas particularmente perjudiciales para la sociedad.

[7] (Constitución de la República del Ecuador, 2008)
[8] (Código Orgánico Integral Penal)

Tipificación del SIM Swapping y su tratamiento en otras legislaciones

Estados Unidos

La figura del SIM Swapping, no se encuentra tipificado de manera específica en la mayoría de las legislaciones de algunos países, pero esto no quiere decir que dicho delito no sea considerado como tal. Revisada la legislación de países de primer mundo, se ha seleccionado la legislación estadounidense, por ser uno de los países pioneros y más completos en la materia de delitos informáticos. Las actividades que tienen que ver con el delito del SIM Swapping, han sido cubiertas por leyes que tienen que ver con delitos como: estafa, fraude, robo de identidad, acceso a sistemas informáticos sin autorización, entre otros delitos que van por la misma vía.

En Estados Unidos, la figura del SIM Swapping, según lo indica la Comisión de Comercio de los Estados Unidos (FTC) "ha aumentado drásticamente en los últimos años". En este país, en California, Santa Clara, un estudiante universitario fue uno de los primeros sentenciados por este delito. Joel Ortiz fue sentenciado a diez años en prisión por el delito de SIM Swapping. Esta nueva modalidad de fraude fue utilizada por este estudiante para lograr el robo de alrededor de $7.5 millones de dólares a más de 40 víctimas. (Leal, 2019)

Esta nueva modalidad delictiva castiga a las personas que cometen este tipo de delito en base a delitos que tienen que ver con el fraude, estafa, robo de identidad, acceso no autorizado a dispositivos o servicios informáticos. La tarjeta de SIM o chip incluye información valiosa, por aquello el robar o duplicarla resulta muy lucrativo para cualquiera (El Heraldo de México, 2021). Algunas de las leyes federales y estatales que son importantes para sancionar este delito en Estados Unidos, son:

- La Ley de Fraude y Abuso Informático: es una de las normas más importantes de ciberseguridad dentro de Estados Unidos. Esta norma tipificó siete conductas con relación al acceso no autorizado a computadoras que puedan causar una vulneración a las normas contenidas dentro de esta ley, se dan por niveles, y pueden ir desde una sanción monetaria hasta pena de prisión de máximo cinco años. De manera que la CFFA, busca garantizar la protección de los ciudadanos estadounidenses frente a los ciberdelitos. (Case Guard, 2022)
- La Ley de Usurpación de Identidad: Esta ley sanciona la utilización de la identificación de una persona de manera ilegal, la sanción por este delito puede llegar a ser de hasta quince años. (Glaesser & Alonso, 2014)
- Ley de Fraude y Dispositivos de Acceso: Esta ley sanciona el uso de dispositivos de acceso, como por ejemplo tarjetas, contraseñas y la tarjeta de SIM, puesto que estas son utilizadas para obtener beneficios financieros sin autorización del titular. El SIM Swapping podría ser considerado como un delito bajo esta ley, puesto que implica el uso fraudulento de dispositivos de acceso. (Glaesser & Alonso, 2014)

Chile

En Chile existe el Departamento de Gestión de Reclamo (DGR), el cual pertenece a la Subsecretaría de Telecomunicación de Chile (SUBTEL). En el Departamento de Gestión de Reclamo se han recibido varias denuncias de los usuarios de teléfonos móviles, que han sufrido de la suplantación de su tarjeta SIM o SIM Swapping. Esta nueva modalidad de robo pone en alerta a los usuarios chilenos, quienes están realmente alarmados por esta situación. (TrendTIC, 2020)

La SUBTEL, ha recomendado a las empresas que prestan servicios de telefonía móvil que se fortalezcan los protocolos para evitar este tipo de estafas en el país. Ya que, el primer paso para combatir ese delito es verificar que la persona que esté solicitando la reposición del SIM, sea la

misma que contrató el servicio de telefonía móvil al inicio. Aunque en Chile no exista una legislación determinada para este tipo de delito, existen leyes que son posibles que sean relacionadas con el Sim Swapping. (TrendTIC, 2020)

La Ley número 21.259 fue promulgada por el Congreso Nacional Chileno el 20 de junio de 2022, y que reemplaza a la Ley 19.223, sobre figuras penales relativas a la informativa. Esta nueva ley establece la normativa acerca de los delitos penales en Chile, uno de los antecedentes para la creación de esta nueva ley es la normativa del Convenio de Budapest. La finalidad de la creación de esta nueva ley es brindar seguridad a los usuarios en cuestiones de ataques, accesos ilícitos, interceptaciones ilícitas a los sistemas informáticos. Las penas pueden variar, dependerá de los agravantes, y sus consecuencias, pero van desde los seis meses hasta los cinco años. (Bascur & Peña, 2022)

Colombia

En Colombia los ciberdelitos son cada vez más comunes, las industrias de telecomunicaciones son las afectadas por estos nuevos delitos, el phishing ocupa uno de los primeros lugares en denuncias sobre delitos de este tipo, seguido por el SIM Swapping y otras modalidades de delitos informáticos.

A través de la resolución 73/187 la de la Asamblea nacional, denominada “Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos”. En esta Asamblea se trató sobre los problemas que se enfrentan con el uso masivo de la tecnología y los fines delictivos, cada país miembro presentó un informe para examinarlo y presentar una resolución final. A su vez, por medio de esta resolución fue creado el Convenio sobre la ciberdelincuencia, también llamado Convenio de Budaquest, fue celebrado en el año 2001 en Hungría, en el cual se determinaron leyes para afrontar la ciberdelincuencia. (Medina Martínez, Cárdenas Osorio, & Mejía Lobo, 2021)

La Ley 1273 de 2009 es específica para delitos informáticos, puesto que la misma establece sanciones para delitos de acceso abusivo a sistemas informáticos, intercepción de datos o utilización de software maliciosos, las penas de prisión pueden ser de cuarenta y ocho a noventa seis meses, además de las multas, todo esto dependerá de la gravedad del ciberdelito y sus consecuencias. (Medina Martínez, Cárdenas Osorio, & Mejía Lobo, 2021)

Por otra parte, tenemos a la Ley 1298 del 2018 que aprueba el “Convenio sobre la ciberdelincuencia” y la Ley 1587 de 2012 que tiene relación con la protección de datos personales. El uso indebido de datos personales, así como su obtención ilegal es una de las características principales de este ataque, por lo mismo su accionar podría estar sujeto a sanciones establecidas en esta norma. (Medina Martínez, Cárdenas Osorio, & Mejía Lobo, 2021)

Concurso de infracciones que surgen a partir del SIM Swapping

El concurso de infracciones se produce cuando una persona comete múltiples delitos al mismo tiempo, o al menos en una secuencia cercana. Prácticamente, trata de la concurrencia de varias infracciones penales que pueden ser encasilladas dentro de un mismo contexto, realizadas por una misma persona a través de ciertas actuaciones ilícitas. En general, existen dos tipos de concurso de infracciones, siendo estas el ideal y el real.

El concurso ideal se da cuando una sola acción viola múltiples normas o ataca varios bienes jurídicos. En estos casos se suele aplicar una sola pena la cual corresponderá al delito más grave, por tanto, los demás delitos se “absorben” por el delito principal. Por otra parte, el concurso real se da cuando una persona comete varios delitos independientes entre sí, pero dentro de un

mismo contexto o período de tiempo, debiendo ser juzgados y sancionados por separado, al contrario del concurso ideal, aquí las penas suelen sumarse o acumularse.

Con respecto al concurso real de infracciones, este es considerado como un tratamiento sancionador que debe dársele por una conexión que ha permitido su acumulación en el mismo proceso punitivo. Varios hechos o acciones, cada uno de los cuales constituye un delito particular e independiente, aunque puedan merecer un solo procedimiento penal. Sin embargo, consideramos que este no aplica a nuestra problemática, ya que nos habla de acciones realizadas de manera independiente y que pueden incurrir en daños distintos en distintas víctimas. (Jiménez Alemán, 2018)

El SIM Swapping si bien son distintas acciones ilícitas, van todas dirigidas a un mismo objetivo. El criterio que se aplicará deberá tomar en cuenta el tiempo y la conexidad material de los ilícitos cometidos, pues no pueden acumularse sin tener una relación entre ellos. El concurso ideal involucra la comisión de dos o más ilícitos, es decir, un solo hecho genera una tipicidad múltiple (Gavilanes Domínguez, 2022). En este contexto, podemos deducir que el Sim Swapping encaja en el concurso ideal, porque a través de un solo delito incurren múltiples infracciones.

Dentro del concurso ideal existen dos supuestos: concurso ideal heterogéneo y homogéneo. El heterogéneo es cuando la conducta abarca varios tipos penales y el homogéneo cuando la conducta significa una concurrencia del mismo tipo penal, infringido múltiples veces y perjudicando a varias víctimas. En conclusión, un solo hecho da lugar a dos o más delitos. Tenemos, además, que para definir si estamos ante una sola acción debemos aplicar el criterio de unidad, el cual se divide de la siguiente forma:

El criterio de la unidad típica de acción: Se refiere a la inclusión de puntos de referencia jurídicos, es el Derecho que establece los elementos. Por otra parte, el criterio de unidad de acción determinada conforme al número de resultados: el número de hechos debe coincidir con el número de resultados materiales. (Jiménez Alemán, 2018)

Por otra parte, cuando los ilícitos pretenden desincentivar la misma conducta, debemos analizar si los hechos pueden subsumirse a un solo tipo penal, ya que en base a este resultado será posible determinar si nos encontramos frente al cometimiento de ilícitos que protegen un mismo bien jurídico. Debemos tener en cuenta también el concurso de leyes o concurso aparente. Este se basa en 4 principios, sin embargo, haremos énfasis solamente en los mencionados a continuación, puesto que son los que más encajan con la problemática tratada en el presente artículo.

En primer lugar, tenemos al principio de subsidiariedad, el cual se aplicará únicamente de manera supletoria cuando el precepto de la acción no se subsume plenamente a la disposición principal. Por otro lado, tenemos al principio de consunción, el cual hace referencia a los casos donde los preceptos engloban otros hechos.

Si bien no es materia de análisis, es importante hacer una breve mención del concurso medial y del principio de continuidad de infracciones. El concurso medial procede cuando uno de los delitos sea medio necesario para cometer otro, para Gómez Tomillo es una forma de concurso real, ya que se trata de un cúmulo de infracciones.

Ahora, con respecto al principio de una continuidad de infracciones, esta es una exposición criminal en virtud de la cual el sujeto activo ejecuta de manera repetida numerosos actos particulares, siendo la característica principal de que estos actos tengan una estrecha relación entre sí, en el sentido de depender unos actos de otros. Por tanto, el supuesto de hecho llegaría a formarse en una unidad final de acción. Con respecto a aquello, es pertinente señalar que el delito continuado si bien se menciona dentro del COIP, no está descrito.

El delito puede ser explicado por teorías que indican la estructura básica del mismo, por ejemplo, la que manifiesta que este debe estar conformado por la tipicidad, antijuricidad y culpabilidad, siendo estos elementos necesarios que conllevan a que estas conductas sean consideradas como una infracción penal dentro del ordenamiento jurídico.

La tipicidad es un elemento importante dentro del análisis de esta investigación, ya que la falta de esto con respecto al SIM Swapping, es la problemática central de nuestro enfoque. Por tanto, es importante analizar qué es la tipicidad. Entendido esto como la adecuación de hechos ilícitos a las descripciones de las mismas dentro de la normativa penal. Por tanto, habrá tipicidad cuando las conductas se adecuen debidamente al tipo penal, encontrando su fundamento en el principio de legalidad y subsunción. (Vallejo Naranjo, 2019)

La ausencia de una adecuada clasificación legal representa un obstáculo evidente para la imposición de sanciones por determinada conducta, ya que un delito sólo existirá si puede ser correctamente enmarcado dentro de los elementos específicos establecidos en el código penal. Por lo tanto, aunque la conducta pueda considerarse como contraria a la ley, culpable y prohibida, no podrá ser objeto de un proceso judicial si no se ajusta a los criterios legales requeridos.

Los componentes esenciales del concurso ideal son dos: la unidad de acción y la existencia de múltiples infracciones en un solo acto. Además, la conexión entre los delitos es un aspecto intrínseco al concurso ideal. (Vallejo Naranjo, 2019)

El SIM Swapping como integrante de otras infracciones penales en el COIP

La complejidad del SIM Swapping radica en que para realizarse radica en la infracción de varios delitos (suplantación de identidad, violación a la intimidad), si no, además, que puede ser llevado a cabo con diferentes objetivos. Por ejemplo, este delito es más conocido dentro de fraudes informáticos, teniendo un interés económico, lo cual también es aplicable en la extorsión y estafa.

Sin embargo, el infractor puede que no tenga ningún interés económico, sino que busca directamente dañar a la víctima en niveles psicológicos y morales, como lo sería en el caso del acoso, llegando inclusive a la instigación al suicidio, incurriendo en consecuencia en violencia psicológica.

Podemos identificar entonces el tremendo alcance del SIM Swapping al ser una serie de conductas que, si bien son independientes, llegan a conectarse y entrelazarse al nexo de causa efecto, razón por la cual explica la importancia de que esta clase de delitos sean reconocidos dentro del ordenamiento jurídico penal, ya que como bien ha sido mencionado con anterioridad, al incurrir en varias infracciones penales, a su vez vulnera varios bienes jurídicos de un mismo individuo.

La falta de tipificación del SIM Swapping vulnera la seguridad jurídica de los ciudadanos

La seguridad jurídica es un tema que se debate diariamente en los tribunales, todas las personas y profesionales del Derecho la enuncian, sin embargo, en delitos informáticos esta problemática suele resultar escasa, y hasta cierto punto puede considerarse ausente, por la complejidad de la misma y la falta de conocimiento al respecto. Nuestra Constitución a partir del 2008, ha dejado consagrado en su Art. 82 que el derecho a la seguridad jurídica encuentra su fundamento principalmente en respetar a lo contenido dentro de la Constitución, además de que las acciones por parte de las autoridades competentes deberán realizarse en base a las normas jurídicas previas, claras y públicas. (Maldonado Padilla, 2016)

Dado que el primer bien jurídico que hay que proteger en un entorno digital confiable es el de la información, es fundamental subrayar que la seguridad jurídica también debe extenderse al

ámbito de los delitos informáticos. El objetivo de las medidas de seguridad de la información es desarrollar herramientas que puedan anticipar y responder a estas novedosas formas de delincuencia para que, de esta forma, no se comprometan derechos como la intimidación, la integridad y los datos personales, entre otros. (Oropeza Mendoza, 2012)

Lo mencionado anteriormente, es un asunto que debe ser tratado desde una perspectiva global, más aún por que nos encontramos en la era de la digitalización, y todos los Estados deben estar preparados para estos nuevos retos de criminalidad. Debido a este carácter internacional, los problemas de este tipo de delitos trascienden las fronteras, lo que plantea un serio desafío a la legislación vigente, y una mayor cooperación con el resto de los países.

Puede tener un impacto negativo en la seguridad jurídica de los ciudadanos, y esto no solamente refiriéndonos al SIM Swapping, sino a cualquier otra actuación delictiva que pueda poner en riesgo la seguridad de los ciudadanos. Recordemos que la tipificación atribuye a que contemos con sanciones específicas para juzgar y sancionar actos delictivos. Por tanto, al no encontrarse este delito informático en la normativa, se crea un vacío legal que podría impedir que las autoridades sancionen al encontrarse frente a estos hechos.

No solamente eso sino también que puede existir una mayor dificultad para prevenir y detectar este tipo de delitos. Tomemos en cuenta que los delitos informáticos aún no son lo suficientemente reconocidos en la sociedad, existe cierta desinformación al respecto lo cual complica que las personas puedan tomar medidas de prevención para su seguridad, teniendo como consecuencia una menor probabilidad de brindar una protección debida a los ciudadanos y que se puedan prevenir dichos ataques.

Recordemos que el enfoque de este artículo es también desde el interés de que se expanda la información de este delito informático, ya que puede haber víctimas que, al encontrarse frente a este delito, no logren comprender siquiera como pudo llevarse a cabo, dejándolos en plena vulnerabilidad. Inclusive profesionales del derecho desconocen de estas conductas, mucho menos contamos con jueces o tribunales especializados en esta materia, ¿entonces cómo la justicia ecuatoriana puede prevenir y proteger a los ciudadanos de estas modalidades delictivas que son cada vez más comunes?

CONCLUSIÓN

Los delitos informáticos son toda aquella actividad que tiene por fin último dañar o poner en peligro, un bien jurídico protegido utilizando medios tecnológicos electrónicos. El SIM Swapping, según lo analizado, reúne todas las características propias del delito, siendo un acto típico, jurídico y culpable, sin embargo, este tipo de delito tiene una característica propia: el uso de elementos informáticos al momento de ocasionar el daño, vulnerando derechos recogidos en nuestra normativa vigente.

Podemos afirmar de manera general que el bien jurídico protegido frente a los ciberdelitos es la propia información que según las diversas formas de delito se ve afectada, sin embargo, las lesiones se extienden a bienes jurídicos tradicionalmente protegidos como el patrimonio, seguridad, intimidad, honor, integridad del individuo tanto física como psicológica.

Cuestiones como el avance tecnológico acelerado, y la falta de conocimiento de estas nuevas modalidades de delitos, hacen que cada vez la delincuencia comprometa el aspecto socioeconómico del país. Estos nuevos delitos, evolucionan diariamente de tal manera que se incorporan nuevas tecnologías para lograr con su objetivo de delinquir como se demuestra en el presente estudio.

En la normativa ecuatoriana al referirnos al delito del SIM SWAPPING, podemos observar que no se encuentra especificado como tal, sin embargo, se la puede encasillar dentro del artículo 178 del COIP, pero esto no es suficiente, puesto que no se desglosa las conductas que derivan del delito mismo. Por aquello mencionamos en esta investigación la necesidad que este delito debería tener su propio apartado, tomando de referente otros países, cuya normativa se encuentra más avanzada en el tema de delitos informáticos, esto en cuanto que la comisión de este delito genera muchos más perjuicios que los que se menciona en la norma.

La no tipificación de este delito podría ocasionar que los ciber delincuentes realicen este delito sin recibir una pena legal adecuada, creando un clima de impunidad e inseguridad entre los ecuatorianos. El legislador deberá considerar que nos encontramos en una era informática, y que si no existe una ley que penalice este delito, este fraude informático incrementará de manera evidente.

REFERENCIAS

Albors, J. (30 de Marzo de 2020). We Live Security. Obtenido de SIM Swappin: qué es y cómo funciona este fraude: https://www.welivesecurity.com/la-es/2020/03/30/que-es-sim-swapping-como-funciona/

Bascur, G., & Peña, R. (2022). Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459. Primera parte. Revista de Estudios de la Justicia, 1-38. doi:https://rej.uchile.cl/index.php/RECEJ/article/view/67885/72263

Case Guard. (29 de Junio de 2022). Obtenido de La Ley de Fraude y Abuso Informático de 1986: https://caseguard.com/es/articles/la-ley-de-fraude-y-abuso-informatico-de-1986/#:~:text=La%20Ley%20de%20Fraude%20y%20Abuso%20Inform%C3%A1tico%20o%20CFAA%20por,los%20Estados%20Unidos%20de%20Am%C3%A9rica

Cevallos López, Y. D., Pupo Kairuz, A., Calderón Ramíez, M. A., & Ponce Ruiz, D. V. (2020). La interpretación extensiva y la analogía en los delitos de estafa con documentos bancarios. Revista Científica Mundo de la Investigación y el Conocimiento, 4-12. Obtenido de https://www.recimundo.com/index.php/es/article/download/774/1293?inline=1#:~:text=La%20interpretaci%C3%B3n%20extensiva%20es%20aquella,se%20incide%20en%20la%20analog%C3%ADa.

(s.f.). Código Orgánico Integral Penal. Asamblea Nacional. Obtenido de https://vlex.ec/vid/codigo-organico-integral-penal-631464447

Constitución de la República del Ecuador. (2008). Ecuador. Obtenido de https://educacion.gob.ec/wp-content/uploads/downloads/2012/08/Constitucion.pdf

Cuatrecasas. (21 de Abril de 2022). Obtenido de La Agencia Española de Protección de Datos ha sancionado a distintas empresas del sector telefónico por sucumbir ante el "SIM swapping: https://www.cuatrecasas.com/es/global/propiedad-intelectual/art/espana-el-sim-swapping-y-el-motivo-por-el-que-la-aepd-esta-multando-a-empresas-de-telefonia

Cyber Intelligence Team. (20 de Diciembre de 2022). TARLOGIC. Obtenido de SIM Swapping, cuando tu teléfono y tu dinero, quedan al descubierto.: https://www.tarlogic.com/es/blog/sim-swapping-tu-telefono-queda-descubierto/

El Heraldo de México. (6 de Marzo de 2021). ¡Se pasó de listo! Estudiante BECADO robó más de 7.5 millones usando los CHIPS de celulares. Obtenido de https://heraldodemexico.com.mx/mundo/2021/3/6/se-paso-de-listo-estudiante-becado-robo-mas-de-75-millones-usando-los-chips-de-celulares-266476.html

Fernández, S. (29 de Agosto de 2022). Xataka Android. Obtenido de Así funciona el 'SIM Swapping', un método de robo de identidad que puede causarnos muchos problemas : https://www.xatakandroid.com/seguridad/asi-funciona-sim-swapping-metodo-robo-identidad-que-puede-causarnos-muchos-problemas

Gavilanes Domínguez, C. D. (2022). EL CONCURSO IDEAL DE INFRACCIONES EN RELACIÓN A LOS DELITOS QUE SE DESPRENDAN DE LA ASOCIACIÓN ILÍCITA. Ambáto: Pontifica Universidad Católica del Ecuador.

Glaesser, M.-L., & Alonso, M. (09 de Octubre de 2014). BCN INFORME. Obtenido de Los delitos cibernéticos en la legislación estadounidense: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20864/5/FINAL%20_%20Informe%20_%20Cibercrimen%20en%20EEUU_v5.pdf

Hacienda: Secretaría de Hacienda y Crédito Público. (2023). Fraudes Financieros. Cuídate del SIM SWAPPING. Obtenido de Educación Financiera en tu Institución: https://www.uv.mx/iiesca/files/2023/01/EFI_H_Cuidate-del-SIM-Swapping.pdf

Intercambio de SIM O SIM Swapping: una estafa de teléfono móvil. (2021). Obtenido de https://s1.aebanca.es/wp-content/uploads/2021/10/sim-swapping-cyberscamses.pdf

Islas Montes, R. (2009). Sobre el principio de legalidad. Anuario de Derecho Constitucional Latinoamericano, 97-108. Obtenido de https://www.corteidh.or.cr/tablas/r23516.pdf

Jendruszak, B. (17 de Marzo de 2022). SIM Swapping: Qué es y cómo prevenirlo. Obtenido de SEON: https://seon.io/es/recursos/que-es-el-sim-swapping/

Jiménez Alemán, J. A. (2018). Notas acerca del concurso de infracciones en el Derecho Administrativo Sancionador: caso peruano. Derecho & Sociedad, 55-78.

Kierszenbaum, M. (2009). EL BIEN JURÍDICO EN EL DERECHO PENAL. ALGUNAS NOCIONES BÁSICAS DESDE LA ÓPTICA DE LA DISCUSIÓN ACTUAL. Lecciones y Ensayos , 187-211. Obtenido de http://www.derecho.uba.ar/publicaciones/lye/revistas/86/07-ensayo-kierszenbaum.pdf

La justicia restaurativa y el derecho al debido proceso en contextos educativos. , 456-20-JP (Corte Constitucional del Ecuador 10 de Noviembre de 2021).

Leal, A. (23 de Abril de 2019). Criptonoticias. Obtenido de 10 años de cárcel por robar criptoactivos pirateando teléfonos inteligentes: https://www.criptonoticias.com/seguridad-bitcoin/10-anos-carcel-robar-criptoactivos-pirateando-telefonos-inteligentes/

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (1995). España. Obtenido de https://www.boe.es/eli/es/lo/1995/11/23/10/con

Maldonado Padilla, E. N. (2016). Los delitos informáticos y el derecho constitucional a la seguridad jurídica. Babahoyo: Universidad Regional Autónoma de los Andes. Obtenido de https://dspace.uniandes.edu.ec/bitstream/123456789/7137/1/TUBAB089-2016.pdf

Medina Martínez, J. J., Cárdenas Osorio, C. H., & Mejía Lobo, M. (2021). ANÁLISIS DEL PHISHING Y LA LEY DE DELITOS INFORMÁTICOS EN COLOMBIA. Cuaderno de Investigaciones Semilleros Andina, 75-80.

Ministerio del Interior y Seguridad Pública. (2021). Ciberconsejos de seguridad para evitar los peligros del SIM Swapping. Obtenido de https://www.csirt.gob.cl/media/2021/06/Landing-SIM-Swapping-2021-1.pdf

Oropeza Mendoza, D. K. (2012). LA SEGURIDAD JURÍDICA EN EL COMERCIO ELECTRÓNICO FRENTE A LAS CONDUCTAS DELICTIVAS QUE LESIONAN SU DESARROLLO. Veracruz: Estudios Jurídicos contemporáneos VIII, del Instituto de Investigaciones Jurídicas de la Universidad Veracruzana.

Piza Burgos, N. D., Amaiquema Márquez, F. A., & Beltrán Baquerizo, G. E. (2019). Métodos y técnicas de la investigación cualitativa. Algunas precisiones necesarias. . Conrado. Revista pedagógica de la Universidad de Cienfuegos.

Sierra, A. (20 de Julio de 2018). El Mundo. Obtenido de ¿Qué es el "sexting" y por qué supone un riesgo?: https://www.elmundo.es/vida-sana/sexo/2018/07/20/5b50b3eb468aeb2a7d8b464e.html

TrendTIC. (11 de Noviembre de 2020). Obtenido de CHILE: ALERTAN ANTE AUMENTO DE 'SIM SWAPPING' O SUPLANTACIÓN DE LA TARJETA SIM CHILE: ALERTAN ANTE AUMENTO DE 'SIM SWAPPING' O SUPLANTACIÓN DE LA TARJETA SIM: https://www.trendtic.cl/2020/11/chile-alertan-ante-aumento-de-sim-swapping-o-suplantacion-de-la-tarjeta-sim/

Universidad de Cádiz . (Junio de 2018). Los Soportes de Información . Obtenido de https://sistinfo.uca.es/wp-content/uploads/2018/06/documento_explicativo_bloque_II_los_soportes-UCA.pdf

Vallejo Naranjo, D. E. (2019). La aplicación del concurso real de infracciones en relación al debido proceso penal ecuatoriano. Ambáto: Pontificia Universidad Católica del Ecuador.