ISSN: 2806-5697
Vol. 4 – Núm. E2 / 2023

La protección de datos de carácter personal frente al delito de interceptación ilegal de datos

The protection of personal data against the crime of illegal data interception

A proteção dos dados pessoais contra o crime de interceção ilegal de dados

Sebastián Alejandro Cornejo Ramos
Universidad Tecnológica Indoamérica
scornejo@indoamerica.edu.ec
https://orcid.org/0009-0000-1771-7022

Danny Xavier Sánchez
Universidad Tecnológica Indoamérica
dannysanchez@uti.edu.ec
https://orcid.org/0000-0001-5783-2682

DOI / URL: https://doi.org/10.55813/gaea/ccri/v4/nE1/192

Como citar:

Cornejo S. & Sánchez, D. (2023). La protección de datos de carácter personal frente al delito de interceptación ilegal de datos. *Código Científico Revista de Investigación*, 4(E2), 984-1023.

Recibido: 25/08/2023 **Aceptado:** 26/09/2023 **Publicado:** 29/09/2023

Resumen

La protección de datos personales ha cobrado una importancia crucial en la era de la creciente digitalización y el desarrollo tecnológico para proteger los derechos fundamentales y la privacidad de las personas en línea. El objetivo principal de este estudio es analizar el sistema legal actual de Ecuador para proteger la información personal de la interceptación no autorizada. Para lograr este objetivo, se realizará un análisis exhaustivo de la Ley Orgánica de Datos Personales y el Código Orgánico Integral Penal con relación al delito de interceptación ilegal de datos a fin de determinar y comprender cómo estas leyes respaldan y protegen los datos de los ciudadanos contra los delitos cibernéticos. El problema cuestionarnos si la normativa legal ecuatoriana es adecuada para proteger la información personal y cuestionar si la norma penal es la vía más adecuada para su protección. Comprender el alcance y la complejidad de este problema, así como la necesidad de tomar precauciones sensatas para reducir los riesgos que plantea, es crucial dada la rapidez con la que se desarrolla el entorno digital. La metodología utilizada será inductiva, documental y analítica, con un análisis minucioso de las disposiciones legales pertinentes en Ecuador. El artículo busca ofrecer una visión integral para futuras políticas de protección de datos en Ecuador.

Palabras Clave: Protección, personales, datos, interceptación y delito.

Abstract

Protection of personal data has become crucially important in the era of increasing digitalization and technological development to protect the fundamental rights and privacy of people online. The main objective of this study is to analyze Ecuador's current legal system to protect personal information from unauthorized interception. To achieve this objective, an exhaustive analysis of the Organic Law of Personal Data and the Comprehensive Organic Criminal Code will be carried out in relation to the crime of illegal interception of data in order to determine and understand how these laws support and protect citizens' data against cybercrimes. The problem is to question whether the Ecuadorian legal regulations are adequate to protect personal information and to question whether the criminal law is the most appropriate means for its protection. Understanding the scope and complexity of this problem, as well as the need to take sensible precautions to reduce the risks it poses, is crucial given how quickly the digital environment is developing. The methodology used will be inductive, documentary and analytical, with a thorough analysis of the relevant legal provisions in Ecuador. The article seeks to offer a comprehensive vision for future data protection policies in Ecuador.

Keywords: Protection, personal, data, interception and crime**.**

Resumo

A proteção dos dados pessoais tornou-se crucialmente importante na era da crescente digitalização e do desenvolvimento tecnológico para proteger os direitos fundamentais e a privacidade das pessoas online. O principal objetivo deste estudo é analisar o atual sistema jurídico do Equador para proteger as informações pessoais contra interceptação não autorizada. Para atingir este objetivo, será realizada uma análise exaustiva da Lei Orgânica dos Dados Pessoais e do Código Penal Orgânico Integral em relação ao crime de interceção ilegal de

dados, a fim de determinar e compreender como essas leis apoiam e protegem os dados dos cidadãos. contra crimes cibernéticos. O problema é questionar se as regulamentações legais equatorianas são adequadas para proteger as informações pessoais e questionar se as regulamentações penais são o meio mais adequado para a sua proteção. Compreender a dimensão e a complexidade deste problema, bem como a necessidade de tomar precauções sensatas para reduzir os riscos que representa, é crucial dada a rapidez com que o ambiente digital está a desenvolver-se. A metodologia utilizada será indutiva, documental e analítica, com uma análise aprofundada das disposições legais relevantes no Equador. O artigo procura oferecer uma visão abrangente para futuras políticas de proteção de dados no Equador.

Palavras-chave: Proteção pessoal, dados, interceptação e crime.

Introducción

En la sociedad actual, la protección de datos de carácter personal se ha convertido en una cuestión de importancia. En un mundo cada vez más digitalizado, las vidas de los seres humanos están profundamente entrelazadas con la tecnología, lo que hace a los seres humanos vulnerables a posibles ataques cibernéticos que comprometan la privacidad y derecho a la intimidad. Ante esta situación es de importancia llevar a cabo un análisis minucioso de la legislación ecuatoriana pertinente, en especial la Ley Orgánica de Datos Personales [LODP] (2021) y el Código Orgánico Integral Penal [COIP] (2014), para evaluar su eficacia en la protección de datos frente a estos delitos informáticos.

De esta forma dentro de los delitos en análisis, se encuentran prácticas como el acceso no autorizado a sistemas informáticos, la obtención ilícita de datos personales y el robo cibernético de información sensible. Estas actividades criminales, llevadas a cabo por individuos malintencionados, no solo comprometen la privacidad, sino que pueden tener consecuencias devastadoras para la vida y la confianza en la tecnología que tanto nos beneficia.

Es fundamental comprender si la legislación ecuatoriana actual es lo suficientemente robusta para prevenir y sancionar estos delitos informáticos, y si se encuentran en constante actualización para adaptarse a las nuevas y sofisticadas formas de ataque. También es esencial

identificar posibles lagunas en el marco legal, para así fortalecer las leyes y políticas en torno a la protección de datos, garantizar la privacidad y la seguridad de cada individuo.

Es así que, la protección de datos personales frente al delito de interceptación ilegal de información es una cuestión realmente importante en la actualidad, dado que, vivimos en una era digital donde la privacidad está expuesta a diversos riesgos, por lo que es urgente que la legislación en Ecuador esté siempre actualizada y preparada para enfrentar las nuevas amenazas cibernéticas que van surgiendo. Todos, ciudadanos, empresas e instituciones, debemos unir esfuerzos para construir un entorno digital seguro y confiable, donde podamos proteger los derechos fundamentales en este mundo en constante cambio

El objetivo jurídico principal de la Protección de Datos de Carácter Personal frente al delito de interceptación ilegal de datos es salvaguardar la privacidad y la integridad de la información personal de los individuos, garantizando su derecho fundamental a la protección de datos. Esto implica establecer mecanismos legales y regulaciones que prevengan, sancionen y disuadan la interceptación no autorizada o ilegal de datos personales. Sin embargo, la interceptación ilegal de datos se refiere a la obtención, acceso, divulgación o uso no autorizado de información personal, ya sea electrónica o física, por parte de terceros sin el consentimiento del titular de los datos. La protección de datos busca prevenir que esta actividad ilícita ocurra, así como proporcionar mecanismos para que las personas afectadas puedan ejercer sus derechos y tomar medidas legales en caso de violación de su privacidad. La norma que tiene leyes y regulaciones de protección de datos establecen una serie de principios y obligaciones que las organizaciones y personas deben cumplir al procesar datos personales, incluyendo el consentimiento informado del titular de los datos, la implementación de medidas de seguridad adecuadas y la notificación en caso de violaciones de seguridad. En caso de que se produzca una interceptación ilegal de datos, las leyes pueden establecer sanciones y procedimientos legales para hacer frente a la infracción y compensar a las personas afectadas.

Esto con lleva a garantizar el respeto y la protección de la privacidad de las personas, así como establecer mecanismos efectivos para prevenir y sancionar cualquier actividad ilegal relacionada con la obtención y uso no autorizado de datos personales.

realizará un análisis exhaustivo de las leyes de protección de datos personales del Ecuador, con énfasis en la Ley Orgánica de Datos Personales (2021) y el Código Orgánico Integral Penal (2014). El objetivo es determinar qué tan bien protegen estas leyes la información personal de los ciudadanos contra los delitos cibernéticos, como la piratería informática, la obtención ilegal de información personal y el robo cibernético de datos confidenciales.

La seguridad de los datos personales es ahora fundamental para proteger la privacidad y la intimidad de las personas en el entorno digital cada vez más complejo de la sociedad actual. Para prevenir y sancionar de manera efectiva los delitos cibernéticos relacionados con el acceso y uso indebido de datos personales, es importante saber si las leyes vigentes son sólidas y están actualizadas.

Será posible identificar fallas o vacíos en el sistema legal actual a través de un análisis metódico y completo. Para garantizar la privacidad y seguridad de cada persona en el entorno digital moderno, a fin de realizar recomendaciones bien informadas para fortalecer y mejorar las leyes y políticas en torno a la protección de datos. Es necesario cuestionarnos en este sentido si la vía penal es la estructura legal correcta para la protección de esta clase de datos.

Los resultados de este estudio deberían influir significativamente en la creación y aplicación de políticas efectivas para salvaguardar los datos personales en el Ecuador abordando este objetivo desde un punto de vista legal. Además, pretende aumentar la comprensión sobre la importancia de contar con una legislación sólida y vigente que permita enfrentar los nuevos desafíos en el ámbito digital y garantice un entorno confiable y seguro para todos los ciudadanos y sus datos personales.

Delito de interceptación ilegal de datos.

1. **La ciberdelincuencia en Ecuador**

Para La ciberdelincuencia en Ecuador ha ido en aumento en los últimos años, representando un desafío significativo para la seguridad digital de los ciudadanos y las instituciones. En un mundo cada vez más conectado, los delincuentes informáticos aprovechan las vulnerabilidades de los sistemas y las redes para llevar a cabo una variedad de actividades delictivas, como el robo de información personal, la suplantación de identidad, el fraude en línea y el ciberacoso. Uno de los principales factores que contribuye al aumento de la ciberdelincuencia en el país es el crecimiento exponencial de la tecnología y el acceso a Internet. A medida que más personas se conectan en línea, aumenta el potencial de ser víctimas de ataques cibernéticos, dado que,

> Las relaciones sociales han innovado con la aplicación de las tecnologías de información y con información personal auténtica o ficticia y acceder a un mundo de comunicaciones e interacciones con amigos, familiares, compañeros o simplemente relacionarse con usuarios completamente desconocidos que cuente con un perfil dentro de una red social como Facebook, convirtiéndose sin lugar a dudas en el instrumento favorito para el contacto e intercambio de experiencias (Obregón, Gómez, & López, 2017, p. 2).

Es por esto que, los delincuentes utilizan diversas técnicas sofisticadas para infiltrarse en sistemas informáticos, lo que pone en riesgo la privacidad y la seguridad de la información personal. El phishing y el malware son dos de las tácticas más comunes utilizadas por los ciberdelincuentes para obtener información confidencial y acceder a sistemas de manera no autorizada. (Cruz, Delgado, Ponce, & Marcillo, 2022)

El phishing, por ejemplo, se presenta como correos electrónicos falsos que engañan a los usuarios para que revelen datos personales valiosos, como contraseñas o información

financiera. Por otro lado, el malware es un software malicioso que puede dañar sistemas y permitir accesos no deseados a la información.

Esta particular moda surgió como un juego, a finales de 2004, en el barrio londinense de Lewisham, cuando los jóvenes grababan en vídeo la cara de sorpresa que ponían otros menores al recibir una colleja (golpe que se da en la nuca con la palma de la mano); a partir de ahí, la conducta degeneró volviéndose cada vez más violenta y agresiva, al tiempo que se extendía por toda Europa y Estados Unidos, hasta que se produjo la primera muerte (Pérez, 2013, p.1).

Además, la ciberdelincuencia también abarca delitos como el grooming, el cual se manifiesta como acoso sexual hacia niños y adolescentes a través de las redes sociales, y el "happy slapping", que es una agresión física capturada en video y compartida en línea como un juego peligroso entre jóvenes, con actos que pueden llegar a la muerte de la otra persona por el golpe que se realiza en la cabeza, estas agresiones se publican, comparten o se suben a la red con el fin de ser visualizadas por otras personas y para llegar a ser una tendencia popular.

Este tipo de delitos generalmente quedan en la impunidad por la volatilidad de la información, la globalización del internet y el anonimato. La falta de procesos claros y el desconocimiento por parte del usuario sobre el marco legal existente, para penalizar este tipo de prácticas antijurídicas, crean dificultad para identificar a los autores materiales e intelectuales del hecho, siendo este, uno de los principales problemas al emprender investigaciones de delitos realizados por medios telemáticos en el Ecuador (Obregón, Gómez, & López, 2017, p.2).

En respuesta a este creciente problema, Ecuador ha promulgado la Ley Orgánica de Protección de Datos Personales, buscando garantizar el ejercicio del derecho a la protección de datos y regular mecanismos de tutela. Sin embargo, es fundamental que todos los organismos

y la sociedad en general se involucren en la concienciación y prevención de estos delitos, así como en el desarrollo de nuevas estrategias para combatir la ciberdelincuencia.

El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela (Ley Orgánica de Protección de Datos Personales, 2021, art.1).

Si bien se han implementado medidas y avances significativos en la protección contra el ciberdelito en Ecuador, todavía existen desafíos y amenazas persistentes en el ámbito digital. Las autoridades gubernamentales y las instituciones han trabajado arduamente para fortalecer la seguridad en línea y promulgar leyes que protejan los datos personales de los ciudadanos. Sin embargo, en un mundo tecnológicamente cambiante, es esencial mantenernos alerta y seguir avanzando en la concienciación y prevención de los delitos cibernéticos.

En dicho problema y gracias a la ayuda de las paginas en la cual se destacan datos relevantes en el Ecuador como el uso que cada ecuatoriano mantiene dentro de las redes sociales, juegos, interfaces, entre otras. Se toma en cuenta las principales estadísticas de la rutina que se crea día a día dentro del territorio.

El ecuador al tener 18.47 millones de habitantes la que mantiene un uso del internet. Sin embargo, Google un sistema la cual mantiene dentro de las misma diferentes interfaces que es de fácil de acceso con el fin de dar un ambiente cibernético familiar, profesional, entre otros aspectos. Se toma en cuenta que al menos el 76% de la población ecuatoriana está dentro de la red, este se conecta por diferentes medios tecnológicos como computadoras, teléfonos, tabletas u otro medio con software.

El ecuador al ser un país que está en constate desarrollo en este medio del internet. Sin embargo, en el litoral existe mayor acogida de redes sociales con un 26% y la parte interandina con un 20%, las demás regiones no tienen acogida al sistema o interfaz del mundo en línea.

El apoyo o colaboración entre organismos gubernamentales, el sector privado y la sociedad civil es clave para abordar los desafíos que plantea la ciberdelincuencia. La educación y la capacitación sobre seguridad en línea son herramientas poderosas para empoderar a los ciudadanos y ayudarles a protegerse en el mundo digital. Además, el desarrollo de tecnologías avanzadas y la adopción de prácticas de seguridad sólidas son fundamentales para mantenernos un paso adelante de los ciberdelincuentes.

Es importante comprender que ninguna nación está completamente inmune a los delitos cibernéticos, y el Ecuador no es una excepción. Sin embargo, al continuar trabajando juntos y manteniéndonos actualizados con las mejores prácticas de seguridad, podemos seguir fortaleciendo la defensa contra el ciberdelito y proteger la privacidad y seguridad de los datos personales en el entorno digital en constante evolución. La protección contra el ciberdelito es una responsabilidad compartida, y es vital que todos se comprometan hacer parte para mantenernos seguros en línea.

2. La Forma de Control preventivo y correctivo

Las formas de control preventivo y correctivo frente al uso desmedido de información personales una forma que permite mantener la intimidad e integridad de las personas a salvo. deben proteger los datos personales con el objetivo de que la información se encuentre resguardada o segura. Cada uno de los controles cibernéticos de seguridad que se manifiesta en cada página o donde se pueda reservar información deben mantener un protección alta e inviolable para las personas la cual puedan afectar con dichos módulos.

Los datos están empezando a hacer usados y reutilizados para los más diversos propósitos, muchos de los cuales puede ser perjudiciales para su titular. Por tanto, resulta necesario actualizar el significado del derecho a la privacidad en una economía digital, en la que la protección de los datos personales se ha convertido en una pieza fundamental (Porcelli, 2019, p.1).

Los datos personales de cada uno de los ecuatorianos se mantienen en un sistema tanto público como privado dentro del software que almacena datos.

Cada uno de estos datos Personales deben ser confidenciales para las personas por la cual preguntan, ya que son de carácter personal. Cada uno de los sitios mencionados mantiene un protocolo y su seguridad va incrementando según los ataques cibernéticos que recibe, esto se produce como algo negativo para la sociedad, ya que los datos pueden estar encriptándose desde dispositivos la cual no consten como amigable y estos se mantenga en venta en el mercado negro dentro del internet.

En Ecuador, la lucha contra el delito de ciberseguridad se basa en un enfoque integral que combina medidas preventivas y correctivas para proteger a los ciudadanos y las instituciones de los ciberdelincuentes. Estas estrategias abarcan tanto el ámbito público como el privado, y tienen como objetivo fortalecer la seguridad en línea y reducir los riesgos asociados con el ciberdelito, en términos de control preventivo, las autoridades ecuatorianas han trabajado en la promulgación de leyes y políticas para proteger los datos personales y prevenir el acceso no autorizado a sistemas y redes. La Ley Orgánica de Protección de Datos Personales, por ejemplo, establece principios y mecanismos de tutela para garantizar el ejercicio del derecho a la protección de datos, esto bajo la normativa internacional.

Estándares de Protección de Datos de los Estados Iberoamericanos. Consisten en un conjunto de directrices orientadoras cuyo objetivo reside en proporcionar un marco normativo que guíe los proyectos de ley de protección de datos personales en la región iberoamericana en

aquellos países que aún no cuentan, en sus ordenamientos jurídicos, con una legislación, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes (Porcelli, 2019, p.2).

Además, se fomenta la concienciación y la educación en materia de ciberseguridad a través de campañas y programas destinados a informar a la población sobre las amenazas cibernéticas y las mejores prácticas de seguridad en línea. La colaboración entre instituciones gubernamentales, el sector privado y la sociedad civil también es clave para compartir información y recursos, así como para implementar estrategias conjuntas para combatir el ciberdelito.

Por otro lado, en cuanto al control correctivo, Ecuador cuenta con unidades especializadas en delitos informáticos y ciberseguridad que se encargan de investigar y perseguir a los ciberdelincuentes. Estas unidades trabajan en estrecha colaboración con las fuerzas de seguridad y las instituciones judiciales para identificar y detener a los responsables de delitos cibernéticos y llevarlos ante la justicia. Asimismo, se promueve la adopción de tecnologías avanzadas y sistemas de seguridad en las instituciones y empresas para detectar y prevenir posibles ataques cibernéticos. (UNODC,2022)

La actualización constante de software y la implementación de medidas de protección de datos son fundamentales para mantenerse protegido ante las amenazas cibernéticas en constante evolución, por este motivo Ley Orgánica de Protección de Datos Personales (2021) menciona que este ordenamiento jurídico “se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior” (art.2)

La ley que se presenta en el territorio menciona que todo dato personal será tratado de la manera que este no pueda ser vulnerado por otros usuarios que se encuentren dentro de la red, esto consta en ordenadores u otros medios en la que se puedan almacenar datos de carácter

personal, el automatizado que debe mantener debe ser de gran impacto para estos delincuentes con el fin de que el derecho a la intimidad no sea violado de manera fácil. La modernización que surge en el país es un gran paso, ya que este, protege de mejor manera. Sin embargo, este sistema debe estar en renovación.

El internet al ser una herramienta la cual crece y mantiene ventajas, los sistemas deben renovarse y mantener mejor seguridad para el usuario. Es así que, el control preventivo y correctivo del delito de ciberseguridad en Ecuador implica un esfuerzo conjunto y continuo por parte de todos los actores involucrados. A través de la colaboración, la educación y la implementación de tecnologías avanzadas, se puede fortalecer la defensa contra los ciberdelincuentes y garantizar un entorno digital seguro y protegido para todos, tomando en cuenta la normativa promulgada por el país como una forma de seguridad.

3. La Intimidad como bien jurídico protegido ante el delito de intercepción ilegal de datos.

En El concepto de intimidad se ha convertido en un bien jurídico fundamental y protegido en la era digital actual, especialmente frente al delito de intercepción ilegal de datos. La privacidad de las personas, en el ámbito tanto personal como familiar, es esencial para mantener la autonomía y proteger los derechos fundamentales. Sin embargo, en este mundo conectado y tecnológicamente avanzado, la intercepción ilegal de datos representa una amenaza constante a la intimidad y seguridad en línea.

La intercepción ilegal de datos, también conocida como "hackeo" o "acceso no autorizado", implica la intromisión en sistemas informáticos o redes para obtener información confidencial sin el consentimiento de los titulares. Esta práctica pone en peligro la privacidad y la confidencialidad de los datos personales, lo que puede resultar en consecuencias devastadoras para las personas afectadas.

En comparación con el bien jurídico, el concepto de delito informático ha sido abordado por un número mucho menor de autores, fundamentalmente porque constituye un término relativamente reciente, cuyo surgimiento no es imaginable sin la existencia de computadoras. Se trata, no obstante, de una expresión equívoca, ya que se la emplea para aludir a realidades que no son coincidentes entre sí (Mayer, 2017, p.3).

Los datos de carácter personal pueden ser identificados como un bien jurídico protegido debido a su relevancia en la vida de las personas y su impacto en la privacidad y la seguridad individual. Estos datos son una parte fundamental de la identidad y contienen información confidencial, como nombres, direcciones, números de teléfono, correos electrónicos, entre otros.

La protección de estos datos se vuelve esencial en un mundo cada vez más digitalizado, donde la información personal circula constantemente a través de internet y otras plataformas. El acceso no autorizado o el uso indebido de estos datos puede llevar a consecuencias negativas, como el robo de identidad, el fraude, el acoso o la discriminación.

El Código Orgánico Integral Penal (2014) establece sanciones para quienes cometan delitos informáticos, como la interceptación ilegal de datos. De acuerdo con el artículo 227 del COIP, "La persona que, sin autorización o excediendo la que tenga, interceptare comunicaciones privadas, captare comunicaciones no públicas o accediere indebidamente a sistemas informáticos o a redes de telecomunicaciones, será sancionada con pena privativa de libertad de uno a cinco años".

Por esta razón, diversas legislaciones y normativas, como la LOPD y el COIP en Ecuador, establecen medidas para garantizar la privacidad y seguridad de la información personal. Estas leyes buscan asegurar que los datos de carácter personal sean utilizados de manera legítima, transparente y bajo el consentimiento del titular, protegiendo así el derecho a la intimidad y la autodeterminación informativa.

Por ende, los datos de carácter personal son considerados un bien jurídico protegido debido a su importancia para preservar la privacidad y la dignidad de cada individuo en un entorno digital en constante cambio. La regulación adecuada y el cumplimiento de las normativas en materia de protección de datos, como la LOPD y el COIP en Ecuador, son fundamentales para salvaguardar los derechos en el mundo digital actual.

Cabe mencionar que, la protección de los datos personales ante un delito de carácter informático solo tendrá consecuencia dentro del mundo de la red, esto quiero decir que este solo es ejecutado dentro de los dispositivos tecnológicos con software y hardware que son capaces de contener información y sean de fácil acceso. El tiempo cambia y la forma de operar cada vez se refleja de mejor manera, esto quiere decir que las encriptaciones se disfrazan de alguna manera y roban información.

En este sentido, los avances tecnológicos y la adopción de prácticas de seguridad sólidas son cruciales para prevenir y detectar posibles violaciones de la intimidad. La colaboración entre las autoridades gubernamentales, el sector privado y la sociedad civil es clave para desarrollar estrategias efectivas de protección de datos y promover una cultura de conciencia y respeto hacia la privacidad en línea.

La intimidad como bien jurídico protegido debe ser resguardada a través de la implementación de leyes y medidas de seguridad que desalienten y sancionen la intercepción ilegal de datos. Asimismo, es importante que cada individuo tome conciencia de la importancia de proteger su privacidad y adopte prácticas seguras en el uso de la tecnología. Es así que la protección de la intimidad como bien jurídico es esencial para garantizar los derechos y libertades en el mundo digital. La intercepción ilegal de datos representa una amenaza constante, por lo que es imperativo que tomemos medidas proactivas para salvaguardar la privacidad y seguridad en línea.

Por su parte como se ha mencionado, en Ecuador, el robo de información es considerado un delito y está establecido en el Código Orgánico Integral Penal (2014). Estas medidas legales están destinadas a proteger los derechos de las personas y evitar que sus derechos legales sean vulnerados.

Sin embargo, hay cierta confusión sobre qué se entiende como bien jurídico en este contexto. Algunas personas argumentan que el "software" también es un bien de valor económico y que su dueño tiene derechos reconocidos o permitidos por la ley (Mayer, 2017, p.8). Este tema se centra en si el software debería ser considerado como un bien protegido por las leyes, al igual que la propiedad o el patrimonio.

Por ende, el robo de información es un delito sancionado en Ecuador, pero existe un debate sobre qué bienes jurídicos están involucrados, especialmente en lo relacionado al software y sus derechos legales.

De la misma en cuanto a los aspectos subjetivos de este delito, es fundamental considerar el fraude como un elemento clave para la configuración del delito. Esto implica que la actividad delictiva debe ser cometida con pleno conocimiento e intención por parte del sujeto activo. Por lo tanto, debe tener la intención específica de acceder, divulgar o utilizar información personal protegida sin el conocimiento o consentimiento del interesado.

También deberá tenerse en cuenta el conocimiento específico que tenga el sujeto activo sobre el estado de protección de los datos a los que acceda o comunique ilícitamente. Esto demuestra cuán crucial es que el autor sea consciente de que sus acciones sugieren una violación del derecho a la privacidad y los datos personales del titular. Elementos como el acceso, divulgación o uso de datos personales se destacan cuando se trata de los aspectos objetivos del delito. El comportamiento delictivo común puede tomar muchas formas diferentes, como el acceso no autorizado a una base de datos protegida, la publicación de

información privada en los medios o el uso no autorizado de la información personal de una persona.

Es necesario que los datos en cuestión sean datos personales, o información que pueda utilizarse para identificar o hacer identificable a una persona física, para que se establezca el delito. Esto garantiza que el propósito de la protección de datos es proteger la privacidad de las personas y prevenir el mal uso de su información personal. Adicionalmente, el delito de protección de datos personales suele consistir en que el sujeto activo actúe en contra de la voluntad expresa del titular de los datos o sin su debida autorización o consentimiento. De esta forma, el hecho de que el titular haya dado su consentimiento válido para el tratamiento de sus datos es información relevante para la investigación penal. Para una protección eficaz de los datos personales y su protección contra posibles violaciones, es necesario un análisis exhaustivo y profundo de los componentes subjetivo y objetivo.

En la era digital, ahora es de vital importancia proteger el derecho a la privacidad de la interceptación de datos no autorizada. Las comunicaciones personales deben mantenerse privadas y confidenciales para proteger la dignidad, la autonomía y la libertad de las personas en un mundo conectado y tecnológicamente dependiente. Pero con el avance de la tecnología, también se ha facilitado el acceso de individuos ilegales a la información personal y la realización de interceptaciones, lo que presenta serios problemas para la defensa de los derechos tanto individuales como colectivos.

Por varias razones, la intimidad es crucial como un derecho legal protegido contra el delito de recopilación de datos no autorizada por varias razones:

1. El respeto a la vida privada incluye todas las áreas de la vida privada de una persona, como sus comunicaciones, correspondencia y otras actividades que no deben estar sujetas a un escrutinio excesivo o interferencia de terceros, como el Estado o cualquier otra entidad.

2. Para promover la confianza en el uso de las tecnologías y las comunicaciones, se debe proteger la privacidad. Las personas pueden abstenerse de utilizar tecnologías que podrían mejorar sus vidas o su participación en la sociedad si no confían en que se respetará su privacidad.

3. Prevención del abuso y la discriminación: la interceptación ilegal de datos puede resultar en el uso indebido de la información obtenida, lo que podría dar lugar a abusos contra las personas afectadas, como extorsión, chantaje y otras formas de extorsión.

4. Protección de derechos conexos: Las libertades de expresión, asociación y el libre flujo de información son solo algunos ejemplos de los derechos fundamentales con los que se relaciona la privacidad. La invasión de la privacidad puede tener un impacto negativo en estos derechos, restringiendo el libre intercambio de ideas y la participación ciudadana.

5. Equilibrio entre seguridad y privacidad: es fundamental lograr el equilibrio adecuado entre el derecho a la protección de la privacidad y la necesidad justificable de mantener la seguridad y el orden públicos. Es necesario establecer garantías y procedimientos adecuados para el acceso a los datos personales a fin de proteger la privacidad y evitar el abuso de poder.

6. Confianza y seguridad en línea: en la era digital, muchas actividades diarias, incluidas las comunicaciones personales, la banca y las compras, se realizan en línea. Para garantizar la seguridad y la confianza en estos procedimientos, la protección de la privacidad es crucial. Las personas pueden ser reacias a usar servicios en línea o compartir información confidencial si la interceptación ilegal de datos se convierte en un lugar común, lo que podría tener un impacto en la economía digital y la participación ciudadana.

7. Protección contra el abuso y la discriminación: la obtención ilegal de datos puede dar lugar a situaciones de abuso, acoso, extorsión o discriminación contra las personas cuyos datos se obtuvieron. Como resultado, la confianza en las instituciones y en la sociedad

en su conjunto puede verse dañada, lo que puede tener un efecto devastador en las personas afectadas.

8. Vigilancia y control estatal: la interceptación ilegal de datos por parte del Estado u otras entidades puede utilizarse para ejercer un control excesivo sobre la población, socavando los valores fundamentales de una sociedad libre y democrática. Un control vital contra el abuso de autoridad y una garantía de que las personas no son objeto de vigilancia injustificada es la protección de la privacidad.

9. Marco legal y respeto por los derechos humanos: El marco legal y los tratados internacionales de derechos humanos sirven como base para la protección de la privacidad en el contexto de la interceptación ilegal de datos. Estas herramientas definen claramente cuándo y cómo se puede acceder a los datos personales para salvaguardar intereses legítimos, como la seguridad pública.

De esta manera la privacidad protege la dignidad, la autonomía, la libertad de expresión y pensamiento, la seguridad de las personas y es un derecho fundamental protegido contra la interceptación ilícita de datos. Su protección es fundamental para garantizar una sociedad democrática, justa y respetuosa de los derechos humanos en la era digital.

Ahora bien, en el contexto del tipo penal la contrariedad de un comportamiento con la norma jurídica se conoce como antijuricidad. En Ecuador, surge cuando alguien actúa de manera que viola el derecho fundamental de otra persona a mantener su vida privada y a proteger sus datos personales. La Constitución de la República reconoce el derecho a la intimidad, en particular el artículo 66 que establece que "Las personas tienen derecho a la intimidad en su vida personal y familiar y en su hogar". En cualquier medio, tienen derecho a la inviolabilidad y protección de su correspondencia y comunicaciones privadas.

Examinar en detalle una serie de aspectos importantes es necesario para un análisis más profundo del tipo penal de protección de datos personales frente al delito de interceptación ilegal de datos en el Ecuador tales como:

1. Derecho a la Privacidad y Protección de Datos Personales:

En Ecuador, la Constitución de la República consagra el derecho a la privacidad y la protección de datos personales, y la Ley Orgánica de Protección de Datos Personales sirve como soporte legal adicional.

Estos derechos están acordes con los estándares internacionales de protección de datos y privacidad, como los marcados por la Unión Europea (Reglamento General de Protección de Datos).

2. Tipificación del Delito:

El artículo 178 del Código Orgánico Integral Penal (COIP) tipifica la interceptación ilícita de datos. Lo anterior indica que las acciones que impliquen la adquisición no autorizada de datos informáticos o de telecomunicaciones están categóricamente prohibidas por la legislación penal ecuatoriana.

3. Delito Doloso y Elementos del Tipo Penal:

Como ya se mencionó, Ecuador generalmente considera la interceptación ilegal de datos como un delito. Esto sugiere que el delincuente es consciente de sus acciones y actúa con la intención deliberada de cometer el delito.

"Acceder", "interceptar", "obtener" o "reproducir" datos informáticos, electrónicos, telemáticos o de telecomunicaciones no autorizados son ejemplos de actos delictivos. Estos componentes específicos describen lo que es y lo que no es un comportamiento legal.

4. Sujetos y Verbos Rectores:

Es sujeto activo de este tipo de delito la persona que realiza la actividad ilícita, o quien comete la interceptación ilícita de datos.

La persona cuya privacidad ha sido invadida o a cuyos datos personales se ha accedido sin su consentimiento es el sujeto pasivo, quien también es víctima de la violación de su privacidad.

Para identificar las acciones precisas que constituyen el delito, son esenciales verbos rectores como "acceder", "interceptar", "obtener" o "reproducir". Cada uno de estos verbos refleja un caso específico de acceso a datos sin autorización y violación de la privacidad.

5. Sanciones y reparaciones:

El COIP establece sanciones específicas para quienes intercepten datos de forma ilegal. Sanciones, multas y otras medidas correctivas son todas sanciones posibles.

Además de enfrentar sanciones penales, las víctimas también tienen derecho a solicitar reparación y protección de sus derechos, lo que les faculta a presentar una demanda para recuperar los daños y perjuicios causados por la interceptación indebida de sus datos.

6. Legislación Comparada:

Es importante señalar que las leyes que rigen la protección de datos y la privacidad varían de un país a otro. En Ecuador, la interceptación ilegal de datos se aborda desde una perspectiva tanto de protección de datos como de delito.

De esta manera, Ecuador ha desarrollado un marco legal sólido para proteger la privacidad y la información personal de sus ciudadanos, con un enfoque en prevenir la recopilación de datos no autorizada. El análisis en profundidad de este tipo de delito demuestra la definición, prohibiciones y sanciones asociadas con acciones que violan la privacidad y seguridad de la información dentro de la nación. Establece un marco legal sólido para enfrentar el cibercriminal y salvaguardar la privacidad de las personas en la era digital. Esto refleja un compromiso con los derechos fundamentales de privacidad y datos.

Es ilegal interceptar las comunicaciones privadas a menos que sea un delito flagrante y la autoridad competente lo decida por razones justificadas, previa notificación a las personas

involucradas, y solo durante el tiempo que dure la situación que lo justifique. Dado que viola el derecho constitucional a la privacidad y la inviolabilidad de la correspondencia y las comunicaciones privadas, la intercepción ilegal de datos o la violación de la intimidad de una persona sin su consentimiento o sin la autorización adecuada se consideraría antijurídica.

Por su parte la tipicidad se refiere a la adecuación del comportamiento a la descripción que hace la ley penal de un delito específico. Por lo tanto, para que una conducta sea considerada delito, debe cumplir con las especificaciones establecidas en el tipo penal que protege la intimidad. El Código Orgánico Integral Penal de Ecuador establece una variedad de delitos relacionados con la protección de la intimidad y la privacidad de las personas. El artículo 178 del COIP sanciona la infracción de "Intervención ilegal en sistemas informáticos o de telecomunicaciones" si se accede, intercepta o utiliza datos informáticos, electrónicos, telemáticos o de telecomunicaciones que estén protegidos o presentes en un sistema informático o de telecomunicaciones sin autorización.

Este tipo de ley tiene como objetivo proteger la confidencialidad de las comunicaciones y datos de las personas y castigar a quienes la vulneren. El Ecuador tiene una Ley Orgánica de Protección de Datos Personales que regula cómo se tratan los datos personales y protege la privacidad de las personas. Esta ley también busca garantizar la seguridad y confidencialidad de los datos de los ciudadanos y prohíbe el uso indebido de datos personales.

La necesidad del uso del derecho penal para proteger datos de carácter personal en Ecuador es una cuestión fundamental en la era digital y se fundamenta en varios aspectos clave tales como:

1. Protección Efectiva de los Derechos Fundamentales: los datos personales y la privacidad son derechos fundamentales reconocidos en la Constitución de la República del Ecuador y respaldados por leyes específicas, como la Ley Orgánica de Protección de Datos Personales. Para la protección de la libertad y la dignidad de las personas, estos derechos son

cruciales. Debido a que el derecho penal ofrece sanciones y medidas disuasorias para quienes intenten violar estos derechos, se convierte en una herramienta necesaria para asegurar la protección efectiva de estos derechos.

2. Crecimiento de las amenazas en línea: con la llegada de Internet, cada vez se almacena más información personal en línea. Como resultado de esto, las amenazas digitales como la divulgación no autorizada de información personal y la interceptación ilegal de datos han aumentado. Para hacer frente a estas amenazas y disuadir a posibles delincuentes, el derecho penal se vuelve esencial.

3. Conciencia de la Gravedad de los Ciberdelitos: Tanto la sociedad ecuatoriana como la global son cada vez más conscientes de la gravedad de los ciberdelitos y las consecuencias que pueden tener. La pérdida de privacidad, el robo de identidad, el acoso en línea y otros daños emocionales y financieros son sólo algunos de los efectos devastadores que pueden resultar de la pérdida de datos personales. El derecho penal establece penas proporcionales a la gravedad de estos delitos y deja muy claro que ese comportamiento no será tolerado.

4. Repercusiones legales: La existencia de leyes de privacidad y protección de datos por sí sola es insuficiente para proteger adecuadamente a las personas y sus datos. La aplicación de sanciones legales es crucial para garantizar que quienes cometen delitos cibernéticos, como la interceptación ilegal de datos, enfrenten sanciones graves por sus acciones. Esto protege a las víctimas y disuade a otros de cometer los mismos crímenes. El derecho penal también se centra en prevenir y controlar los delitos digitales, además de imponer sanciones. Disponer de leyes penales claras y eficaces en este ámbito sirve como elemento disuasivo para quienes, de otro modo, podrían considerar la posibilidad de cometer delitos cibernéticos. Además, permite a las fuerzas del orden investigar, detener y procesar a los infractores, mejorando la ciberseguridad y la protección de datos del país.

5. Armonización con estándares internacionales: el uso del derecho penal para proteger datos personales ayuda a la armonización con estándares internacionales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Esto es fundamental en el mundo conectado de hoy porque hace que las transferencias internacionales de datos sean seguras y garantiza que las empresas y organizaciones que operan en Ecuador cumplan con los estándares internacionales de privacidad.

Por ende, el uso del derecho penal para proteger los datos personales en Ecuador es esencial para garantizar la protección efectiva de los derechos fundamentales a la privacidad y los datos en la era digital, previniendo los delitos cibernéticos, sancionando delincuentes y mantener el cumplimiento de las normas internacionales. Esto mejora tanto la seguridad de los datos como la confianza de la sociedad en mantener su privacidad en un entorno digital en constante cambio.

De esta manera cabe mencionar que, en Ecuador, los delitos relacionados con la violación de la privacidad y el acceso ilegal a datos personales se clasifican como delitos relacionados con el derecho a la intimidad. La antijuricidad ocurre cuando se vulneran los derechos fundamentales de una persona al acceder, interceptar, divulgar o utilizar datos personales o información privada sin su consentimiento o sin una base legal válida. La tipicidad se realiza para determinar si el comportamiento realizado cumple con las definiciones establecidas en la ley penal ecuatoriana, como los delitos tipificados en el COIP y otras leyes relacionadas con la protección de datos personales.

Ahora bien, los delitos se clasifican en dos categorías principales en el derecho penal: delitos dolosos y delitos culposos. La diferencia radica en el propósito del autor al actuar de manera punible.

el derecho penal es esencial en el ámbito personal frente al delito de interceptación ilegal de datos, ya que establece un marco legal que protege los derechos individuales, disuade

el delito, establece consecuencias claras, busca la justicia y la equidad, y garantiza la consistencia en la aplicación de la ley.

El derecho penal se establece como un mecanismo de ultima ratio con el fin de penar los ciberdelitos, estos delitos son ejecutados de manera dolosa, este tiene características como la punibilidad y el dolo, ya que este se establece en una acción antijuridica. Sin embargo, el sujeto está consciente de lo que comete.

De esta manera, cuando el autor actúa con la intención de cometer el hecho ilícito, se considera delito doloso. El autor, en este caso, actúa con la intención de lograr un resultado específico que la ley prohíbe, aunque es consciente de la naturaleza y las consecuencias de su acción. En el contexto de la violación a la intimidad, Si una persona accede ilegalmente a datos personales o información privada con la intención de obtener, divulgar o utilizar dicha información, estaría frente en un delito doloso en el contexto de la violación a la intimidad. Por su parte, cuando el autor actúa sin intención de cometer el delito, pero lo hace debido a negligencia, imprudencia, impericia u omisión de deberes de cuidado, se considera delito culposo. Si una persona accede a datos personales de manera negligente o imprudente sin tener la intención directa de violar la privacidad de otra persona, podríamos estar frente an un delito culposo en el contexto de la violación a la intimidad.

En el caso específico de la violación a la intimidad, en muchos sistemas jurídicos, incluyendo el Ecuador, la violación a la intimidad se consideraría un delito doloso. Esto se debe a que el acceso ilegal a datos o información privada generalmente implica que el autor intenta obtener información confidencial sin el consentimiento del titular. Por ende, el delito de intercepción ilegal de datos protege la Intimidad como bien jurídico, y se considera doloso porque el autor actúa con dolo al acceder, interceptar o utilizar datos protegidos sin el consentimiento de las personas, violando así la privacidad y confidencialidad de las personas como lo estipula la CRE.

Es necesario mencionar que el derecho a la intimidad posee sujetos y verbos que deben ser analizados en este caso cabe mencionar que, el sujeto activo es quien realiza el delito, es decir, quien interpone datos ilegalmente o viola la intimidad de otra persona. El autor o los autores de la conducta ilícita son responsables del delito de intercepción ilegal de datos si acceden, interceptan, obtienen, reproducen o divulgan información privada o datos personales sin la debida autorización o consentimiento.

El sujeto pasivo, por otro lado, es la víctima de la conducta delictiva. El sujeto pasivo en el caso de protección de la intimidad sería la persona cuya privacidad ha sido violada, o la persona cuyos datos personales o información privada han sido objeto de acceso o divulgación no autorizados.

El verbo rector, también conocido como verbo nuclear o verbo típico, es el elemento crucial en la descripción del tipo penal y define la acción específica que constituye el delito. El verbo rector en el caso del derecho a la intimidad puede variar según la tipificación del delito en cada nación. Algunos verbos rectores posibles en el tipo penal relacionado con la intimidad son:

- Acceder: se refiere a ingresar u obtener acceso a información o datos personales sin la autorización adecuada.
- Intercepta: se refiere al acto de interrumpir o capturar comunicaciones o datos de manera no autorizada.
- Obtener: se refiere a la adquisición o adquisición de información o datos sin el consentimiento del propietario.
- Reproducir: se refiere al acto de copiar o duplicar datos o información sin el permiso del titular.
- Divulgar: se refiere a la revelación o divulgación de información o datos que deberían mantenerse privados.

Estos verbos describen las acciones que conducen a la violación de la intimidad, como acceder a sistemas informáticos sin autorización, capturar comunicaciones privadas, obtener información personal sin consentimiento o revelar datos confidenciales a terceros.

Para conocer el verbo rector y la redacción precisa del tipo penal que protege el derecho a la intimidad y regula la intercepción ilegal de datos, es esencial consultar la legislación específica de cada país, como el Código Orgánico Integral Penal en el caso de Ecuador. Para proteger la privacidad y la confidencialidad de las personas y promover una sociedad en la que los derechos fundamentales sean respetados y protegidos, la ley establecerá las sanciones correspondientes para aquellos que cometan este delito.

La Protección de datos de carácter personal

1. Marco jurídico en materia de protección de datos de carácter personal

La legislación en materia de protección de datos de carácter personal en Ecuador es fundamental en la era digital actual, donde la recopilación, procesamiento y almacenamiento de información personal están cada vez más presentes en diversas actividades cotidianas. La principal ley que rige esta protección es la Ley Orgánica de Protección de Datos Personales (2020)

La LOPD (2020) establece una serie de principios que deben ser respetados en el tratamiento de datos, tales como el principio de consentimiento informado, que requiere que las personas den su consentimiento expreso y previo para que sus datos sean utilizados con fines específicos y legítimos. Además, la ley establece las obligaciones de los responsables y encargados del tratamiento de datos, quienes deben implementar medidas técnicas y organizativas adecuadas para garantizar la confidencialidad, integridad y disponibilidad de la información.

Para asegurar el cumplimiento efectivo de la LOPD (2020) y garantizar la protección de los derechos de los ciudadanos en cuanto a sus datos personales, se creó el Instituto de Datos Personales [IDP]. Este organismo es el encargado de supervisar y regular el tratamiento de datos personales por parte de instituciones públicas y privadas. Además, el IDP tiene la función de emitir guías, normativas y recomendaciones para promover buenas prácticas en el manejo de datos y brindar asesoramiento a los ciudadanos sobre sus derechos en relación con la protección de sus datos.

En Ecuador la Ley evoluciona constantemente para adaptarse a los avances tecnológicos y a las nuevas amenazas cibernéticas. La protección de datos de carácter personal se ha vuelto una prioridad para preservar la privacidad de los individuos y fortalecer la confianza en el uso responsable de la información en la sociedad digital. La colaboración entre el Estado, la sociedad civil y el sector privado es esencial para seguir avanzando en este ámbito y garantizar que los derechos fundamentales de los ciudadanos estén protegidos en el entorno digital en constante transformación.

En si la norma en materia de protección de datos de carácter personal en Ecuador es amplia y está compuesto por varias leyes y normativas que buscan garantizar la privacidad y seguridad de la información de los ciudadanos. A continuación, menciono algunas de las leyes y normativas más relevantes:

- Constitución de la República del Ecuador: En el artículo 66 de la Constitución se reconoce el derecho a la intimidad y a la protección de datos personales como un derecho fundamental de los ciudadanos.
- Ley Orgánica de Comunicación (LOC): Esta ley regula los derechos de comunicación y establece disposiciones sobre la protección de datos personales en el ámbito de los medios de comunicación.

- Ley Orgánica de Protección de Datos Personales (LOPD): Esta ley tiene como objetivo garantizar el ejercicio del derecho a la protección de datos personales y regula la recolección, procesamiento, uso y divulgación de la información personal.
- Ley Orgánica de Telecomunicaciones (LOT): En el artículo 94 de esta ley se establece la protección de datos personales en el ámbito de las telecomunicaciones.
- Código Orgánico Integral Penal (COIP): En el COIP se tipifican los delitos informáticos, incluyendo aquellos relacionados con la interceptación ilegal de datos y el acceso no autorizado a sistemas informáticos.
- Reglamento General a la Ley Orgánica de Protección de Datos Personales (RLOPD): Este reglamento desarrolla y complementa las disposiciones de la LOPD y establece las pautas para el cumplimiento de la ley.

Además de estas leyes y normativas, existen otras disposiciones legales y reglamentos específicos que regulan la protección de datos en sectores particulares, como el sector financiero, de salud, educativo, entre otros.

Es importante mencionar que el marco jurídico en materia de protección de datos está en constante evolución y adaptación a los cambios tecnológicos y sociales. El objetivo es fortalecer la protección de la información personal de los ciudadanos y garantizar su derecho a la privacidad en el entorno digital.

La protección de datos de carácter personal frente al delito de interceptación ilegal de datos es un tema crucial en la sociedad actual, donde la digitalización y la conectividad son cada vez más comunes. La recopilación y procesamiento de datos personales se ha vuelto una práctica habitual en diversos sectores, lo que ha generado preocupación sobre la seguridad y privacidad de la información.

La protección de datos de carácter personal es un desafío multidisciplinario que involucra a diversos actores, como el Estado, la sociedad civil, el sector privado y la comunidad

académica. La colaboración entre estos actores es esencial para desarrollar soluciones integrales y efectivas que garanticen la privacidad y seguridad de los datos en el entorno digital en constante cambio. Asimismo, la investigación y el desarrollo de nuevas tecnologías de protección de datos son fundamentales para fortalecer la seguridad y la confianza en el uso responsable de la información en la sociedad digital. Solo mediante un enfoque integral y colaborativo podremos enfrentar los desafíos y oportunidades que presenta la protección de datos de carácter personal en la actualidad.

2. El derecho a la intimidad y privacidad ante la protección de datos de carácter personal

En el contexto actual, los datos personales se han convertido en un recurso de gran valor para diversos actores, como empresas, gobiernos e instituciones. La recopilación masiva de información ha impulsado el desarrollo de tecnologías avanzadas, como el aprendizaje automático y la inteligencia artificial, que ofrecen beneficios significativos en diversos ámbitos. No obstante, este acceso a datos personales también ha suscitado preocupaciones en torno al uso inapropiado de la información y el potencial riesgo de vulnerar la privacidad de las personas.

Para afrontar estos desafíos, la protección de datos de carácter personal se ha convertido en una prioridad tanto para legisladores como reguladores a nivel mundial. En Ecuador, la Ley Orgánica de Protección de Datos Personales (2021) ha establecido principios y normas que garantizan el ejercicio de este derecho fundamental. La ley subraya la importancia de tratar los datos personales de manera lícita, equitativa y transparente, asegurando que solo se recopilen con el consentimiento del titular o en casos donde exista una base legal para su procesamiento.

A pesar de los esfuerzos implementados para proteger la privacidad de los ciudadanos, persisten desafíos en la efectiva implementación de la LOPD y en mantener una vigilancia constante frente a los avances tecnológicos. La creciente interconexión de dispositivos y

plataformas en línea ha creado nuevos riesgos de vulnerabilidad y exposición de datos personales. Los delitos informáticos, como el robo de información y el phishing, amenazan la seguridad de la información y la privacidad de los individuos.

En el ámbito social, sigue siendo relevante el debate sobre cómo encontrar un equilibrio adecuado entre el avance tecnológico y la protección de la intimidad. Mientras algunos argumentan que los beneficios de la recopilación y análisis de datos superan las preocupaciones sobre la privacidad, otros enfatizan la importancia de preservar la privacidad individual frente al uso indiscriminado de información personal.

De esta manera el problema científico también se relaciona con el equilibrio entre el avance tecnológico y la protección de la intimidad. Por un lado, el desarrollo de tecnologías como el aprendizaje automático y la inteligencia artificial ha llevado a la generación y análisis masivo de datos, lo que ha impulsado la innovación en diversos campos. Sin embargo, este progreso también ha abierto la puerta a un mayor acceso y uso de datos personales, lo que plantea interrogantes sobre cómo garantizar la privacidad individual en un mundo impulsado por la recopilación y análisis de información.

La globalización y la naturaleza transfronteriza del entorno digital también complican la protección de datos personales. La información puede ser compartida y almacenada en servidores ubicados en diferentes países, lo que dificulta la regulación y el control efectivo de cómo se utilizan y protegen esos datos en jurisdicciones extranjeras.

Asimismo, la falta de conciencia y educación sobre los riesgos cibernéticos entre los usuarios representa otro desafío. Muchas personas pueden no ser conscientes de la importancia de proteger su información personal o pueden caer en prácticas inseguras, como compartir contraseñas débiles o hacer clic en enlaces sospechosos, lo que aumenta el riesgo de ser víctimas de delitos cibernéticos.

La investigación científica en este campo debe abordar estos desafíos y buscar soluciones multidisciplinarias que involucren la tecnología, el derecho, la ética y la educación. Se necesitan estrategias efectivas de ciberseguridad que protejan la privacidad de los datos personales y al mismo tiempo permitan el uso responsable y beneficioso de la información en beneficio de la sociedad.

La colaboración entre gobiernos, organizaciones internacionales, empresas y la sociedad civil es esencial para abordar este problema de manera integral. Además, el establecimiento de estándares internacionales y marcos regulatorios sólidos que promuevan la protección de datos y la privacidad puede ser clave para enfrentar los desafíos actuales y futuros en el ámbito de la protección de datos de carácter personal dado que,

El tratamiento de datos personales por cuenta del responsable del archivo, registro, base o banco de datos. Toda operación de información que comprometa datos personales, en procedimiento mecánico o automatizado que tenga como fin la recolección, ordenamiento, conservación, almacenamiento, modificación, evaluación, destrucción, procesamiento de datos, así como el acceso de terceros por cualquier medio, deberá observar estrictamente la normativa prevista, bajo los derechos de protección y salvaguardia de identidad (Álvarez, 2017 p.9).

De esta manera el conflicto jurídico en torno a la protección de datos de carácter personal ante el delito de intercepción ilegal de datos es un desafío importante en la sociedad actual. Por un lado, el avance tecnológico ha permitido el uso masivo de datos para impulsar innovaciones significativas en diversas áreas. Sin embargo, esto también ha dado lugar a preocupaciones sobre la privacidad y la seguridad de la información personal.

El robo de datos y otros delitos cibernéticos amenazan la privacidad y la intimidad de las personas, lo que hace necesario establecer regulaciones sólidas y efectivas para proteger los

derechos individuales. La falta de una legislación adecuada y la implementación inadecuada de medidas de seguridad pueden exponer la información personal a riesgos innecesarios.

Además, surge un debate sobre qué bienes jurídicos deben ser protegidos en este contexto. Algunos argumentan que el software y otros activos digitales también deben ser considerados como bienes jurídicos protegidos, lo que ha generado discusiones en el ámbito jurídico.

Por ende, con la investigación se a logrado determinar que el conflicto jurídico en la protección de datos personales se centra en encontrar el equilibrio entre el avance tecnológico y la salvaguardia de los derechos fundamentales de privacidad e intimidad de las personas. Es esencial contar con regulaciones adecuadas y colaboración activa para abordar los desafíos de la ciberseguridad y proteger adecuadamente los datos en el mundo digital en constante cambio.

Metodología

Este trabajo se desarrolló mediante un paradigma cuantitativo en donde ‘‘el sujeto investigador aborda el objeto con neutralidad, busca las causas de los fenómenos sociales mediante la cuantificación y medición de variables, cuyo rigor científico viene dado por la validez y confiabilidad de los instrumentos que se aplican’’ (Finol y Vera, 2020, p. 7).

En cuanto a diseño de trabajó mediante un diseño de campo mismo que según Arias (2012) consiste en ‘‘la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes’’ (pág. 31).

Discusión de resultados

La Protección de datos de carácter personal frente al delito de interceptación ilegal de datos.

El derecho penal ha sido sugerido como uno de los sistemas para tratar el tema, pero su eficacia y suficiencia han suscitado discusiones y llevado a ideas adicionales.

Para sancionar y castigar a quienes vulneren la seguridad y privacidad de los datos personales, el derecho penal proporciona un marco legal sólido. Las sanciones penales, como las multas y el tiempo en la cárcel, pueden disuadir a los posibles infractores y ayudar a detener más delitos.

Además, el enfoque punitivo del derecho penal tiene como objetivo reparar el daño de las víctimas y castigar a los infractores. Esto puede aumentar la confianza en el sistema legal al dar a aquellos cuyos datos se han visto comprometidos un sentido de justicia y legitimidad.

Puede ser difícil atrapar a los delincuentes en línea. El carácter anónimo e internacional del ciberespacio dificulta la búsqueda y aprehensión de los responsables, lo que puede dificultar la aplicación de las sanciones previstas en el marco penal.

Argumentos a favor del Derecho Penal:

Como sistema de protección de datos personales, el derecho penal tiene una serie de beneficios. Las amenazas de sanciones penales pueden servir como elemento disuasorio para aquellos que intentan violar la seguridad y privacidad de la información personal. Las repercusiones legales graves pueden disuadir a los posibles delincuentes y disminuir la probabilidad de que se cometan delitos.

La justicia y la reparación son objetivos del enfoque punitivo del sistema de justicia penal, cuyo objetivo es responsabilizar a los violadores de la privacidad de las víctimas y reparar cualquier daño causado. Esto puede verse como una forma de justicia y ayudar a restablecer la confianza en el sistema legal. De la misma manera el derecho penal ofrece un

marco legal sólido para abordar los delitos relacionados con la protección de datos. Las leyes penales definen claramente el comportamiento prohibido y las sanciones asociadas.

Argumentos en contra del derecho penal.

A pesar de sus beneficios, el derecho penal tiene algunos inconvenientes cuando se trata de proteger la información personal tales como:

- Eficacia contra los delitos cibernéticos complejos: a medida que las herramientas y estrategias de los delincuentes digitales avanzan rápidamente, es un desafío para el derecho penal mantenerse al día con todos los problemas que surgen en el mundo en línea.
- Enfoque punitivo limitado: si bien el derecho penal se concentra en la sanción y el castigo de los delincuentes, no aborda de manera integral la prevención y la protección proactiva de los datos personales. Para abordar la protección de datos de manera más general, se necesitan enfoques complementarios.

La naturaleza anónima e internacional del ciberespacio dificulta localizar y llevar ante la justicia a los responsables de las filtraciones de datos. Muchos operan desde lugares aislados, lo que dificulta encontrarlos y detenerlos.

Puntos de vista alternativos.

Es necesario adoptar estrategias complementarias que aborden los problemas de manera integral para fortalecer la protección de datos personales.

- Educación y conciencia: las personas deben estar informadas sobre la seguridad digital para proteger activamente sus datos y tomar decisiones acertadas en el mundo digital.
- Regulación y Acciones Preventivas: Es crucial fortalecer las leyes de protección de datos y asegurar que se cumplan al pie de la letra. Para disminuir riesgos y vulnerabilidades se deben tomar medidas proactivas, como implementar protocolos de seguridad en empresas e instituciones.

La colaboración de los actores es necesaria para una protección eficaz de los datos personales entre empresas, gobiernos y el público en general. Para enfrentar los desafíos juntos, es esencial fomentar el intercambio de conocimientos y mejores prácticas.

No existe una respuesta clara a la pregunta de si el sistema de justicia penal es el mejor sistema para proteger la información personal. El derecho penal proporciona herramientas cruciales como la disuasión y la reparación, pero dada la complejidad del delito cibernético y el rápido avance de la tecnología, su eficacia puede verse limitada, para abordar la prevención, regulación y educación en seguridad digital, complementarios hay que tener en cuenta los enfoques. La protección efectiva de los datos personales en el entorno digital actual depende de la cooperación entre varios actores y la adopción de medidas preventivas. Encontrar un equilibrio entre el enfoque punitivo y las medidas más preventivas es difícil para abordar la protección de datos de manera completa y exitosa.

La interceptación ilegal de datos representa una amenaza seria para la privacidad de las personas. Los datos personales pueden ser objeto de robos y ser utilizados para cometer delitos como el fraude financiero, la suplantación de identidad o el espionaje. Estos delitos pueden tener consecuencias devastadoras para los individuos afectados, afectando tanto su seguridad financiera como su bienestar emocional.

Para hacer frente a estos desafíos, es esencial implementar medidas de protección sólidas. Esto incluye el establecimiento de políticas de seguridad efectivas en las organizaciones y empresas, el uso de técnicas avanzadas de encriptación de datos para salvaguardar la información sensible y la implementación de sistemas de detección de intrusiones para monitorear y prevenir cualquier intento de acceso no autorizado a los datos.

Además, la educación y concientización de los usuarios son aspectos clave en la protección de datos personales. La falta de conocimiento sobre las amenazas cibernéticas y las prácticas inseguras en línea pueden aumentar la vulnerabilidad de los individuos frente a los

delitos informáticos. Por lo tanto, es importante fomentar la formación en seguridad informática desde temprana edad y promover una cultura de protección de datos en la sociedad.

De esta manera la protección de datos de carácter personal frente al delito de interceptación ilegal es un desafío multifacético que requiere la participación activa y colaborativa de diversos actores.

Fortalecer el marco legal, implementar medidas técnicas de seguridad, educar a los usuarios y abordar los desafíos emergentes son pasos esenciales para garantizar la privacidad y seguridad de la información en el mundo digital en constante transformación. Solo a través de una combinación de esfuerzos y una comprensión integral de estos temas podremos proteger eficazmente los derechos fundamentales de los ciudadanos en el entorno digital actual

Conclusiones

1. la Protección de Datos de Carácter Personal frente al delito de interceptación ilegal de datos tiene como propósito fundamental resguardar la confidencialidad y la integridad de la información personal de los individuos, asegurando su derecho primordial a la salvaguarda de los datos personales. Esta meta involucra la implementación de marcos legales y reglas que no solo prevengan y penalicen la obtención no autorizada o ilegal de información personal, sino que también disuadan tales acciones. Este abarca la adquisición, acceso, revelación o empleo de información personal, tanto en formatos electrónicos como físicos, por parte de terceros sin el consentimiento del propietario de los datos. la protección de datos no solo es prevenir esta actividad ilícita, sino también proporcionar vías para que las personas afectadas puedan ejercer sus derechos y adoptar medidas legales cuando se vulnere su privacidad.

2. La ciberdelincuencia en Ecuador ha experimentado un preocupante aumento en los últimos años debido al crecimiento de la tecnología y la amplia disponibilidad de Internet. Esto ha abierto oportunidades para los delincuentes informáticos, quienes emplean tácticas cada vez más sofisticadas, como el phishing y el malware, para infiltrarse en sistemas y redes,

comprometiendo así la privacidad y seguridad de la información personal de los ciudadanos. Es fundamental que tanto el gobierno como el sector privado continúen trabajando en estrecha colaboración para fortalecer la seguridad digital en el país. Además, la concienciación y educación sobre seguridad en línea deben ser prioridades para empoderar a los usuarios y prevenir futuros ataques cibernéticos. La implementación de políticas y tecnologías de vanguardia será esencial para mantener un entorno digital seguro en un mundo tecnológico en constante evolución.

3. La intimidad, como bien jurídico protegido, cobra una relevancia crítica ante el delito de intercepción ilegal de datos. En un entorno digital donde la información personal es de alto valor, la privacidad de las personas se vuelve vulnerable. Es por ello que las leyes ecuatorianas han establecido medidas legales, como la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal, para salvaguardar la integridad y confidencialidad de los datos personales de los ciudadanos. Sin embargo, es importante reconocer que la ciberdelincuencia sigue evolucionando, y es fundamental mantener un enfoque proactivo en la protección de la intimidad y los datos personales. Esto implica una continua actualización de tecnologías y prácticas de seguridad, así como una colaboración activa entre las autoridades gubernamentales, el sector privado y la sociedad en general. La educación y la concienciación sobre la importancia de la protección de datos también juegan un papel clave para empoderar a los ciudadanos a tomar medidas preventivas y salvaguardar su privacidad en el mundo digital.

4. En el debate sobre la protección de datos personales y los derechos legales del software, no posee una relación clara con el desarrollo tecnológico y la salvaguardia de la privacidad. Si bien el software y la recopilación de datos son fundamentales para la innovación, también es esencial establecer regulaciones que protejan los derechos de propiedad intelectual y, al mismo tiempo, garanticen la seguridad y privacidad de la información personal. Una colaboración activa entre diversos actores permitirá evolucionar el marco jurídico y adaptarse

a los cambios tecnológicos y sociales, asegurando así una protección efectiva de los datos personales en la sociedad actual.

Conclusiones

Como resultado de los hallazgos de este estudio, es claro que, en Ecuador, donde la digitalización va en aumento, es crucial abordar la seguridad de los datos confidenciales, así como el delito de interceptación no autorizada de datos. Debido a que no existen suficientes protecciones para garantizar la seguridad y privacidad de los datos almacenados en la nube, se ha demostrado que la nación enfrenta serias amenazas en el mundo basado en Internet. La información personal de cada persona está en peligro, por lo que es urgente tomar acciones para garantizar un nivel de seguridad e inviolabilidad que fomente la confianza en el manejo de esta información sensible.

La investigación muestra que Ecuador, a pesar de tener leyes y protecciones, es insuperable en términos de protección de la privacidad y protección de datos en el entorno digital. Se han identificado áreas de mejora en la política y legislación de protección de datos con el objetivo de reforzar y actualizar las políticas existentes.

En el debate sobre la protección de datos personales y los derechos legales del software, no posee una relación clara con el desarrollo tecnológico y la salvaguardia de la privacidad. Si bien el software y la recopilación de datos son fundamentales para la innovación, también es esencial establecer regulaciones que protejan los derechos de propiedad intelectual y, al mismo tiempo, garanticen la seguridad y privacidad de la información personal. Una colaboración activa entre diversos actores permitirá evolucionar el marco jurídico y adaptarse a los cambios tecnológicos y sociales, asegurando así una protección efectiva de los datos personales en la sociedad actual.

Es fundamental que tanto el gobierno como el sector privado continúen trabajando en estrecha colaboración para fortalecer la seguridad digital en el país. Además, la concienciación y educación sobre seguridad en línea deben ser prioridades para empoderar a los usuarios y prevenir futuros ataques cibernéticos. La implementación de políticas y tecnologías de vanguardia será esencial para mantener un entorno digital seguro en un mundo tecnológico en constante evolución.

Estos resultados constituirán una base sólida para el desarrollo de propuestas concretas encaminadas a mejorar la protección de datos de los ciudadanos ecuatorianos. Recomienda enfoques efectivos e innovadores y fomenta la colaboración entre las partes interesadas del sector público y privado para lograr una mayor seguridad y privacidad en la seguridad digital. De esta manera es necesario fortalecer las leyes de protección de datos de Ecuador con miras a proteger mejor la privacidad y los derechos de protección de los ciudadanos en desarrollo.

El estudio destaca la importancia de establecer políticas y medidas efectivas para abordar este tema, que se perfila como un gran desafío en el actual entorno digital en materia de protección de datos personales. La necesidad de fortalecer y mejorar los mecanismos de protección de datos de Ecuador queda clara en los resultados y conclusiones alcanzados. Estas actualizaciones son necesarias para garantizar que la gestión de la información personal sea segura y confiable, promoviendo así un entorno en línea más confiable y seguro para los ciudadanos.

De la misma manera ayuda aumentar la conciencia sobre la importancia de implementar salvaguardas prácticas para garantizar la seguridad e inviolabilidad de la información personal en el entorno digital. La protección de datos personales es un tema de gran importancia en la sociedad actual. El desafío de preservar la privacidad individual en la esfera digital que cambia rápidamente solo puede superarse mediante la adopción de medidas adecuadas y la cooperación entre varios actores.

Referencias bibliográficas

Álvarez, L. (2017). Paradigmas de la protección de datos. Obtenido de https://repositorio.uasb.edu.ec/bitstream/10644/5945/1/05-TC-Enriquez.pdf

Codigo Orgánico Integral penal, COIP. (10 de febrero de 2014). Registro Oficial. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Finol, M. y Vera, J. (2020). Paradigmas, enfoques y métodos de investigación: análisis teórico. Revista científica Mundo Recursivo, 3(1), 1-24. Recuperado de https://www.atlantic.edu.ec/ojs/index.php/mundor/article/view/38

Ley Orgánica de proteccion de Datos Personales. (21 de mayo de 2021). Registro Oficial. LEXIS S.A.

Ley Organica de Protección de Datos Personales. (26 de mayo de 2021). Ley organica de protección de datos Personales. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Mayer, L. (2017). El Bien Jurídico Protegido En Los Delitos. Obtenido de https://www.scielo.cl/pdf/rchilder/v44n1/art11.pdf

Obregón, L., Gomez, E., & López, G. (2017). Delitos a través redes sociales en el Ecuador. I+D Tecnológico.

Oficina de Drogas y Crimen de las Naciones Unidas. (2022, 13 de abril). Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). https://www.unodc.org/

Pazmiño, S. (agosto de 2017). Factores que contribuyen y efectos que emergen de la caducidad de los procesos judiciales del tipo penal "interceptación ilegal de datos". Obtenido de https://repositorio.iaen.edu.ec/bitstream/handle/24000/6398/ARTICULO%20CIENT%c3%8cFICO%20%20FACTORES%20QUE%20CONTRIBUYEN%20Y%20EFECTOS%20QUE%20EMERGEN%20DE%20LA%20CADUCIDAD%20DE%20LOS%20PROCES.pdf?sequence=1&isAllowed=y

Pérez, C. (2013). ¿Qué delito es el Happy Slapping? Obtenido de file:///C:/Users/User/Downloads/Dialnet-QueDelitoEsElHappySlapping-4219693%20(1).pdf

Porcelli, A. (2019). La Protección De Los Datos Personales En El Entorno Digital. Obtenido de file:///C:/Users/User/Downloads/40175-164123-1-PB.pdf

Segarra, E., & Ramírez , M. (2011). Derecho a la intimidad. Análisis a la normativa ecuatoriana. Cuenca, Azuay, Ecuador: UNIVERSIDAD DEL AZUAY 50 AÑOS.