ARTICULO ORIGINAL

Derecho a la intimidad y la ciberdelincuencia. Efectos sociales y económicos en víctimas ecuatorianas

The right to privacy and cybercrime. Social and economic effects on Ecuadorian victims

Recibido: 30/09/2022
Aceptado: 20/11/2022
Publicado: 31/12/2022

Washington Manuel Salvador Quiñonez
https://orcid.org/0009-0006-5927-9730
Investigador Independiente
Ab.wsalvador@hotmail.com

Magister en Derecho Constitucional. Diplomado Internacional en Ciberdelitos. Diplomado Internacional en Seguridad Ciudadana. Abogado de los tribunales y juzgados de la República del Ecuador. Subgerente de Seguridad Integral Banco Guayaquil.

Resumen

Desde la llegada de la pandemia COVID-19, y debido al confinamiento y aislamiento social, se ha incrementado la vulneración del derecho a la intimidad mediante los ciberdelitos cometidos en Ecuador. Esta investigación, describe el derecho a la intimidad y la ciberdelincuencia, así como sus efectos sociales y económicos en las víctimas ecuatorianas. El presente estudio tiene un enfoque cuantitativo de diseño no experimental, siendo su nivel descriptivo–analítico y de carácter longitudinal, por cuanto se efectúa un estudio de la evolución y comportamiento de los delitos cibernéticos desde el año 2017 hasta el 2021, haciendo un especial énfasis en el año 2020. Por otra parte, las técnicas de investigación utilizadas fueron documentales, a partir de la teoría de autores citados en relación con la vulneración del derecho a la intimidad a través de ciberdelitos, así como también, del análisis estadístico de los delitos informáticos cometidos en el Ecuador, suministrado por el Sistema integrado de Actuaciones Fiscales. Los resultados muestran cuáles fueron los ciberdelitos cometidos en Ecuador que vulneraron el derecho a la intimidad de las personas durante la pandemia; concluyéndose que, de los delitos informáticos mencionados en el Código Orgánico Integral Penal, los de mayor frecuencia fueron la violación a la intimidad y la estafa. Por su parte, dentro de los ciberdelitos cometidos en Ecuador que vulneraron el derecho a la intimidad de las personas antes y durante la pandemia, se encuentran la suplantación de identidad; la falsificación y uso de documentos falsos; la apropiación fraudulenta por medios electrónicos; y el acceso no consentido a un sistema informático; lo que afectó de manera negativa el patrimonio de las víctimas.

Palabras clave: Derecho a la intimidad, Ciberdelitos, Estafas electrónicas, COVID-19.

Abstract

Since the arrival of the COVID-19 pandemic, and due to confinement and social isolation, the violation of the right to privacy has increased through cybercrimes committed in Ecuador. This research describes the right to privacy and cybercrime, as well as their social and economic effects on Ecuadorian victims. The present study has a quantitative approach of non-experimental design, being its descriptive-analytical and longitudinal level, since a study of the evolution and behavior of cyber crimes from 2017 to 2021 is carried out, with a special emphasis on the year 2020. On the other hand, the investigation techniques used were documentary, based on the theory of the authors cited in relation to the violation of the right to privacy through cybercrimes, as well as the statistical analysis of computer crimes committed in Ecuador, provided by the Integrated System of Fiscal Actions. The results show which cybercrimes were committed in Ecuador that violated people's right to privacy during the pandemic; it was concluded that, of the computer crimes mentioned in the Integral Organic Criminal Code, the most frequent were the violation of privacy and fraud. On the other hand, among the cybercrimes committed in Ecuador that violated people's right to privacy before and during the pandemic, there are identity theft; the falsification and use of false documents; fraudulent appropriation by electronic means; and non-consensual access to a computer system; which negatively affected the property of the victims.

Key words: Right to privacy, Cybercrimes, Electronic scams, COVID-19.

Introducción

La presencia de la internet y la diversidad de sistemas informáticos, ha supuesto un antes y un después en la manera cómo las personas tienen acceso a los sistemas de información y comunicación, en los que cada acción se ve reflejada, ya que la red es un nuevo espacio en el que los roles y funciones de los diferentes agentes se construyen, evolucionan y cambian cada día (Alonso-García, 2015). Uno de esos cambios tiene que ver con comportamientos delictivos asociados a estos nuevos paradigmas e instrumentos cibernéticos. Por lo tanto, con el crecimiento de las redes informáticas, los llamados ciberdelincuentes también avanzan, proponiendo técnicas y métodos eficaces para vulnerar los sistemas de seguridad y encontrar víctimas fáciles.

En la actualidad, el avance de la tecnología a nivel global ha hecho que el hombre tenga mejores herramientas que le hagan la vida más fácil, es decir, que muchas situaciones que años atrás parecían complejas hoy en día se hagan con el clic a un ordenador. Sin embargo, el desarrollo de la tecnología también se ha prestado para que estas nuevas plataformas tecnológicas sean usadas de manera negativa o con fines delictuales, ello ha hecho que nazca una nueva tipología de delitos los cuales se conocen como ciberdelitos (Aboso, 2017).

Según Antúnez (2020), con el comienzo de la pandemia de COVID-19 y con el inicio del confinamiento a partir del mes de marzo del año 2020, los delitos más concurrentes fueron las estafas digitales con modalidad de suplantación de identidad y la apropiación fraudulenta a través de medios electrónicos, es decir, se puede evidenciar que fue vulnerado el derecho a la intimidad de los ciudadanos ecuatorianos. En el presente artículo se pretende demostrar mediante un análisis cuantitativo, el aumento de los delitos informáticos en el Ecuador durante la pandemia.

El problema que se plantea en la presente investigación, radica en el hecho que, a partir de la pandemia COVID-19, cuando en el Ecuador se ordenó el confinamiento de la población para evitar los contagios (Diario El Universo 2020), se vieron afectados todos los niveles de la sociedad, desde los más productivos hasta los medios y bajos (Accenture 2023), incluso personas que habitualmente se ganaban la vida honradamente, así como aquellos que lo hacían de forma ilegal a través de delitos económicos, estafas, robos, hurtos, entre otros (López, 2020).

Ahora bien, ante tal situación muchos delincuentes buscaron alternativas que les permitieren seguir delinquiendo, esta vez desde sus domicilios, ya que les estaba prohibido salir de ellos, en consecuencia, la única vía que tenían era la web, y, tomando en consideración que todas las personas estaban en sus hogares, comenzaron a utilizar esta forma. Por lo tanto, iniciaron promocionando elementos esenciales para la pandemia como mascarillas, alcohol y algunas medicinas, ofertándolos vía web, situación que hacía que muchas personas, ante la necesidad,

efectuaran el pago vía transferencia o tarjeta de crédito o débito, los cuales resultaban en estafas, un tipo de ciberdelito (López, 2020).

Esta situación no se quedó en simples estafas, sino que evolucionó a tal punto que muchos delincuentes optaron por la vía digital y cibernética y comenzaron a operar por la web, trayendo como consecuencia un aumento en el número de delitos cometidos, así como también, la vulneración de la intimidad de las víctimas, por cuanto uno de los modus operandi que utilizaban los delincuentes era solicitar el correo electrónico de la víctima, enviándole cualquier tipo de información, de tal manera que al abrir el correo se liberaba un virus para sustraer información confidencial, vulnerando así su derecho a la intimidad (Antúnez 2020).

Por todo lo señalado anteriormente, en el presente artículo, se abordará cómo los ciberdelitos constituyen una forma directa de vulneración al derecho de intimidad de las personas, por lo que se requieren políticas públicas de seguridad a los efectos de disminuir de manera progresiva este tipo de delitos los cuales, en el año 2020, producto del confinamiento derivado de la pandemia, experimentaron un pico máximo, llegando a reportarse 2.108 denuncias por estos delitos (Ecuador News, 2020).

Por lo antes mencionado, el presente artículo científico, pretende demostrar cómo, a propósito del confinamiento debido a la pandemia del COVID-19, surge la necesidad de utilizar con mayor frecuencia la red informática, trayendo como consecuencia que, ante la imposibilidad de efectuar estafas tradicionales, se utilizó la internet a los fines de efectuar estafas digitales. En este punto, hay que señalar que los delitos informáticos han ido aumentando de forma progresiva en el Ecuador tal como se ha evidenciado de las denuncias presentadas en Fiscalía, ya que de acuerdo a las estadísticas emanadas del Sistema integrado de Actuaciones Fiscales (SIAF), en el año 2018 hubo 11.250 estafas informáticas, en el año 2019, 12.047 y para el año 2020 18.950.

En otro orden de ideas, desde el punto de vista metodológico, el presente estudio tiene un enfoque cuantitativo de diseño no experimental, siendo su nivel descriptivo-analítico. La investigación tiene un carácter longitudinal por cuanto se efectúa un estudio de la evolución y comportamiento de los delitos cibernéticos desde el año 2017 hasta el 2021, haciendo un especial énfasis en el año 2020. Por otra parte, las técnicas de investigación utilizadas fueron documentales, a partir de la teoría de autores citados en relación con la vulneración del derecho a la intimidad en los ciberdelitos, así como también, del análisis estadístico de los delitos informáticos cometidos en el Ecuador, suministrado por el Sistema integrado de Actuaciones Fiscales.

El derecho a la intimidad

La intimidad es un concepto de única pertenencia al ser humano, por lo que ningún individuo tiene derecho sobre la intimidad de otro. No obstante, el derecho a la intimidad no es absoluto puesto que encuentra ciertos límites en el momento que empieza el derecho del otro individuo. En resumen, la intimidad es un derecho que

protege la esencia más íntima y personal de un ser humano, reservada, secreta y fundamental. (Alvarado, 2018)

El derecho a la intimidad se menciona en el numeral 20 del Artículo 66 de la Constitución de la República del Ecuador, al decir, el cual reconoce y garantiza a las personas el derecho a la intimidad personal y familiar. También hace referencia a este derecho el Código Orgánico Integral Penal, el cual en su artículo 178 que tipifica el delito de violación a la intimidad. Adicionalmente, la Declaración Mundial de los Derechos Humanos (1948), en el artículo 12 menciona que nadie será objeto de injerencias arbitrarias en la vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o a su reputación y que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

La intimidad es el derecho personal que protege la reserva espiritual de la vida del ser humano, asegurando su libre desenvolvimiento en lo que respecta a lo personal, sus expresiones y afectos (Zavala, 1982). Es uno de los derechos más importantes del ser humano, ya que gracias a él una persona puede excluir del conocimiento público ciertos aspectos que considera privados, y que solamente le conciernen a él o a su grupo familiar. Tal derecho, es la facultad que posee todo individuo de compartir o no elementos que forman parte de su vida privada, en consecuencia, va a depender de toda persona qué elementos de ella quiere compartir con el resto de la sociedad. (Zavala, 2018).

En la actualidad, este derecho no es tan absoluto como lo era décadas atrás, ya que la existencia de redes sociales, del internet y la utilización de drones, ha hecho que cada día más las personas se encuentran expuestas a la sociedad, sin embargo, ello no basta para que una persona decida sobre qué o cuáles aspectos de su vida pueda excluir del conocimiento público. Por tal motivo, en el ejercicio de este derecho una persona puede determinar qué aspectos de su vida pueden ser conocidos por la sociedad, y cuáles no, en consecuencia, si un tercero vulnera este derecho, el sujeto activo podrá ejercer acciones legales en su contra.

El derecho a la intimidad es bastante amplio, ya que él no se encuentra dirigido a un aspecto especifico de la vida privada de una persona, sino a su familia, así como también, a cualquier aspecto que una persona desee excluir del conocimiento de la colectividad. Está formado por los sentimientos, opiniones, gustos, hábitos y costumbres; las relaciones filiales; la situación patrimonial; alguna enfermedad que presente la persona o allegados a su núcleo familiar como cónyuge e hijos; algún hecho del pasado que pueda traer una situación vergonzosa o exposición al rechazo público; entre otros (Morales, 2018).

La vida privada está formada por hechos que el titular de este derecho decide excluir del conocimiento de terceros, pero también forma parte de este sus datos personales, como su identificación, datos financieros, claves bancarias, contraseñas de correos electrónicos, entre otros; y la exposición de ellos a terceros traería consecuencias

perjudiciales a sus titulares. De acuerdo a lo mencionado, el realizar cualquier tipo de actos que atenten contra la seguridad de los documentos privados de una persona constituye de una manera directa la vulneración al derecho de la intimidad (Perarales, 2018).

En síntesis, la vida privada de toda persona se encuentra formada por un conjunto de situaciones que la propia persona decide excluir del conocimiento público o por una decisión netamente personal; basta que ella decida qué información será o no del dominio público. Así pues, quedarían apartados de la vida privada de una persona aquellos hechos o informaciones que ya fuesen de manejo público.

La ciberdelincuencia: conceptualizaciones y tipologías

El espacio cibernético, o ciberespacio, puede describirse como un tipo de dominio artificial edificado por el hombre y que se diferencia de los otros cuatros dominios de guerra, a saber: la tierra, el aire, el mar y el espacio; aunque tiene su formalización en fechas recientes, el ciberespacio puede afectar a las actividades en los otros dominios. Además de ello, el ciberespacio está fuertemente vinculado y apoyado por medios físicos, como las redes eléctricas. Si esta interconexión es atacada, puede tener graves consecuencias sobre las políticas de seguridad existentes. (Curtis, 2011).

A partir del desarrollo de la internet, surgen nuevos términos como cibercrimen, ciberdelito o ciberdelincuencia, los cuales abarcan aspectos ilícitos cometidos en el ciberespacio, cuyas características específicas son: se cometen fácilmente; requieren pocos recursos comparados al daño que causan; pueden ser cometidos en una jurisdicción sin necesariamente estar de forma física presentes; y están favorecidos por lagunas de punibilidad que existen en determinados Estados, llamados paraísos cibernéticos, por su nula voluntad política de ser sancionados (Subijana, 2008).

Los ciberdelitos son considerados como aquellas actividades delictivas que se efectúan a través de medios tecnológicos como un pc, una laptop, un dispositivo móvil o internet. Anteriormente era común efectuar cualquier tipo de estafa o engaño en una actuación comercial, pero para ello se necesitaba generalmente la presencia física de dos o más personas; en la actualidad para hacer un negocio o cometer una estafa informática, basta que se realice una operación comercial mediante internet y un dispositivo tecnológico, con la agravante que, en la mayoría de estos casos, no se tiene conocimiento de la persona con quien se está tratando.

Otro de los problemas que se presenta con el avance de las nuevas tecnologías y formas delictivas, es la obtención mediante virus de datos financieros de las personas, con el fin de posteriormente causar un daño patrimonial a favor de un tercero. En este sentido muchas personas son víctimas de ciberdelitos y solamente se enteran al revisar sus estados financieros y, en la mayoría de los casos, ya es demasiado tarde. La forma como operan este tipo de delitos es bastante sencilla, se le envía un correo electrónico a la víctima que al abrirlo libera un programa que copia toda la información,

con la intención de sustraer las claves bancarias para disponer de los fondos de la víctima (Gomez, 2019).

Los ciberdelitos son actividades que con el paso del tiempo se han ido perfeccionando, al punto que es más difícil para las autoridades la aprensión de los delincuentes, ya que a diferencia de los delitos comunes los cuales siempre dejan rastros, testigos o evidencias, los ciberdelitos se producen en la red y en muchas oportunidades nunca se ha tenido contacto con el delincuente ya que se accede o se tiene contacto a él solo por medios digitales como redes sociales o correos electrónicos.

Teniendo clara la conceptualización de ciberdelincuencia, existen diferentes tipos de delitos que han vulnerado de una u otra manera el derecho a la intimidad de las personas. Antúnez (2020), hace mención de los siguientes:

Estafa Online y Phishing: Realizada con mensajes de textos y correos electrónicos de fuentes de confianza como autoridades sanitarias, cuerpos de seguridad del Estado, establecimientos y comercios, bancos, compañías eléctricas, entre otros, que remiten información adjuntando un link en el que se deben rellenar datos imprescindibles, según el mensaje recibido; siendo en su mayoría mensajes falsos buscando con esto obtener datos personales o bancarios.

Bulos Y Fake News: Representa uno de los métodos de ingeniería social más utilizado por los ciberdelincuentes, en el que se implantan alarmas generales que provoquen caos, del cual obtendrán beneficios para ejecutar cualquier técnica de hackeo, robo de identificaciones, instigación al odio, fraudes o estafas financieras.

Malware y Apps Maliciosas: Utilizados comúnmente durante la pandemia de COVID-19 para sustraer datos confidenciales con fines lucrativos o de comercio. Las pequeñas y medianas empresas son consideradas las más desprotegidas ante este escenario, en virtud que el teletrabajo es un instrumento de doble filo para los maléficos de la red.

Ciberacoso: Es conocido como acoso virtual, en el que se usan medios digitales para molestar o acosar a una persona mediante ataques personales, divulgación de información personal o falsa entre otros medios. Pueden producirse chantajes, ofensas, campañas de resentimiento y permanentes secuencias de discusión con faltas de respeto implícitas sobre contenidos de opinión.

Además de los Ciberdelitos antes mencionados, Antúnez (2020) establece otra tipología de delitos que vulneran los derechos de intimidad y que atentan contra la integridad de las personas, estos son:

Incitación al odio: Tiene que ver con información en las redes sociales que no solo se utiliza para dañar la imagen de alguien, sino que van más allá, pues fomenta, promueve o incita al odio, hostilidad, discriminación o violencia, ya sea contra una persona o incluso contra todo un colectivo.

Injurias y Calumnias: Las calumnias se recogen dentro del capítulo de los delitos contra el honor y constituyen expresiones que tienen como fin perjudicar la honorabilidad de instituciones, grupos o individuos. La calumnia es la imputación de un delito hecha con conocimiento de su falsedad o con un temerario desprecio de la verdad, es decir, afirmar que se ha cometido un delito apuntando a alguien en concreto sabiendo que no es así, con el fin de desprestigiar o provocar un daño mayor. Por su parte, las injurias, se consideran expresiones ejecutadas en deshonra, descrédito o menosprecio de otra persona, atentando contra su reputación o contra su propia estima.

Delito de desórdenes públicos: Rebelión o altercados que alteran la paz pública cometidos al crear historias falsas en la red que pueden ser castigadas. Este podría ser el caso de quien, difundiendo información falsa, intente alterar la paz pública e incite a una manifestación masiva en contra de determinadas personas, autoridades o instituciones.

Falsas alertas de seguridad: Delito asociado a la simulación de un escenario de peligro para generar temor y alarmar a la sociedad, en el que se moviliza a los servicios de emergencia o a la policía.

Ciberacoso: Es el uso de redes sociales para molestar o acosar a una persona o grupo de personas, mediante ataques personales, divulgación de información confidencial o falsa entre otros medios.

Grooming: Son conductas y acciones emprendidas por un adulto, a través de Internet, con el objetivo deliberado de ganarse la amistad de un menor de edad, creando una conexión emocional con el mismo, con el fin de abusar sexualmente de él.

Sexting: implica la recepción o transmisión de imágenes o videos de contenido sexual a través de las redes sociales, ya sea con o sin autorización de quien lo envía primero.

Formas más comunes de ciberdelitos económicos

Los ciberdelitos tienen su razón de ser en el hecho de causar cierto daño patrimonial a un tercero; las personas que se dedican a este tipo de actividades anteriormente efectuaban estafas tradicionales o de igual manera se dedicaban a delinquir; pero muchas de ellas a consecuencia de la pandemia por COVID-19 se han visto en la obligación de migrar al mundo digital ya que producto de muchas restricciones gran parte de los negocios se efectúan por medios digitales.

En la actualidad el comercio electrónico ha crecido a niveles exponenciales, gran parte de los bienes que se adquieren se hacen por páginas web y mucho más a raíz de las medidas implantadas a consecuencia de la pandemia, trayendo como consecuencia que se oferten productos inexistentes que luego de pagarlos, resultan ser totalmente diferentes a lo que el comprador esperaba o, en peores casos, nunca llega el producto.

Todo delito electrónico ya ha sido preparado de forma previa por parte del autor del hecho punible. En la actualidad son muchas las vías electrónicas que se utilizan para

este tipo de delitos, una de las formas más comunes de cometerlo es mediante el phishing el cual constituye en la actualidad un tipo de estafa electrónica usual; su función consiste en conseguir datos básicos del usuario víctima, principalmente datos bancarios como contraseñas de tarjetas de débito o crédito, a fin de poder sustraer cantidades de dinero de la víctima. Actualmente se constituye como uno de los ciberdelitos más utilizados (Gomez, 2019).

El interés en la comisión de este tipo de delitos, siempre es la afectación económica de la víctima en provecho del delincuente o de un tercero, que puede ser una persona natural o jurídica, esta actividad es tan usual que en el mercado negro de la informática se venden kits para defraudar, es decir, virus que sustraen la información de un pc para poder visualizar toda la información de la víctima, siendo la más importante los datos económicos (Antúnez 2020).

Otra forma común de comisión de ciberdelitos es la clonación de tarjetas de crédito, situación que ocurre de dos maneras: la primera cuando de forma presencial la víctima en un local físico entrega su tarjeta de crédito para pagar por un producto o servicio y la misma es cambiada con el fin de obtener los datos del tarjetahabiente; la segunda cuando, al hacer un pago electrónico, es obligatorio suministrar los datos de pago de la tarjeta para procesar el pago y en ese momento se sustraen las contraseñas para posteriormente efectuar transacciones en nombre de la víctima (Antúnez 2020).

Otro tipo es la estafa nigeriana, la cual se lleva a cabo principalmente vía correo electrónico no deseado o spam (Rosenberg, 2007). Su modus operandi consiste en que el delincuente hace ver a la víctima que es una persona que posee muchos recursos económicos pero que sus cuentas están bloqueadas y que, por tal razón, no puede disponer de sus recursos económicos, pero que con su ayuda lo puede hacer, a cambio de pagarle un porcentaje del dinero recuperado.

El proceso de sustracción de los fondos de la víctima ocurre ya que el estafador pide a la víctima sus datos y contraseñas bancarias ya que se efectuarán unas deducciones mínimas por la prestación del servicio bancario, y es en el momento del delincuente poseer la información bancaria cuando se efectúa el vacío de las cuentas de la víctima. Este tipo se puede ejecutar desde cualquier país indistintamente del motivo de enriquecimiento por el cual se engañe, por tal motivo se recomienda a las personas en general poseer antivirus actualizados en sus computadores, así como también no abrir correos de remitentes desconocidos (Morales, 2018).

Resultados

En el presente apartado se procede a realizar el análisis de los resultados, el cual se centra en los delitos informáticos mencionados en el Código Orgánico Integral Penal más frecuentes, durante el periodo 2017-2021, basados en la cantidad de denuncias a nivel nacional; además de ello, el análisis explica los tipos de delitos presentes en Ecuador que violan el derecho a la intimidad, en el mismo período de estudio. Los

datos han sido tomados del Sistema Integrado de Actuaciones Fiscales de Ecuador, para lo cual se han construido las *Tablas 1 y 2*.

Tabla 1. Delitos informáticos COIP con mayor frecuencia durante los años 2017-2021

	Año 2017	*Año 2018*	*Año 2019*	*Año 2020*	*Año 2021*
COIP Art. 178 violación a la intimidad 1-3 años	1.666	2.069	2.044	3.780	1.830
COIP Art. 186- Estafa 5 - 7 años	14.057	14.448	17.221	21.328	14.328
COIP art. 230 Interceptación ilegal de datos 3 - 5 años	63	41	57	165	52
COIP art. 232 Ataque a la integridad de sistemas informáticos 3-5 años	86	87	92	215	105
COIP art 234 Acceso no consentido a un sistema informático, telemático o de telecomunicaciones 3-5 años	218	236	245	403	260

Fuente: Sistema integrado de Actuaciones Fiscales (2021)

La *Tabla 1* muestra los delitos informáticos mencionados en el Código Orgánico Integral Penal que han tenido un mayor impacto y una mayor frecuencia durante los años 2017-2021 en Ecuador, tomando como base la cantidad de denuncias a nivel nacional, de lo cual se puede evidenciar que el confinamiento producto de la pandemia COVID-19 que inició a finales del año 2019, refleja un aumento en los delitos informáticos en los años 2020 y 2021; por cuanto muy pocas personas salían de sus casas, situación que hizo que muchos delincuentes utilizaran la vía informática para cometer hechos ilícitos.

La estadística anterior demuestra cómo aumentaron los delitos informáticos en el año 2020 ya que se registraron 25.891 casos, a diferencia de los años anteriores donde se registraron 19.659 casos en el año 2019; 16.881 en el 2018; y 16.090 en el 2017. Pese a lo anterior, en el año 2021 se fueron recobrando las estadísticas habituales que se habían presentado en los años 2017, 2018 y 2019 registrando un promedio de 16.575 casos.

Cabe recalcar que, entre los delitos informáticos que registran mayor frecuencia, se encuentran la violación a la intimidad y la Estafa; alcanzando un promedio de 2.277,8 y de 16.276,4, respectivamente, durante los cinco años de estudio. Ahora bien, se muestra en último lugar la interceptación ilegal de datos, con un promedio de 75,6

casos en el período 2017-2021; todos ellos teniendo como punto común, un incremento en el año 2020, producto de la llegada de la pandemia.

Tabla 2. Delitos informáticos en el Ecuador años 2017-2021

Tipos de delitos	*Año 2017*	*Año 2018*	*Año 2019*	*Año 2020*	*Año 2021*
Suplantación de identidad	3376	3467	3385	4657	3260
Falsificación y uso de documento falso	3183	3348	3379	4265	3280
Apropiación fraudulenta por medios electrónicos	960	1250	1350	2315	1760
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	218	255	248	350	297
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	163	172	185	315	220
Ataque a la integridad de sistemas informáticos	86	95	79	215	122
Interceptación ilegal de datos	63	88	94	207	115
Transferencia electrónica de activo patrimonial	75	95	110	357	123
Revelación ilegal de bases de datos	33	42	53	212	83

Fuente: Sistema integrado de Actuaciones Fiscales (2021)

La *Tabla 2* es más amplia, comparada con la Tabla anterior, por cuanto evidencia los delitos informáticos específicos, que, al igual que los más cometidos citados anteriormente, se pudo demostrar cómo en el año 2020 existió un aumento bastante considerable en todos los delitos informáticos, ya que era la vía ideal que utilizaban los delincuentes para cometer hechos ilícitos. En ese año hubo una importante migración de la delincuencia en general hacia los delitos informáticos, ya que tradicionalmente siempre habían existido, pero en el año 2020 hubo un aumento bastante considerable; inclusive analizando las estadísticas del año 2021 se observa cómo ya se retoman las estadísticas habituales de años anteriores a la pandemia.

La *Taba 2* muestra claramente que los delitos más comunes en Ecuador, antes y durante la pandemia, fueron: la suplantación de identidad; la falsificación y uso de documentos falsos; la apropiación fraudulenta por medios electrónicos; y el acceso no consentido a un sistema informático, telemático o de telecomunicaciones; quedando en los últimos lugares la interceptación ilegal de datos y la revelación ilegal de bases de datos.

Discusión de los resultados

En las décadas más recientes, se ha evidenciado en Ecuador un tipo de delitos que hace años atrás no se conocía o apenas se nombraba; y que hoy es conocido como ciberdelitos. Sobre ellos, Subijana (2008) menciona que es gracias al desarrollo de la internet, que han ido apareciendo, y abarcan aspectos ilícitos cometidos en el ciberespacio. Adicional a ello, Aboso, (2017) explica que el desarrollo de la tecnología se ha prestado también para que las nuevas plataformas tecnológicas sean usadas de manera negativa o con fines delictuales, dando origen a los ciberdelitos (Aboso, 2017).

Muchos delincuentes prefieren este tipo de delitos por cuanto consideran que en la actualidad les reportan excelentes resultados, sin tanto esfuerzo, y con poca inversión de tiempo y dinero. Al respecto, Subijana (2008) menciona que los ciberdelitos tienen características específicas como: se cometen fácilmente; requieren pocos recursos comparados al daño que causan; pueden darse en una jurisdicción sin necesariamente estar de forma física presentes; y están favorecidos por lagunas de punibilidad que existen en determinados Estados.

Las oportunidades para estos delincuentes se abrieron más aún con la llegada de la pandemia, ya que según el análisis de los resultados presentados en esta investigación se evidencia que el número de casos y denuncias se incrementó en el tiempo de confinamiento y distanciamiento social obligatorio, por lo que se infiere que, debido al mayor uso de medios tecnológicos, los ciberdelitos se intensificaron a mayor escala. Esta situación concuerda con lo expresado por López (2020), quien menciona que, ante la pandemia, muchos delincuentes buscaron alternativas que le permitieren seguir delinquiendo, esta vez desde sus domicilios. Comenzaron inicialmente promocionando vía web productos necesarios de protección; ante la necesidad, muchas personas efectuaron pagos electrónicos, los cuales resultaron en estafas.

El estudio también arrojó que los delitos más comunes en Ecuador durante el periodo pandémico, fueron la suplantación de identidad; la falsificación y uso de documentos falsos; la apropiación fraudulenta por medios electrónicos; y el acceso no consentido a un sistema informático, telemático o de telecomunicaciones; situación que concuerda con lo expresado por Antúnez (2020), al decir que, con el inicio del confinamiento, los delitos más concurrentes fueron las estafas digitales con modalidad de suplantación de identidad y la apropiación fraudulenta a través de medios electrónicos.

Independientemente del tipo de ciberdelito, lo anterior muestra una violación del derecho a la intimidad de los ciudadanos ecuatorianos, un derecho que, de acuerdo con Zavala (2018), representa uno de los más importantes del ser humano, ya que gracias a él la persona puede excluir del conocimiento público ciertos aspectos que considera privados, y que solamente le conciernen a él o a su grupo familiar. Tal derecho, es la facultad que posee todo individuo de compartir o no elementos que

forman parte de su vida privada, en consecuencia, va a depender de toda persona qué elementos de ella quiere compartir con el resto de la sociedad.

Sobre este derecho, la Constitución de la República del Ecuador (2008), reconoce su importancia y garantiza a los individuos ecuatorianos el derecho a la intimidad personal y familiar. Este es un derecho que, al ser violado, debe ser castigado y penalizado, haciendo valer y honrar la intimidadde cada persona. Sobre ello, la Declaración Mundial de los Derechos Humanos (1948), menciona que nadie debe ser objeto de injerencias arbitrarias en la vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o a su reputación y que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

En referencia a lo anterior, es importante mencionar que en la actualidad a pesar de que existen leyes y normas establecidas, y se ha dado a conocer explícitamente las sanciones y castigos que deben imponerse a los delincuentes, los delitos no cesan y cada vez es mayor el número de ciberdelitos que se cometen en Ecuador, aumentando así lo casos de vulneración de derechos a los ciudadanos, principalmente aquellos que, por ciertas circunstancias, se ven en la necesidad de utilizar frecuentemente medios electrónicos.

De modo que, se infiere que se presta poca atención al castigo que pudiera recibir un ciberdelincuente; de hecho, algunas fuentes documentales relacionadas con ciberdelitos, han dado a conocer casos no procesados de este tipo de delitos que luego se siguen cometiendo a mayor escala; a pesar de que el Código Orgánico Integral Penal establece el castigo de cualquier transgresión a la esfera íntima del ser humano. Por esta razón, es necesaria la existencia de una mayor rigurosidad en la aplicación de las normas establecidas sobre derechos a la intimidad y de castigos establecidos en el código que los rige.

Conclusiones

El derecho a la intimidad es inherente a todo ser humano, por cuanto implica la facultad que tiene una persona de reservar para sí y excluir del conocimiento público de terceros, ciertos aspectos personales que a su criterio no deben ser revelados. Este derecho es bastante amplio ya que lleva dentro de sí elementos personales que, de acuerdo a su naturaleza, deben mantenerse en secreto.

El derecho a la intimidad por lo general se da en el ámbito económico y patrimonial. Muchos delincuentes utilizan los medios electrónicos para obtener información sobre cuentas bancarias, datos de tarjetas, claves o contraseñas de operaciones electrónicas, entre otros, las cuales son de dominio exclusivo de su titular, pero, al estar en manos del ciberdelincuente, pueden afectar de manera negativa la situación financiera de la víctima.

El año 2020 en Ecuador se sufrieron las consecuencias de la pandemia COVID-19, una de las principales fue el confinamiento, que limitó la capacidad de movimiento de

muchas personas, ante esta situación, muchos delincuentes decidieron migrar sus actividades al mundo tecnológico cometiendo actos delictivos mediante correos electrónicos, cuentas en redes sociales falsas, oferta engañosa de productos entre otros, evidenciándose un aumento en los delitos electrónicos. Por lo tanto, se concluye que, el confinamiento trajo como consecuencia que la delincuencia utilizara la tecnología para cometer delitos cibernéticos con el fin de lograr un provecho propio en perjuicio de las víctimas

Finalmente, se llega a la conclusión que, de los delitos informáticos mencionados en el Código Orgánico Integral Penal, los de mayor frecuencia, de acuerdo al número de denuncias, fueron: la violación a la intimidad la y estafa. Por su parte, dentro de los ciberdelitos cometidos en Ecuador que vulneraron el derecho a la intimidad de las personas durante la pandemia, se encuentran: la suplantación de identidad; la falsificación y uso de documentos falsos; la apropiación fraudulenta por medios electrónicos; y el acceso no consentido a un sistema informático; lo que afectó de manera negativa el patrimonio de las víctimas.

Referencias Bibliográficas

Aboso, G. (2017) *Derecho Penal Cibernético. La cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Buenos Aires. Editorial BdeF. Ltda.

Accenture (2023) COVID-19: *Impacto por sectores económicos. De grandes desafíos a cambios significativos*. https://www.accenture.com/es-es/services/consulting/coronavirus-industry-impact

Alonso-García, J. (2015) *Derecho penal y redes sociales*. Madrid: Aranzadi.

Alvarado, B. (2018). *La libertad de expresión en la publicación de fotografías y vídeos en la red social facebook y el derecho a la intimidad personal, Lima Norte, 2017.* Perú. file:///C:/Users/Usuario/Downloads/Alvarado_GBD.pdf

Antúnez, S. (2020) *Los delitos de ciberdelincuencia se disparan en confinamiento por la crisis sanitaria del Covid-19*. https://elderecho.com/los-delitos-ciberdelincuencia-se-disparan confinamiento-la-crisis-sanitaria-del-covid-19

Código orgánico integral penal. Asamblea Nacional del Ecuador (2022) Suplemento del Registro oficial no. 180. 10 de febrero de 2014. Ultima reforma: edición constitucional. registro oficial 20. 16 de marzo de 2022

Constitución de la República del Ecuador (2008). Publicado en el R.O No 449 el día 20 de octubre del 2008.

Curtis, S. (2011) Global Cities and the Transformation of the International System. *Review of International Studies* 37 (4): 1923-1947.

Declaración Mundial de los Derechos Humanos (1948). Asamblea General de las Naciones Unidas. París. Resolución 217 A (III)

Diario El Universo. (2020) *Las medidas que toma Ecuador, en emergencia sanitaria por coronavirus: cuarentena de pasajeros internacionales, suspensión de clases y eventos masivos.* Diario El Universo. https://www.eluniverso.com/noticias/2020/03/12/nota/7778376/coronavirus-ecuador-viaje-restriccion-vuelos-pasajeros-aeropuertos/

Ecuador News (2020) *Ciberdelitos en Ecuador crecen durante la pandemia*. https://ecuadornews.com.ec/2020/11/12/ciberdelitos-en-ecuador-crecen-durante-la-pandemia/

López, S. (2020). *Así afecta el Coronavirus a los delincuentes del mundo.* Diario AS actualidad. https://as.com/diarioas/2020/03/28/actualidad/1585389757_065038.html

Morales, J. (2018). Derecho a la intimidad. Palestra editores.

Perarales, A. (2018). El derecho a la intimidad. Tirant lo Blanch.

Rosenberg, E. (2007). *Fraude en Internet en EE. UU. en su punto más alto / estafa 'nigeriana' y otros delitos cuestan $ 198,4 millones.* Periódicos Hearst. https://www.sfgate.com/crime/article/U-S-Internet-fraud-at-all-time-high-Nigerian-2576989.php

Subijana Zunzunegui, Ignacio José. 2008. *El ciberterrorismo: Una perspectiva legal y judicial*. Eguzkilore 22 (2008): 169-187.

Zavala, M. (1982). *Derecho a la intimidad*. Abeledo-Perrot. Buenos Aires.

Zavala, M. (2018). *Derecho a la intimidad*. Abeledo-Perrot.