PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE JURISPRUDENCIA

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA

"LA PRUEBA ELECTRÓNICA EN EL ECUADOR DESDE LA PERSPECTIVA DEL CONVENIO DEL CIBERCRIMEN, ¿CÓMO FACILITAR LA PERSECUCIÓN DE DELITOS INFORMÁTICOS?"

AUTORA: LINA SOFÍA ESCOBAR CÁRDENAS

DIRECTOR: DR. SANTIAGO MARTÍN ACURIO DEL PINO

Quito, mayo 30, 2023

Resumen

Esta investigación se centra en el estudio de las reformas al Código Orgánico Integral Penal (COIP) de fecha marzo de 2023, específicamente a las actuaciones especiales relativas a contenido digital, y más concretamente a las formas de aseguramiento de datos específicos, incluidos los de abonado y de tráfico cuando hay riesgo de manipulación o pérdida; los requisitos para su presentación; la búsqueda, registro, acceso y secuestro de datos informáticos y sobre el rol del agente encubierto informático; todo esto con el objetivo principal de analizar sus especificidades, su forma de aplicación, el valor como prueba dentro de una investigación penal y sobre todo si guardan armonía con la norma legal existente y si para acceder a la información no se violenta los derechos constitucionales a la intimidad y secreto de las comunicaciones. Del análisis se puede apreciar su importancia, si estas reformas han sido necesarias y suficientes para afrontar los problemas que se suscitan en un proceso penal debido a la complejidad de esta materia y el constante desarrollo de la tecnología, o si se necesita de más legislación. Por último, se justificará la necesidad que tiene el Ecuador de adherirse al Convenio de Budapest para no quedarse fuera de un espacio que incentiva y promueve la lucha contra la ciberdelincuencia.

Palabras clave: prueba electrónica, delito informático, sistema informático, contenido digital, cooperación internacional.

Abstract

This research focuses on the study of the reforms to the Código Orgánico Integral Penal (COIP) (Criminal Code) dated March 2023, specifically the special actions related to digital content, and more specifically the forms of specific data assurance, including subscriber data and traffic when there is a risk of manipulation or loss; the requirements for its presentation; the search, registration, access and seizure of computer data and on the role of the computer undercover agent; all this with the main objective of analyzing its specificities, its form of application, its value as evidence within a criminal investigation and especially if they are in harmony with the existing legal norm and if access to information does not violate the constitutional rights to the intimacy and secrecy of the communication. From the analysis its importance can be appreciated, if these reforms have been necessary and sufficient to face the problems that arise in a criminal process due to the complexity of this matter and the constant development of technology, or if more legislation is needed. Finally, the need for Ecuador to adhere to the Budapest Convention will be justified so as not to be left out of a space that encourages and promotes the fight against cybercrime.

Keywords: electronic evidence, cybercrime, computer system, digital content, international cooperation

Índice

Introducción

La vida del hombre siempre ha desarrollado a la par de la de sus semejantes; somos seres sociales que nos necesitamos del uno al otro; en un inicio se interactuaba de manera personal, esto es, frente a frente; las distancias obligaron a que se empiece utilizar documentos como el papel para facilitar la comunicación, posteriormente sirvió el teléfono convencional y actualmente nos encontramos ya en un mundo digital, para ciertas personas fue la pandemia la que empujó el crecimiento de la comunicación a través de las redes sociales, con las repercusiones que también se generaron.

La tecnología se ha incrementado a grandes velocidades y con ella han surgido nuevas formas de cometer delitos en el mundo, sus autores se valen de algún dispositivo electrónico para su ejecución o estos dispositivos fueron el fin de la comisión, resultando esencial la prueba electrónica en casi todas las investigaciones penales. Es así como surge la necesidad de trabajar coordinadamente, que exista colaboración de los países para enfrentar esta problemática global, suscribiéndose el Convenio de Budapest, cuyo objetivo es incrementar la cooperación internacional entre los Estados suscriptores orientándolos a adoptar una normativa homogénea que permita facilitar el combate de los delitos informáticos.

El Ecuador ha reaccionado con lentitud normativa ante los avances tecnológicos, pues el anterior Código de Procedimiento Penal contaba con disposiciones predeterminadas para la prueba física y es con el Código Orgánico Integral Penal en vigencia desde el año 2014 en el que se empieza a dar importancia a la prueba electrónica como un medio probatorio y actualmente se ha establecido una sección sobre actuaciones especiales relativas a contenido digital, reconociendo el su valor como prueba para la lucha contra la ciberdelincuencia.

El artículo 499 del COIP en su numeral 6 menciona que podrá admitirse como medio de prueba todo contenido digital (COIP, 2014), pero no se hace una distinción clara con la prueba electrónica que es toda la información que se encuentra en cualquier formato que sea legible y/o reproducible a través de medios electrónicos y mediante la cual se pretende probar un determinado hecho materia de una controversia judicial (Espinoza, 2022), acreditar tanto la existencia de la infracción como la responsabilidad penal de la persona procesada.

Las estadísticas de la Unidad de Ciberdelitos de la Policía Nacional dan a conocer que en el país se han registrado 3183 delitos informáticos desde el año 2020 hasta julio de 2022, cifras que demuestran que estamos frente a un aumento exponencial de estos delitos de tipo

informático. En el artículo 500 del COIP se aborda de manera básica el procedimiento para tratar el contenido digital, sin embargo, se hace necesario que dicho procedimiento sea regulado para mejorar el tratamiento que se da a la evidencia digital a nivel internacional, debido a que estos delitos pueden tener una carácter transnacional y sobretodo que guarde relación con las actuales reformas.

La prueba electrónica debe adaptarse a la normativa constitucional y legal existente, su inobservancia puede generar riesgo de que se comprometa su recuperación, preservación, presentación y como consecuencia no sea valorada por el juez penal.

La presente investigación se basará en un análisis de las actuaciones especiales relativas al contenido digital y si estas transgreden los derechos constitucionales a la intimidad, secreto de las comunicaciones y protección de datos personales. A su vez justificar sobre la adhesión del Ecuador al Convenio de Budapest como forma de mejorar la persecución de delitos informáticos.

Antecedentes teóricos del problema

Sobre el tema materia de la investigación se han desarrollado estudios previos como el trabajo titulado “La prueba electrónica en el marco nacional y en el internacional en Latinoamérica”, desarrollado por el Programa de Asistencia contra el Crimen Transnacional Organizado que abarca temas sobre la obtención de la prueba electrónica y los medios de incorporación a un proceso penal e identifica los diferentes marcos normativos de los países que forman parte de este proyecto para compararlos con la regulación internacional, en este caso con la normativa que consta en el Convenio de Budapest, con la finalidad de identificar cuáles son las prácticas más favorables así como las lagunas existentes y de esta forma proporcionar sugerencias (El PAcCTO, 2022).

En lo que refiere a Ecuador manifiesta que el COIP en la parte procesal no cuenta con una regulación expresa sobre la prueba electrónica a la cual se la sigue asemejando con la prueba física, lo que genera mayor dificultad en su actuación pero si otorga las primeras pautas para desarrollar esta temática hablando sobre temas de obtención, preservación y la valoración de los datos que se encuentran en dispositivos electrónicos, hace un análisis de normas que pueden permitir recolectar información para un determinado caso pero que no indican cómo hacerlo, por lo que invita a reflexión sobre la necesidad de contar ya en el COIP con un capítulo que refiera específicamente sobre la prueba electrónica.

Se hace constar que con fecha 29 de marzo de 2023 se aprobaron nuevas reformas al Código Orgánico Integral Penal en la que se establece una sección sobre actuaciones especiales relativas a contenido digital, mismas que entraron en vigencia a partir del 29 de abril de 2023, por lo que sobre este tema en específico se han realizado mínimos comentarios.

Estos antecedentes permiten justificar la pertinencia de este tema de investigación, que trata de evidenciar si las normas incorporadas guardan armonía con las existentes en el COIP y si sobre todo si en su aplicación contravienen derechos constitucionales, lo que permitirá confrontar de mejor manera las nuevas formas de cometer delitos a la hora de tramitar un caso.

Sección 1.
La prueba documental en el COIP, clases de prueba y la observación de las garantías al debido proceso

La tecnología avanza a pasos agigantados cumpliendo un papel fundamental en el desarrollo de la sociedad, pero así como proporciona una gran cantidad de beneficios al ser instrumentos indispensable creados para ayudar y mejorar nuestras actividades cotidianas, personas se han aprovechado de estos recursos técnicos para cometer delitos, configurándose nuevas modalidades delictivas que comúnmente son contra la propiedad como las estafas, contra la propiedad intelectual, la intimidad, aumento de la pornografía infantil, entre otras, y que se debe a la posibilidad de adquirir dispositivos electrónicos en los que dejamos un registro de nuestros datos al que se puede acceder con facilidad con el riesgo de ser manipulados o alterados; es decir, se utiliza a las tecnologías de la información y comunicación como objeto del ataque y como medio para cometer delitos (El PAcCto, 2022).

La informática es el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras (Real Academia Española, s.f., definición 3). Por otra parte, Dreyfus entiende a la informática como la ciencia del procesamiento electrónico, como un cimiento del conocimiento y es el resultado de los términos: información y automatización (citado por Jiménez, 2017).

Al ser la informática este medio idóneo para realizar actos ilícitos por el mal uso que se le ha dado a las tecnologías de la comunicación es importante que la normativa vaya a la par con la nueva realidad en la que nos encontramos y de esta forma combatir los delitos informáticos que según Dávara Rodríguez son “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un medio informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software” (citado por Jiménez, 2017, pág. 132).

1.1 La prueba

Estas formas de cometer delitos también han generado que sea la misma tecnología la que desarrolle formas de investigación, siendo la prueba electrónica la base para una posterior persecución penal.

La Enciclopedia Jurídica Omeba (2009) define como prueba a "la demostración de la existencia de un hecho material o de un acto jurídico en las formas admitidas por la ley" (citado por Gaibor, 2022); busca generar convicción en el juzgador de aquello que las partes procesales afirman.

"La prueba es la razón, argumento, instrumento u otro medio con el que se pretende mostrar y hacer patente la verdad o falsedad de algo, es un indicio, señal o muestra que se da de algo" (RAE, s.f.).

"De acuerdo a Cabanellas la prueba es una "demostración de la verdad de una afirmación, de la existencia de una cosa o de la realidad de un hecho" (2006).

Según el COIP, en su artículo 453 "La prueba tiene como finalidad llevar a la o el juzgador al convencimiento de los hechos y circunstancias materia de la infracción y la responsabilidad de la persona procesada" (COIP, 2014).

En el proceso penal ecuatoriano existen tres tipos de pruebas: la documental, testimonial y la prueba pericial (COIP, 2014), serán estas las que servirán de base para que un juez pueda fundamentar sus resoluciones en las causas puestas a su conocimiento, resultando trascendental saber diferenciar a cada una de ellas para que no existan confusiones a la hora de su presentación.

Al ser el tema del presente trabajo de investigación el análisis de la prueba electrónica me limitaré a tratar únicamente sobre la prueba documental ya que en esta se aborda al contenido digital.

1.2 La prueba documental como medio probatorio

La Enciclopedia Jurídica Omeba, en su tomo XXIII, "PRES-RAZO" (2009), define a la prueba documental como:

> Uno de los medios más importantes, para llevar al ánimo del juzgador a la verdad de las afirmaciones que las partes han propuesto como base de la relación procesal. Su gran trascendencia como medio probatorio, tiene atingencia a través de la idoneidad del documento para perpetuar hechos pasados, son como una voz fijada perdurablemente.

En un proceso penal la constituyen los documentos, registros, escrituras, correos electrónicos, fotografías, videos, grabaciones, mensajes que permiten a los sujetos procesales

demostrar las teorías que presentan dentro de un juicio. Dentro del documento se incluye al contenido digital en el artículo 500 del COIP en el que se encuentran las reglas a seguir para su investigación, norma que se encontraba incompleta hasta antes de la reforma sobre actuaciones especiales relativas a contenido digital, donde ya se regula el procedimiento para su obtención, preservación, posterior presentación y valoración en un juicio penal, anteriormente se la adaptaba a la normativa existente para la prueba física, dándole así un tratamiento inadecuado ya que este medio probatorio cuenta con características propias, situación que se busca subsanar con esta reforma.

Para que un documento sea admitido como prueba se debe observar los criterios de valoración que se encuentran mencionados en el artículo 457 del COIP, esto es: su legalidad, autenticidad, sometimiento a cadena de custodia y grado actual de aceptación científica y técnica de los principios en que se fundamentan los informes periciales (COIP, 2014).

Cuando se habla de su legalidad se refiere a que dicha prueba haya sido obtenida dentro de las formas contempladas en la ley, que no existan causas de su exclusión, que haya sido dispuesta por autoridad competente. En cuanto a la autenticidad, dicha prueba debe ser real y no manufacturada o alterada por una de las partes, lo que generaría falta de eficacia probatoria; que sea sometida a cadena de custodia, es decir, que los elementos probatorio encontrados en la escena del crimen o lugar de los hechos deberán ser los mismos que se presenten en la audiencia de juicio. Grado de credibilidad del perito, que sus actuaciones y conclusiones deben respaldarse en criterios científicos, generando certeza, convencimiento, no solo en los jueces sino también en los sujetos procesales. (Gozaini, 2015).

A efectos de saber valorar la prueba electrónica, resulta trascendental tener mayor conocimiento de esta temática y que se defina lo que constituye el contenido digital, datos de tráfico, proveedor de servicios, sistema informático, y para esto se cita lo que el artículo 234.4 del COIP considera:

> a. Contenido digital.- es todo dato informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico o canal de comunicación que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.
> b. Datos de tráfico.- Contenido digital relativo a una comunicación efectuada por medio de un sistema informático o canal de comunicación, generados por este sistema como elemento de una cadena de comunicación, indicando su origen, su destino, su trayecto, la hora, la fecha, el tamaño, la duración o el tipo de servicio subyacente.

> c. Proveedor de servicios.- Cualquier entidad, pública o privada, nacional o internacional, que proporciona a los usuarios de sus servicios la capacidad de comunicarse a través de un sistema informático, o de cualquiera de las tecnologías de la información y comunicación, así como cualquier otra entidad que procese o almacene contenido digital en nombre y por cuenta de aquella entidad proveedora o de sus usuarios.
> d. Sistema informático.- Cualquier dispositivo o conjunto de dispositivos interconectados o asociados, en que uno o varios de ellos desarrolla, ejecutando un programa, el tratamiento automatizado de contenido digital (COIP, 2014, art.234.4).

Es necesario comprender e identificar los términos antes mencionados que serán abordados a lo largo de esta investigación.

1.3 Prueba electrónica

Chinchay y Dávila (2015) la definen como "el medio de información con valor probatorio que se encuentre contenida en un formato electrónico y es transmitida por dicho medio".

Para Delgado (2018) es toda información que tiene valor probatorio y que se encuentra en un medio electrónico o es transmitida por este y es importante recalcar que se trata de cualquier tipo de información producida, almacenada o transmitida por medios electrónicos, la misma que puede acreditar hechos en un proceso penal.

Así mismo, Holguín (2015) plantea que:

> La aportación de una prueba electrónica en cualquier jurisdicción es cada vez más común, aquí se incluyen los comentarios en chats o redes sociales, las grabaciones de video vigilancia, la mensajería de texto, los e-mails, las páginas web, las notas de voz o imágenes, que todos forman parte de una variedad de fuentes probatorias que deben tener acceso al proceso judicial a través de alguno de los medios de prueba que contempla la ley, estos son medios de uso común y forman parte de nuestro día a día. (Citado por Punguil, 2019)

La prueba electrónica tiene características especiales entre las que se encuentra que es volátil, es decir, pueden desaparecer sin dejar algún rastro por lo que es necesaria la conservación rápida de los datos y para ello es importante tomar medidas que permitan la preservación de este tipo de prueba (Nessi, 2017).

En síntesis la prueba electrónica viene a ser toda la información constante en medios electrónicos la que permitirá a los sujetos procesales dentro de un juicio demostrar sus aseveraciones.

1.3.1 Diferencias entre la prueba electrónica y la prueba documental

Una de las principales diferencias es el medio a través del cual se presenta toda la información que permitirá demostrar la veracidad de los hechos dentro de un juicio, en el caso de la prueba documental se trata de algo tangible y ocurre lo contrario con la prueba electrónica que se refiere a la información almacenada en forma digital, entonces si bien los dispositivos de almacenamiento se encuentran en una forma física no sucede lo mismo con los datos en sí.

La prueba electrónica cuenta con características particulares debido a la simplicidad que existe al momento de manipular esta información y aquí radica la importancia de contar con un personal capacitado para la investigación con el objetivo de encontrar un documento o un archivo que servirá como medio de prueba y a su vez que no se haga un uso inadecuado del dispositivo violentando así su derecho a la intimidad, al secreto de las comunicaciones, a su vida privada y a su vez protegiendo los datos personales.

El motivo por el cual se asemeja a la prueba documental con la prueba electrónica fue por cuanto el perito extraía la información de un dispositivo electrónico y posteriormente esta era impresa y presentada como documento en juicio, pero se trata de pruebas diferentes, en la prueba documental puede incluirse facturas, recibos, contratos, etc., mientras que en la prueba electrónica se encuentran correos electrónicos, mensajes de texto, archivos de audio y video, registros de actividades realizadas a través de internet y esto genera la necesidad de adoptar técnicas y herramientas propias para su obtención y presentación.

1.4 Evidencia digital

La evidencia se entiende como todo elemento que permite establecer de una forma clara la relación que existe entre dos elementos encontrados en la escena de un hecho que es el que se va a investigar (Castillero, 2018).

La organización Grupo de Trabajo Científico sobre Evidencia Digital la define como “información de valor probatorio almacenada o transmitida en forma digital”, y esta

información es la que permitirá sustentar o rechazar una teoría de un determinado caso (citado por Sergi, 2018).

En un proceso penal la evidencia es utilizada como la primera herramienta de la investigación, misma que en la primera etapa del proceso puede convertirse en un elemento de convicción y como prueba ya en el juicio oral.

En consideración a que en la actualidad la interacción de las personas se realiza a través de medios electrónicos y telemáticos nace la necesidad de probar las infracciones penales en el formato que se producen, esto es, en digital como un chat de WhatsApp, correo electrónico, páginas web, entre otros.

1.5 Debido proceso en la obtención del contenido digital o evidencia digital. Derecho a la intimidad, al secreto de las comunicaciones y a la protección de datos personales.

Como se mencionó anteriormente, la norma fue pensada en un inicio para regular las investigaciones que se realizaban bajo un entorno físico, pero actualmente en muchas de las investigaciones se utiliza la prueba que incluye contenido digital, por lo que las acciones que se tomen para la obtención de la misma deben ser legales, auténticas, sometiéndolas a cadena de custodia y no afectando los derechos que tienen las personas a su intimidad, al secreto de las comunicaciones y a la protección de los datos personales.

Así surge la interrogante de si la norma con la que se cuenta en el Código Orgánico Integral Penal es la adecuada y a su vez protege los mencionados derechos de las personas procesadas, considerando que la investigación puede realizarse en dispositivos electrónicos, sistemas informáticos, medios de almacenamiento informático donde se encuentra información de interés para determinado caso, la misma que tiene la característica de ser personal.

La Constitución de la República del Ecuador dentro de los derechos de libertad, en su artículo 66 reconoce y garantiza a las personas:

> Numeral 19.- El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (CRE, Registro Oficial 449, 20- oct, 2008)

Es de gran importancia porque protege la vida privada de una persona, su identidad, características, comportamientos y preferencias, debiéndose mantener el control sobre cómo y

en qué circunstancias se puede compartir esta información. Cuando los datos personales sean de importancia dentro de un proceso penal es un aspecto fundamental el que estos sean protegidos para garantizar su integridad y sobretodo su confidencialidad.

Numeral 20.- "El derecho a la intimidad personal y familiar"

De acuerdo con Jiménez (2000) "la privacidad y la intimidad integran una zona de reserva personal, propia de la autonomía del ser humano, irreducible para la intromisión de los restantes habitantes y el poder público".

Para Bidart (2001) "la intimidad es la esfera personal que está exenta del conocimiento generalizado de tercero", y la privacidad es: "la posibilidad irrestricta de realizar acciones privadas (que no dañen a otros) que se cumplan a la vista de los demás y que sean conocidas por estos" (Citado por Villalba, 2021).

La Corte Constitucional del Ecuador en la Sentencia No. 2064-14-EP/21 del 27 de enero de 2021 en referencia al derecho a la intimidad ha determinado:

> El derecho a la intimidad implica la existencia, goce y disposición de una esfera reservada para el individuo, misma que le permita desarrollar libremente, es decir, sin injerencias externas, ni arbitrarias, su personalidad en los distintos ámbitos que componen a su vida (Corte Constitucional del Ecuador, Caso No. 2064-14-EP, 27-enero, 2021).

La Corte Interamericana de Derechos Humanos ha establecido que el derecho a la intimidad no es absoluto, puede ser restringido por cada Estado, siempre que dicha restricción no sea abusiva ni arbitraria, es decir, las limitaciones impuestas deben estar previstas en la ley y buscar un fin legítimo (Corte Interamericana de Derechos Humanos, Caso Tristán Donoso Vs. Panamá, 27-ene-2009).

Por el derecho a la intimidad la persona puede desarrollar sus actividades sin que sea vigilado por otro y que su hacer y decir no sea divulgado a los demás.

Numeral 21.- El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; la misma que no podrá ser retenida, abierta ni examinada, con excepción de los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen (CRE, 2008).

Entendiéndose la correspondencia como las comunicaciones escritas como cartas que era un medio de comunicación a la distancia, correos electrónicos y otros mensajes enviados entre dos o más personas. Es importante mencionar que la Corte Interamericana de Derechos

Humanos ha señalado que las conversaciones telefónicas al ser también una forma de comunicación se encuentran incluidas dentro de la protección a la vida privada. (Corte Interamericana de Derechos Humanos, Caso Tristán Donoso Vs. Panamá, 27-ene-2009).

La Ley Orgánica de Comunicación (LOC) en su artículo 31 dispone que

> Todas las personas tienen derecho a la inviolabilidad y al secreto de sus comunicaciones personales, sea que éstas se hayan realizado verbalmente por medio de las redes y servicios de telecomunicaciones legalmente autorizadas o estén soportadas en papel o dispositivos de almacenamiento electrónico (LOC, 2013).

Es importante determinar que las comunicaciones privadas pueden incluir correos electrónicos, mensajes de texto, llamadas telefónicas, mensajes de voz, videoconferencias, comunicaciones por radio y cualquier otro medio que pueda ser utilizado para transmitir información. Cuando este tipo de comunicaciones han sido utilizadas para el cometimiento de una infracción deben ser protegidas porque constituirá en prueba fundamental en el juicio, por lo que resulta necesario tener conocimiento de la forma de recolección, preservación y presentación, observándose las garantías del debido proceso.

Sobre este respecto el COIP en el artículo 470 dispone que:

> No podrán grabar o registrar por cualquier medio las comunicaciones personales de terceros sin que ellos hayan conocido dicha grabación o registro, salvo los casos expresamente señalados en la ley. La información obtenida ilegalmente carece de todo valor jurídico (COIP, 2014).

Norma que obliga a quien realiza la investigación a observar las garantías del debido proceso para evitar que su vulneración afecte el objetivo de la misma y a pesar de que esta pueda demostrar un hecho no pueda ser presentada en juicio.

1.5.1 Derecho a la intimidad dentro del Código Orgánico Integral Penal

El artículo 5 del Código Orgánico Integral Penal lo ha establecido como un derecho al debido proceso penal, desarrollándolo en el numeral 10, determinando:

> Que toda persona tiene derecho a su intimidad personal y familiar. No podrán hacerse registros, allanamientos, incautaciones en su domicilio, residencia o lugar de trabajo, sino en virtud de orden de la o el juzgador competente, con arreglo a las formalidades y motivos previamente definidos, salvo los casos de excepción previstos en este Código.

De igual forma el numeral 1 del artículo 475 ibídem dispone: “la correspondencia física, electrónica o cualquier otro tipo o forma de comunicación, es inviolable, salvo los casos expresamente autorizados en la Constitución y en este Código”

De lo expuesto, al ser la intimidad un derecho humano relevante se lo considera inviolable y solo se lo podrá irrumpir en los casos autorizados por la ley.

Este derecho comprende lo que es la inviolabilidad de secreto, domicilio y la correspondencia. Al respecto el Doctor Felipe Rodríguez refiere:

> Dentro de la intimidad consta, además, la inviolabilidad de secreto, la inviolabilidad de domicilio, la inviolabilidad de correspondencia. Si usted ve pornografía (con actores adultos) en su celular (actividad lícita) nadie puede ingresar a su teléfono para examinar sus preferencias sexuales. Si usted vive de forma ordenada o desordenada, nadie tiene que ingresar a su casa a ver cómo habita, a menos que usted lo invite a hacerlo. (Rodríguez, 2023, p.194)

El COIP de igual forma para garantizar su fiel cumplimiento sanciona a quien lo violente, pues consta tipificado como delito en el artículo 178 que señala:

> La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley (COIP, 2014).

Aparte de lo manifestado, la Constitución de la República, como garantía del debido proceso y con la finalidad de asegurar su respeto y fiel cumplimiento, ha establecido en su artículo 76, numeral 4 que las pruebas obtenidas o actuadas con violación de la Constitución o la ley no tendrán validez alguna y carecerán de eficacia probatoria, significando esto que si se violenta en la obtención de alguna evidencia el procedimiento establecido en la norma o se atenta contra un derecho constitucional, el juzgador, en la etapa procesal correspondiente, a pedido de las partes, deberá declararla ineficaz y por lo tanto no podrá ser practicada en la etapa del juicio.

SECCIÓN 2.
La nueva normativa procesal sobre contenido digital en el Código Orgánico Integral Penal

En esta sección se hace un breve análisis de las actuaciones especiales relativas a contenido digital con la finalidad de conocer su forma de aplicación y sobre todo si en estas actuaciones se está cumpliendo con el debido proceso, requisito para que este tipo de prueba sea valorada.

2.1. Evolución y características de la prueba documental en el Ecuador

El Derecho Penal ecuatoriano a lo largo de los años ha sufrido innumerables reformas en su articulado, varias de ellas tenían relación a las nuevas formas de comisión de delitos y procesalmente a la utilización de los avances tecnológicos en la obtención de la prueba.

Cuando se encontraba vigente el Código de Procedimiento Penal a la prueba se la clasificaba en testimonial, material y documental, esta última se encontraba constituida por los documentos públicos y privados, los cuales eran valorados por la calidad de documentos, así como por su relación con el conjunto de las demás pruebas que obren en el proceso; este Código no hizo una definición de lo que debe ser el documento, por lo que de acuerdo a la RAE se lo considera como un escrito en el que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo (RAE, s.f.), y así era valorado. En este tipo de prueba no se daba importancia a la prueba informática como tal, el juez valoraba lo que expresaba el documento y no lo que la persona declaraba.

Respecto de la prueba documental, se evidencia que el legislador ya empieza a tratar sobre el contenido digital, al cual lo considera como documento semejante, constituyendo este la correspondencia epistolar, telegráfica, telefónica, cablegráfica, por télex o por cualquier otro medio de comunicación, también a las películas, registros informáticos, fotografías, discos u otros documentos semejantes, es decir, era la tecnología de esa época; observándose que no se le daba la importancia que este tipo de prueba podía aportar en un proceso penal.

No obstante, no fue sino hasta el año 2014 que los legisladores comprendieron la necesidad de incluir en el nuevo COIP, las nuevas formas de interacción del ser humano: las redes sociales, el uso del internet, la vida digital, etc., como medio para cometer una infracción, habiendo tipificado varios delitos informáticos y normas procesales que faciliten la probanza;

hasta que en abril de 2023 entró en vigencia una sección sobre la prueba digital, que es lo que se va a analizar, y también determinar si con su aplicación se estaría violentando derechos constitucionales como el secreto de las comunicaciones y de la dignidad.

Se debe tener en cuenta que la existencia de contenido digital no nació con este Código, aquella ya era reconocida por nuestro ordenamiento jurídico, sino que, por desconocimiento de la ciencia informática, no era vista penalmente relevante. Más aún, en el año 2002, entró en vigencia la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, puesto que el desarrollo tecnológico era inminente e implacable. Así las cosas, el Código Orgánico Integral Penal plasmó dentro de sus líneas la posibilidad de emplear contenido digital como elemento probatorio en el proceso penal.

Con la entrada en vigencia de la Ley Orgánica Reformatoria a varios cuerpos legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral se incorpora en el COIP una sección sobre actuaciones especiales relativas a contenido digital que trata de incluir el aseguramiento, presentación, búsqueda, registro, acceso, secuestro, preservación y divulgación de datos informáticos con la finalidad de combatir el cibercrimen pero garantizando la protección de datos personales, esto en consideración a las medidas propuestas por el Convenio de Budapest y su Segundo Protocolo Adicional.

2.2 Mecanismos para la obtención, preservación, presentación y valoración del contenido digital en el Código Orgánico Integral Penal

Con los avances de las tecnologías de la información se han implementado algunos mecanismos para la obtención y práctica de la prueba con contenido digital, esto por la necesidad de que la investigación penal vaya a la par con las nuevas formas de comisión de delitos y con lo que actualmente nos ofrece la tecnología para demostrar la existencia de una infracción y la participación que tuvo determinada persona en ella.

Como se ha manifestado, el artículo 500 del COIP da una breve definición de lo que constituye el contenido digital para posteriormente indicar reglas a seguir en una investigación, recomendando aplicar técnicas digitales forenses para su recuperación, análisis, presentación y valoración, caracterizándolos a estos medios como volátiles y no volátiles, que dependiendo a la clase que pertenecen tendrán su tratamiento.

En cuanto a los medios volátiles son aquellos que no pueden permanecer inmutables o inalterables con el pasar del tiempo por ser accesibles a través de la red, principalmente de internet y por el contrario, los medios no volátiles son los que permanecen inalterables con el tiempo por encontrarse en soportes físicos, como son discos duros, memorias USB, tarjetas SIM o dispositivos electrónicos (Calaza y Muinelo, 2020).

La prueba volátil como páginas web, redes sociales, blogs, al tener la probabilidad de ser manipulada con facilidad o de desaparecer con el tiempo debe contar con su tratamiento especial para conservarla y así garantizar la integridad de la información. Es así que los medios de comunicación electrónicos como WhatsApp, emails, video-conferencias pueden considerarse como una prueba válida si cumplen con requisitos de validez necesarios y si en su obtención se respetaron las garantías constitucionales.

Por lo tanto, como características de la prueba electrónica es que es volátil, de fácil alteración o modificación, puede ser reproducida de manera ilimitada y también puede ser eliminada de forma rápida (Espinoza, 2022), esto hace necesario e indispensable que para su aseguramiento se deba observar lo que dispone el Manual de Manejo de Evidencias Digitales y Entornos Informáticos para la correcta utilización de la prueba electrónica, lo que le permitirá a la Fiscalía demostrar la existencia de una infracción y su responsable, además ser una guía para el personal del Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses al momento de actuar frente a estos casos de delitos informáticos y que la prueba sea valorada legalmente por el juzgador cumpliendo con los principios de objetividad, autenticidad, legalidad, idoneidad, inalterabilidad. De igual forma, se hace necesario entender el contenido de la normativa constante en la sección 1.1 del COIP referente a las actuaciones especiales relativas a contenido digital, para conocer su alcance, forma de aplicación y así evitar vulneraciones que hagan que la prueba se vuelva ineficaz.

2.3. Armonización entre la reforma del 29 de marzo de 2023 y el Código Orgánico Integral Penal

Artículo 477.1.- Aseguramiento de datos.- Para una mejor comprensión de este artículo es necesario saber las definiciones de lo que son datos informáticos específicos, datos de abonado y datos de tráfico; así:

Los datos informáticos específicos son los de interés del fiscal, es decir, se caracterizan por su especificidad y hacen referencia a un dato concreto.

Los datos de tráfico son aquellos generados para orientar una comunicación desde el origen hasta su destino, es decir, estos son auxiliares a la comunicación, rodean al mensaje que se transmite sin formar parte del mismo. En una llamada telefónica se trata del número de teléfono de la llamada, el nombre y la dirección del abonado de origen, el número de destino y el nombre y dirección del abonado de destino, la fecha y hora del comienzo y fin de la comunicación, el servicio telefónico utilizado, entre otros datos (Fernández, 2016).

Los datos de abonado son los datos personales de tipo estándar que permiten determinar la identidad de un usuario, dirección, ubicación geográfica, número de teléfono, datos sobre la facturación y los pagos que son el resultado de un contrato, es decir, abarca aquella información que tenga un proveedor de servicios y que haga referencia a los abonados de sus servicios (Convenio sobre la ciberdelincuencia, Informe explicativo, 2022), son los datos que otorga un usuario al momento de contratar un servicio.

El aseguramiento de datos hace referencia a la facultad que tiene tanto el titular de la acción penal pública, esto es el fiscal, para realizar actuaciones fiscales urgentes en los casos en los que se requiere obtener, conservar, preservar evidencias o impedir la consumación de un delito, lo puede realizar dentro de una investigación previa o en la etapa de instrucción fiscal que también es investigativa, de ordenar a una o varias personas naturales o jurídicas la conservación expedita de datos informáticos específicos que le sean útiles para su investigación, incluidos los datos de abonado y de tráfico que hayan sido almacenados mediante un sistema informático cuando haya motivos para sospechar que los datos informáticos son especialmente vulnerables a la pérdida o a la modificación. También esta conservación puede ser solicitada por la Policía Nacional, en delito flagrante, cuando medie investigación previa, instrucción fiscal, actuaciones fiscales urgentes, actos administrativos e investigaciones de noticias de personas desaparecidas, en este caso se notificará a la Fiscalía en el plazo máximo de ocho horas posteriores a la solicitud (COIP, 2014). En síntesis se trata de una medida que tiene el objetivo de asegurar los datos, evitando su pérdida o manipulación, no va a existir ningún tipo de divulgación.

El problema sobre esta facultad radica en que no se detalla las técnicas o el camino a seguir para esta conservación de datos y tampoco se conoce si las personas designadas cuentan con las herramientas necesarias para su conservación de manera correcta y sin causar algún tipo de

afectación, así como si están en capacidad de conservar los datos por el tiempo que se encuentra establecido tratándose de un máximo de noventa días que son prorrogables si se mantienen los motivos que fundamentaron la orden.

Considero que la orden de aseguramiento no debe darse a cualquier persona, sino a quienes se encuentren en poder o bajo control de esta información o a personal capacitado del Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses en virtud de que tienen la facultad y el conocimiento para hacerlo, más aun cuando se debe garantizar su eficaz aseguramiento, ya que al ser datos manipulables pueden ser objeto de alteraciones.

En cuanto a los datos específicos no se nos da una definición de en qué consisten estos, pudiendo ser parte los datos de contenido, los que deberían asegurarse, siempre y cuando permitan comprobar el cometimiento de una infracción o impedir la consumación de un delito.

En lo referente a la facultad que también se le ha dado al personal de la Policía Nacional esto podría hacerlo únicamente en flagrancia en razón de que son ellos los que acuden de forma inmediata al lugar de los hechos, cuando se está en investigación o instrucción fiscal esta facultad la tiene Fiscalía.

Así mismo debe observarse la cadena de custodia, diferenciando lo que es continente y contenido, pues el primero hace referencia a los componentes físicos y el segundo a la información y según doctrina la cadena de custodia debe aplicarse a lo material.

Para garantizar la integridad de los datos asegurados no basta solo el sometimiento a la cadena de custodia, sino que debe realizarse el aseguramiento con el uso de los códigos de integridad como por ejemplo el Código HASH que constituye una técnica informática de máxima importancia en lo relativo al aseguramiento de la prueba informática. Se basan en la obtención de datos a través de una copia espejo e identificando la información que se copia de forma única (Gómez, 2019).

Artículo 477.2.- Orden de presentación.- Hace referencia a la facultad que tiene el juez, siempre a pedido del fiscal como titular de la acción penal, de ordenar a cualquier persona natural o jurídica que esté en poder de un dispositivo de almacenamiento de datos informáticos para que presente, remita o entregue datos de contenido alojados en un sistema informático o en un dispositivo de almacenamiento de datos informáticos, siempre y cuando se vinculen con la investigación de un delito concreto; y sin orden judicial cuando se trate de datos de abonado y de tráfico (COIP, 2014).

De igual forma, resulta esencial para comprender este artículo el definir en qué consisten los datos de contenido.

Según Forouzan (2013), “el Modelo OSI se divide en siete capas, cada una proporciona una funcionalidad específica necesaria para el intercambio de datos entre sistemas”, sirve para describir cómo se comunican los dispositivos en una red de computadoras.

Al hablar de datos de contenido nos referimos a las capas de sesión, presentación y aplicación, es decir, se trata de todo lo transmitido como parte de la comunicación que no sean datos de tráfico.

Es apropiado que para obtener datos de contenido que, en otras palabras, es la conversación que mantuvieron dos o más personas se requiera de orden de juez sobretodo porque debe garantizarse la confidencialidad que debe tener este tipo de información, porque se puede agredir derechos fundamentales al revelar aspectos de la vida privada y de la intimidad.

Con respecto a la presentación de datos de tráfico, de igual forma considero que debe otorgarse a pedido del fiscal y con orden del juez ya que si bien los datos de tráfico son los datos que rodean el mensaje que se transmite, también permiten saber ¿quién se ha comunicado con quién?, ¿con qué frecuencia?, ¿en qué momento?, mostrando hábitos de vida cotidiana de una persona, así mismo contiene datos personales que hacen identificables a personas y pueden afectar el derecho a la intimidad, al secreto de las comunicaciones y a la protección de datos personales. Algunos autores manifiestan que los datos de tráfico y de abonado no son tan comprometedores como los de contenido por lo que no necesitarían de una orden judicial para obtenerlos, sin embargo, los datos de tráfico también pueden revelar información sobre la vida personal, de ahí se debe su protección (Asociación por los Derechos Civiles, 2018).

Según La Corte Constitucional Ecuatoriana la intimidad constituye:

> La existencia, goce y disposición de una esfera reservada exclusivamente para el individuo.3 Podría entenderse como aquel ámbito muy propio donde las personas desean “estar a solas” sin la mirada de particulares o del Estado.4 Los mensajes que una persona envía a sus familiares, los chats de grupo de trabajo, las contraseñas que dan acceso a un teléfono celular o correo electrónico, la información respecto de los ahorros y finanzas de una persona, la conversación entre un abogado y cliente, entre otros, son ejemplos de acontecimientos que generalmente no son compartidos de manera pública. (Corte Constitucional del Ecuador, Caso No. 77-16-IN, 27-ene, 2022)

A pesar de lo indicado, la intimidad no es absoluta, la Corte Interamericana de Derechos Humanos (CIDH), en el caso Tristán Donoso vs Panamá. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia de 27 de enero de 2009, explicó que:

> El ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública.
> Por ello, una injerencia en la intimidad puede ser autorizada, aunque deberá cumplir con requisitos simultáneos: (i) estar prevista en ley, (ii) perseguir un fin legítimo, y (iii) ser una medida idónea, necesaria y proporcional (CIDH, 2009, pág 17, párr. 55-56).

Según el COIP hay que saber diferenciar por qué el grado de protección, va a ser mayor tratándose de datos de contenido por cuanto es la información que se transmitió que es distinto a los datos de transmisión de la información o información asociada a la comunicación, a los cuales se les da un menor grado de protección por considerar que no es el mismo nivel de afectación cuando se requiere este tipo de información. En consideración a esto los únicos datos que no necesitan autorización judicial serían los datos de abonado

Artículo 477.3.- Esta disposición legal hace referencia a la facultad que tiene el juez, siempre a pedido de fiscal, de ordenar la búsqueda de información tanto en fuentes abiertas como en fuentes cerradas de datos informáticos almacenados en sistemas informáticos o en un medio de almacenamiento de datos informáticos o electrónicos (COIP, 2014) que puede servir en la investigación que se esté realizando; por ejemplo se pueden hacer búsquedas en Facebook, Google, Twitter, en estas se debe verificar si pertenece a un perfil abierto o cerrado, en el caso de ser abierto se podría realizar la investigación sin necesidad de la orden judicial, pero si este es cerrado, que comparte la información solo a las personas que conoce y que fueron aceptados como amigos o si la información pertenece a un grupo cerrado, necesariamente se debe tener autorización judicial.

Es necesario conocer que al domicilio de las personas solo se puede ingresar con orden de allanamiento, la que debe constar por escrito y señalando los motivos que determinan el registro, las diligencias por practicar, la dirección o ubicación concreta del lugar o lugares donde se ejecuta el allanamiento y su fecha de expedición. En ninguna circunstancia podrá emitirse órdenes de registro y allanamientos arbitrarios. Se hace énfasis en el artículo 481 del COIP porque para efectivizar lo dispuesto en el artículo 477.3 para la mayoría de los casos se tendrá que contar con la orden de allanamiento y para la obtención hay que determinar las diligencias a practicar, si se va a necesitar la preservación de datos informáticos esto también

deber estar en la orden, no deja abierto a posibilidades que puedan darse a la hora del allanamiento, por lo tanto, no cabe la posibilidad de que la orden del juez pueda extenderse o ampliarse a otros sistemas que contengan los datos buscados o se encuentren almacenados, sino que en la petición se hará constar por escrito un sistema informático específico y todas las diligencias por practicar.

El juez podrá disponer "incautar y secuestrar los componentes físicos del sistema y, si fuera necesario, los dispositivos para su lectura"; el término incautar hace referencia a los bienes que posiblemente hayan sido adquiridos fruto de una actividad ilícita; el secuestro tiene la finalidad de que, de manera provisional, se preserve el bien hasta que la autoridad competente tome una decisión (Constante, 2018); en este caso se puede ordenar el secuestro como una medida para la preservación de los datos; esta orden debe concederse siempre y cuando los mismos tengan relación con los hechos que se investigan, garantizando además que se hagan responsables de estos componentes personas que conozcan de su funcionamiento para proteger los datos informáticos que se buscan.

No se debe olvidar que el numeral 17 del artículo 444 (COIP) dispone que para realizar los allanamientos el fiscal solicitará al juez la orden para la preservación de la evidencia digital de los dispositivos de interés para la investigación o el proceso que se encuentren en la escena, los cuales se guardarán con cadena de custodia.

También puede ordenar "hacer u obtener copia íntegra de los datos en cualquier medio de almacenamiento autónomo disponible", entendiéndose esto como un respaldo, porque pueden tener valor para una investigación penal, más aun en consideración de que este tipo de evidencias son volátiles.

"Acciones que permitan hacer inaccesibles los datos informáticos o eliminar los mismos"; no se indica en qué supuestos, pero generalmente esto ordenan los jueces luego de haberse terminado el proceso penal y cuando los dispositivos de almacenamiento deban ser devueltos a sus propietarios, el juez deberá ordenar una acción para que los vuelva inaccesibles o a su vez su eliminación, garantizando que no sean recuperados, tomando en cuenta lo que dispone el artículo 500 del COIP, esto es mediante técnicas digitales forenses.

El COIP no hace alusión en forma específica a las figuras de secuestro de documentos y secuestro de correspondencia epistolar, sino que dentro de las actuaciones especiales en su artículo 475 hace referencia a la retención de correspondencia.

Artículo 477.4.- Sobre la Cooperación Internacional, esta abre paso a que los países ofrezcan una cooperación de manera equitativa para que sean pocas las dificultades que se presenten al momento de requerir esta información, a pesar de ello esta puede traer tanto beneficios como desventajas, esto debido a que se menciona que serán las autoridades nacionales competentes quienes tienen la *obligación* de preservar y divulgar el contenido digital y al hablar de una obligación es pertinente aludir que se debe regular con mayor cuidado esta temática para que no se vea afectada la soberanía frente a exigencias de otros países.

De acuerdo al artículo 66 contemplado en la Constitución (CRE, Registro Oficial 449, 20-oct, 2008) el Ecuador es un Estado soberano, la soberanía radica en el pueblo y su voluntad es el fundamento de la autoridad. La soberanía según Jean Bodin "es el poder absoluto y perpetuo de una república", se refiere a la capacidad que tiene un Estado para tomar decisiones propias y ejercer su autoridad sobre su territorio sin que exista interferencia de un tercero. Puede verse afectada si se adoptan normas que sean contrarias a las dispuestas en nuestro país o si otros países llegaran a imponer ciertas condiciones a cambio de proporcionar información o ciertos datos. Es así que surge la importancia de que se acojan medidas que permitan una cooperación en la que se aborden problemas comunes y que se trabaje en conjunto con otros países, que a su vez la soberanía se vea respetada y se protejan los datos que serán suministrados por dicho país.

De otro lado, por el principio de taxatividad se debe describir los delitos para los cuales cabría la cooperación internacional, ya que de la forma como está narrado no se sabe si es exclusivo para los delitos informáticos o también para aquellos en los que las tecnologías de la información sean el medio para su comisión.

En todo caso se expresa el compromiso que deben tener las autoridades del país de prestar ayuda a sus similares en la investigación o procedimientos relativos a la ciberdelincuencia.

Artículo 477.5.- Trata sobre las reglas para la preservación y divulgación expedita de contenido digital en la cooperación internacional (COIP, 2014). Al hablar de expedita se está indicando celeridad, rapidez, es decir, que para la preservación y divulgación del contenido digital se lo debe hacer sin poner obstáculos ni trabas, sino de manera inmediata cuando lo ha requerido la autoridad extranjera, pero si respetando que no se violenten derechos.

La solicitud de preservación de contenido digital almacenada en un sistema informático que esté ubicado en nuestro país se lo realizará por cualquier vía de comunicación. Lo que es la divulgación se la realizará previa solicitud de asistencia penal internacional; cuando se reciba

una solicitud internacional de preservación de contenido digital, Fiscalía, que es la autoridad competente, dará la orden a quien tenga el control o disponibilidad de este contenido; mientras que para la ejecución de una solicitud de asistencia penal internacional de divulgación, la autoridad judicial será la que de la respectiva orden a quien tenga el control o disponibilidad de ese contenido.

La orden de preservación especificará la naturaleza del contenido digital, el tiempo de preservación del contenido que será por el tiempo de noventa días prorrogables por igual periodo.

El contenido digital preservado y divulgado se podrá poner en conocimiento de la o el fiscal a cargo de la solicitud de asistencia penal internacional o a la autoridad nacional que emitió la orden de preservación. El cumplimiento de estas reglas está condicionada a que nuestro país mantenga acuerdos de cooperación con el solicitante.

Artículo 477.6.- la solicitud de preservación o divulgación de contenido digital será denegada cuando haga referencia a un delito político o similar a este, de conformidad con la legislación ecuatoriana y cuando atente contra la soberanía, seguridad, orden público u otros intereses del Ecuador.

Es decir, la colaboración que va a mantener el Ecuador con la comunidad internacional es exclusivamente en la lucha contra la ciberdelincuencia o la delincuencia transnacional organizada.

Artículo 477.7.- Trata de la facultad que tiene el juez, siempre a pedido del fiscal, en la ejecución de una solicitud de autoridad extranjera, de disponer la búsqueda, el registro, acceso, secuestro del contenido digital así como la divulgación de contenido almacenado en un sistema informático, cuando se trate de situaciones en que el registro y/o secuestro son admisibles en un caso nacional (COIP, 2014); debe realizárselo con la debida diligencia en razón de la vulnerabilidad de este tipo de información ya que tiende a perderse o a modificarse.

De igual forma, estas actuaciones están condicionadas a la existencia de un instrumento internacional aplicable.

Artículo 477.8.- En lo que respecta al acceso transfronterizo a contenido digital de acceso público o con consentimiento se plantea una discusión al otorgarse a las autoridades extranjeras competentes la facultad para que accedan a contenido digital almacenado en un sistema informático sin previa petición a las autoridades del Ecuador o con el consentimiento legal y

voluntario de la persona legalmente autorizada para revelarlos. El acceso transfronterizo de igual manera debe contener una adecuada regulación que no de paso a situaciones en las que se vea vulnerado el derecho a la intimidad, como es el caso de la vigilancia gubernamental en las que los gobiernos pueden controlar las comunicaciones de las personas, pueden presentarse casos en los que las personas sean susceptibles de robo de datos personales al momento de acceder a este contenido digital e incluso la normativa sobre protección de datos personales puede ser contraria a la que dispone nuestro país y esto puede traer consigo efectos negativos. Al ser el Ecuador un país soberano y permitirse que un extranjero libremente acceda a un sistema informático ubicado en su territorio, sin la autorización correspondiente, puede afectar la soberanía.

Artículo 477.9.- Punto permanente de contacto para la colaboración internacional.- Para estos efectos el Ecuador mantendrá una estructura que garantice un punto de contacto disponible en todo momento, las veinticuatro horas del día, los siete días de la semana.

Recibiendo las orientaciones del Convenio de Budapest (2001), la mayoría de los países miembros y los que se han adherido mantienen estas estructuras para la cooperación, lo importante es que se rompan los trámites burocráticos que anteriormente se daban en los exhortos o en la asistencia penal internacional en que por regla general de un lugar determinado se solicitaba este tipo de asistencia al responsable de una provincia, este a su vez remitía la petición al responsable del país, quien a su vez remitía al responsable del país al cual se requiere la información y este a la autoridad competente y los resultados eran remitidos de la misma forma, habiendo retardo en la colaboración; la asistencia inmediata que ofrecen los puntos de contacto incluyen:

1. La prestación de asesoramiento técnico a otros puntos de contacto, por lo que desde ya deben ser personas capacitadas en informática como en la parte legal
2. La preservación expedita de contenido digital
3. La recopilación de la evidencia digital para evitar su manipulación o pérdida
4. La localización de sospechosos y el suministro de información de carácter jurídicos, en casos de urgencia o de peligro en el retraso; y,
5. La transmisión inmediata a la autoridad judicial competente de las solicitudes referentes a medidas de la competencia. (COIP, 2014)

Si se cumplen a cabalidad estas acciones se tendrán resultados positivos en la investigación y confianza del requirente, ya que una de las causas por las que ha perdido credibilidad la

administración de justicia es la demora en la tramitación, existiendo falta de seguridad en nuestra sociedad de que esto se pueda realizar.

Artículo 477. 10.- La interceptación de datos informáticos la ordena el juez previa solicitud totalmente motivada por el fiscal, es decir, justificando su necesidad, cuando existan indicios relevantes para la investigación y se justifique que la medida es idónea y necesaria para una investigación que se desarrolle en el país extranjero.

Nuestro país podrá ejecutar este tipo de peticiones si así lo prevé un acuerdo, tratado o convenio internacional o si se trata de situaciones en que dicha interceptación esté permitida en un caso nacional de características similares. La autoridad judicial determinará el tiempo de interceptación con los límites y garantías establecidas en el COIP y en la Constitución de la República (COIP, 2014).

Artículo 483.1.- En lo que respecta al agente encubierto, este debe ser designado para casos concretos. Cuando se habla de agente encubierto informático no se describe a una persona física, sino a una identidad virtual, se necesita de la existencia de una cuenta distinta, falsa, suplantada que interactúe y busque penetrarse en una organización delictiva; las personas que cometen delitos no se fían a primera vista y tendrán que verificar con quién están interactuando, va a ser revisada esta cuenta, cuándo fue creada, qué hace, cuántos amigos tiene y sobretodo se le va a exigir que presente la información que tiene, por lo tanto este tipo de trabajos es de mucha responsabilidad.

La reforma permite que el fiscal autorice al personal del Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses realice tareas investigativas ocultando su verdadera identidad, asumiendo identidad supuesta, para lo cual deberán realizar patrullajes o acciones digitales en el ciberespacio (COIP, 2014).

De esto se desprende que con la sola autorización de Fiscalía un agente encubierto informático puede realizar actividades de tipo pasivas como infiltrase en grupos de comunicación sin el consentimiento del titular de los datos, sin provocar. Esta acción no solo va dirigida a sospechosos de delitos sino a cualquier persona, el fin descubrir a quienes han cometido determinado delito o investigar si se están cometiendo delitos; para esto se podrá hacer uso de cualquier medio tecnológico en cualquier sitio; esta facultad de investigar a cualquier persona podría violentar el derecho a la intimidad y al secreto de las comunicaciones porque existirán casos en que un agente encubierto informático pueda acceder a un teléfono inteligente donde la información que se obtenga no solo será la de persona a quien se investiga,

sino también de la demás con las que ha mantenido algún tipo de comunicación, conversaciones que son de carácter privado (Enríquez, 2023).

En este sentido la reforma debe guardar conformidad con lo que dispone el artículo 7 de la Ley Orgánica de Protección de Datos Personales que determina las condiciones para que el tratamiento que se le dé a los datos sea legítimo y lícito y cumpliendo los principios de necesidad, idoneidad y proporcionalidad.

Por otra parte, la reforma no determina las circunstancias en las que se puede autorizar la realización de una investigación con un agente encubierto, por lo que en la parte práctica esto podría responder al criterio del fiscal, de acuerdo a lo que él crea pertinente, dando como resultado en algunos casos que exista negligencia por el desconocimiento de esta temática.

Por naturaleza el ciberespacio es transnacional y esto generará que el especialista del Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses designado para cumplir con estas tareas tenga que acceder a sistemas de información que en ocasiones pueden ser de empresas que se encuentren en el extranjero puesto que la reforma tampoco establece los límites y al hacerlo puede incurrir en el cometimiento de un delito en otro país lo que traerá problemas al Estado, siendo necesario que si el objetivo es ingresar a un sistema ubicado en otro país es que se lo realice mediante convenios que permitan la cooperación internacional también a los agentes encubiertos informáticos, temática que también necesita de una regulación precisa para que no se violente la soberanía.

El COIP indica las facultades que se conceden al agente encubierto informático pero no señala las prohibiciones o límites, como por ejemplo el no provocar delitos, sin ninguna salvedad. Las atribuciones son excesivas, pueden vigilar o realizar patrullajes independientemente de que existan o no indicios delictivos; una vigilancia masiva y general es por sí misma sospechosa de desproporción, origina una percepción de control que obstaculiza el ejercicio de derechos (Fernández, 2016).

Este artículo no guarda coherencia con una de las reglas de las operaciones encubiertas, específicamente la constante en el numeral 3 del artículo 484 del COIP en donde se habla de la figura del agente encubierto persona jurídica, por cuanto solo pueden ser agentes encubiertos miembros del Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses; el COIP no indica en qué circunstancias se puede designar a una persona jurídica ni qué características debe reunir esta para su designación, por lo que considero existió una mala redacción, no puede haber agente encubierto persona jurídica.

Artículo 616.1.- Reglas para la exhibición de contenido digital.- La prueba electrónica se está volviendo común en los procesos jurisdiccionales, es necesaria en razón de las nuevas formas de comisión de delitos, las interacciones de los sujetos se hacen por redes sociales, por dispositivos electrónicos, mensajería instantánea, mediante WhatsApp se intimida, extorsiona, se exigen vacunas, son miles los delitos que se cometen de esta forma, obligando a que para su detección y comprobación se deba realizarlo a través de dispositivos de almacenamiento informático, sistemas informáticos, entre otros; aquí se encontrará la evidencia.

Para que una prueba electrónica sea admisible en un juicio debe cumplir con los requisitos que se exigen para cualquier otro medio de prueba: pertinencia, idoneidad, utilidad, licitud; debe ser aportada bajo los principios de oralidad, contradicción, publicidad, inmediación, así como por los principios de integridad, autenticidad, confidencialidad y claridad.

El contenido digital que pretenda ser incorporado como prueba digital se regirá por las reglas siguientes:

- El contenido digital será almacenado en cualquier elemento óptico o sistema de almacenamiento como discos, cintas, memorias extraíbles, entre otros (COIP, 2014), garantizando su autenticidad, integridad y que fueron extraídos de manera lícita.
- Será exhibido y/o reproducido en su formato original (COIP, 2014), esto en consideración a que en muchas pericias, como en el caso de la extracción de mensajes de WhatsApp, lo que se realiza comúnmente es capturas de pantalla y el perito en una audiencia de juicio únicamente lee o expresa lo que pudo observar, pero no se analiza lo que pasó en ese dispositivo, si existió manipulación, si se eliminaron mensajes, si se observaron los códigos de integridad, lo que se suplía obteniendo una certificación otorgada por Notario
- El perito tendrá que indicar cuáles fueron las técnicas digitales forenses practicadas en su pericia. Existe libertad probatoria pero siempre y cuando se cumpla con las reglas.

La prueba electrónica ofrecida mediante la aportación de un mero documento privado, por ejemplo la impresión directa del equipo de informática particular sin la intervención de fiscalía o personal de criminalística, o solo el pantallazo, puede generar dudas en cuanto a su autenticidad, no genera certeza, por lo que no será valorada por el juzgador. Los jueces aceptarán como prueba estos mensajes si fueron acreditados mediante cualquiera de los dispositivos electrónicos de remisión o recepción o por cualquiera de los servidores implicados (Armenta, 2018). La visualización tendrá mejores efectos que una copia.

En resolución de fecha 03 de febrero de 2020 la Corte Nacional de Justicia resolvió que los mensajes enviados por un medio digital como son los de WhatsApp constituyen documentos electrónicos, siempre y cuando cumplan con los requisitos previstos en la ley, es decir, respecto de la autenticidad del mensaje en cuanto a su origen y el titular de la cuenta que lo emitió.

Tratándose del contenido digital que haya sido obtenido mediante asistencia penal internacional, este debe ingresar de manera inmediata al centro de acopio de evidencias del Sistema Nacional de Investigación Integral, Medicina Legal y Ciencias Forenses, bajo cadena de custodia, para someterse a las respectivas pericias si se cuestiona su autenticidad, después de lo cual serán presentadas en la etapa de juicio (COIP, 2014).

Sección 3. Aplicabilidad de la normativa dispuesta en el Convenio de Budapest referente a la prueba electrónica y lo dispuesto en las reformas al COIP

Convenio de Budapest

Este convenio, suscrito en el año 2001 en Budapest y que entró en vigor desde 2004 busca prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos mediante la cooperación entre los Estados partes del convenio para proteger a la sociedad y combatir la ciberdelincuencia (Consejo de Europa, 2001).

El tratado internacional cuenta con varias disposiciones y medidas que deben adoptarse a nivel nacional para aumentar la eficacia de las técnicas de investigación, de la obtención de la prueba electrónica y de la cooperación internacional.

Son varios los países que en Latinoamérica se han adherido a este convenio, el que les ha permitido de mejor forma el enfrentar el mal de la delincuencia transnacional que se ha dado por el mal uso de la tecnología; sin que el Ecuador lo haya ratificado a pesar de que viene siendo víctima de la ciberdelincuencia.

Segundo Protocolo Adicional

Desde la creación del Convenio de Budapest las tecnologías de la información han evolucionado y junto con ellas se ha generado un aumento significativo en el uso de estas para fines delictivos. Este protocolo tiene como objetivo mejorar y reforzar la cooperación en la

ciberdelincuencia así como la capacidad de los operadores de justicia para obtener pruebas que tienen contenido digital para las investigaciones o procedimientos penales, brindando herramientas como la cooperación directa con proveedores de servicios y registros de internet, medios eficaces para obtener información sobre los abonados y datos de tráfico, o cooperación inmediata en casos de emergencia y de investigaciones conjuntas (Consejo de Europa, 2022). Estas herramientas deben garantizar los derechos humanos y la protección de estos datos.

3.1. La aproximación o no de la normativa del Convenio de Budapest a la reforma del 29 de marzo de 2023 del COIP en su parte procesal

La finalidad primordial del Convenio de Budapest ha sido el recomendar a cada país miembro la tipificación de delitos de acuerdo a los avances tecnológicos; establecer procedimientos comunes o eficaces que permitan mejorar la investigación, el procesamiento de quienes han participado en el cometimiento de infracciones en las que ha utilizado para su comisión o para su demostración medios informáticos; y sobre todo el contar con mecanismos rápidos y eficaces de cooperación internacional.

Ya en la parte procesal el Convenio describe normas de procedimiento que los países miembros deben incorporar con el objetivo de facilitar la investigación penal tanto de los delitos que cada país ha tipificado como infracciones, así como también para la obtención de las pruebas digitales relativas a cualquier delito sin que estas recomendaciones sean una camisa de fuerza, pues el convenio permite que cada país pueda mejorar los procedimientos tendientes a este objetivo.

Nuestro entorno es digital y ahora se cuenta con nuevas formas para comunicarse, estas son el resultado del desarrollo de la tecnología y del uso del internet. Entre las más comunes se encuentran las redes sociales como Facebook, Twitter, Instagram en las que constantemente se comparte una gran cantidad de información como fotos y videos personales, noticias, artículos, sirven como una herramienta de trabajo en la que se promocionan productos, ofertas de empleo. Otra forma de comunicación es la mensajería instantánea que incluye aplicaciones como WhatsApp que en Ecuador es una de las más usadas; esto nos ha obligado a adquirir dispositivos electrónicos y a su vez esto se ha convertido en un instrumento para cometer delitos. A continuación se presentan valores proporcionados por el Instituto Nacional de Estadísticas y Censos hasta julio de 2022.

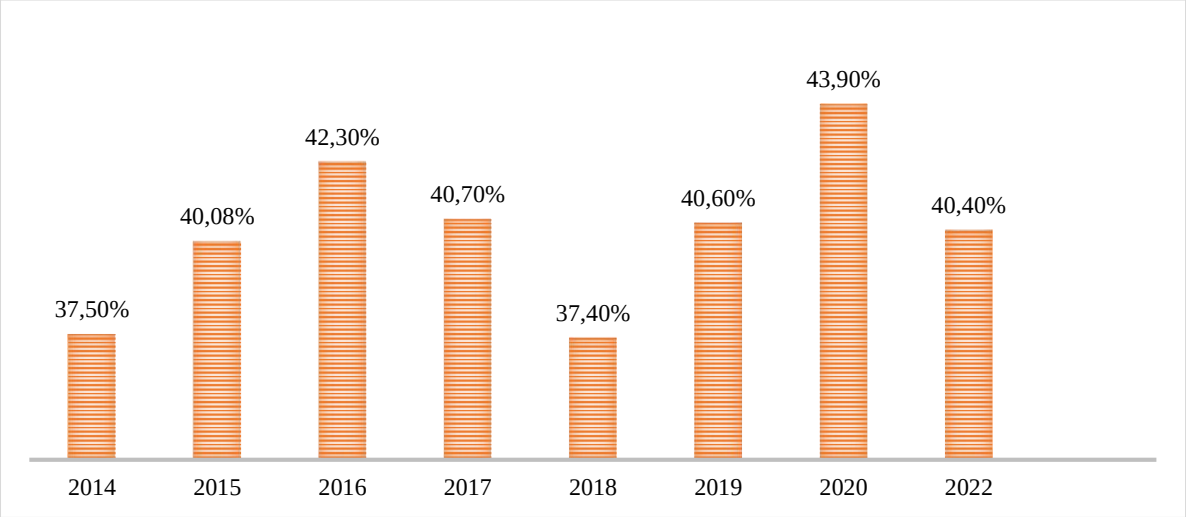

Figura 1: Equipamiento tecnológico del hogar Nacional. Fuente: INEC (2022)

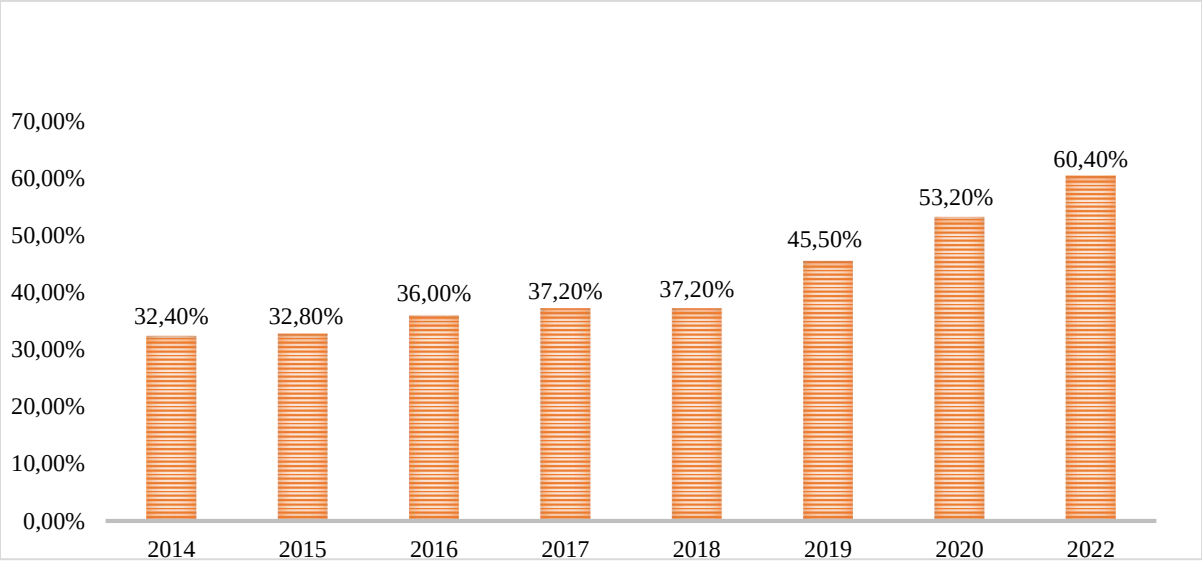

Figura 2. Hogares con acceso a internet. Fuente INEC (2022)

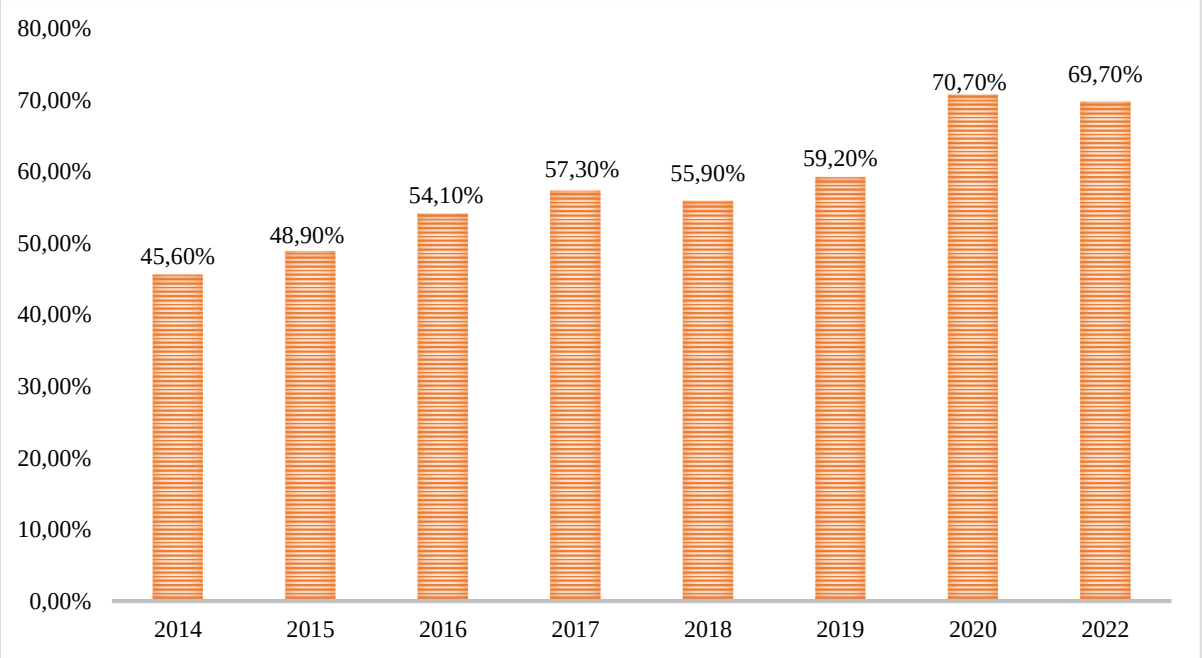

Figura 3. Porcentaje de personas que utilizan internet. Fuente INEC (2022)

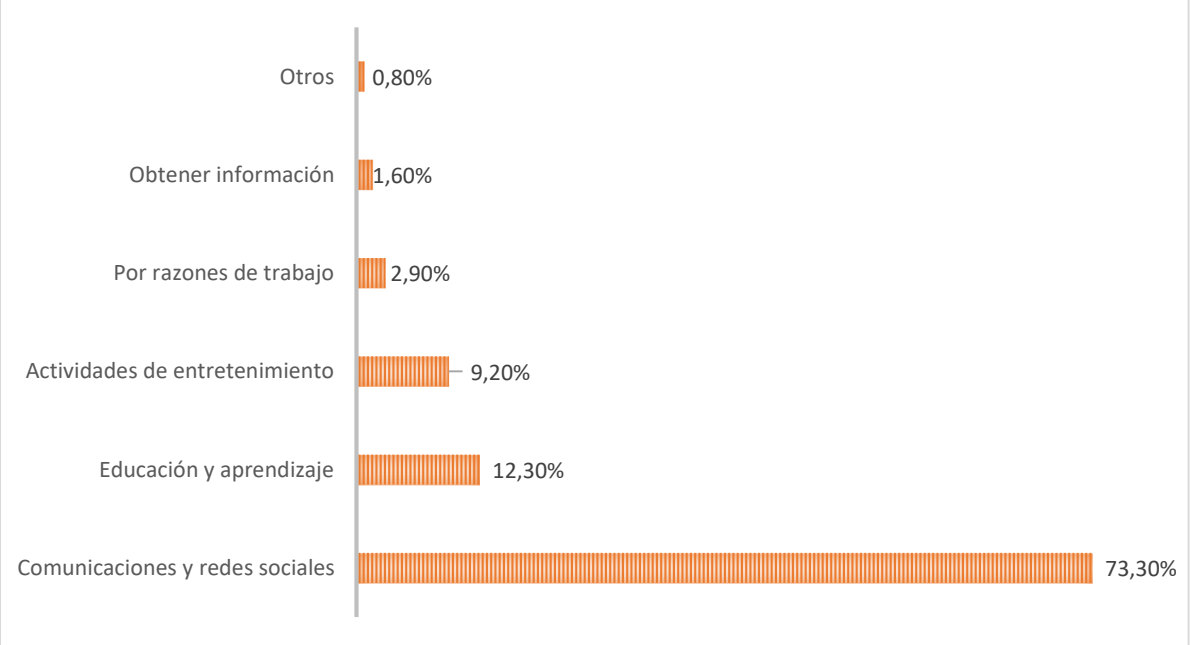

Figura 4. Uso de internet: Servicios y/o actividades. Fuente INEC (2022)

En las figuras se puede observar cómo en los últimos años ha ido incrementando el uso de internet, un gran porcentaje es destinado a las comunicaciones y redes sociales por lo que también se ve el aumento de dispositivos como computadoras, laptops, celulares y tablets.

De igual forma se manifiesta que una gran parte de los delitos se cometen utilizando la tecnología como medio y como fin, estos datos expresan la necesidad de que en el país exista una normativa que proporcione las medidas y los procedimientos de cómo debe ser obtenida la prueba electrónica y cómo de ser presentada de forma correcta para que posteriormente en juicio no se presenten inconvenientes que la terminen invalidando, así mismo esta debe regirse por los derechos y principios, pues una información obtenida ilegalmente carece de valor jurídico.

De la revisión de la normativa constante en las reformas al COIP, específicamente en las actuaciones especiales relativas a contenido digital, se puede manifestar que para su creación se ha observado las recomendaciones que se hace en el Convenio de Budapest, ya que los procedimientos a adoptarse son los que son replicados en los países suscriptores y adherentes y los que les ha permitido de manera más técnica y eficaz combatir los delitos informáticos y cuyo análisis ya se lo ha realizado. Faltando por incorporarse figuras como la vigilancia electrónica que tiene el objetivo de prevenir la comisión de delitos y que no ha sido desarrollada en las reformas.

3.2 ¿Debe Ecuador formar parte del Convenio de Budapest?

El Ecuador ha sido uno de los países que más ciberataques ha recibido en la región, sin embargo, no cuenta con la mayoría de los estándares internacionales que le permitirían enfrentar este problema. Según datos de Kaspersky Lab en su informe de amenazas en tiempo real, en junio del año 2017, Ecuador ocupó en América del Sur el primer lugar con el 2,8 % y el quinto lugar a nivel mundial en cuanto a ciberataques a sus redes. El 49,05 % de estos fueron ocasionados por ataques de fuerza bruta servidores de RDP. El ciberataque es uno de los delitos informáticos que más se ha incrementado desde el 2005, el robo de información y la afectación a instituciones públicas y privadas son los resultados más trascendentales de los ataques cibernéticos (Comisión de Soberanía, Integración y Seguridad Integral, 2023).

Estos datos justifican el hecho de que nuestro país haya trasladado la normativa del Convenio de Budapest a nuestro Código Orgánico Integral Penal, con la finalidad de hacer frente a los delitos informáticos y de contar con un procedimiento para combatir los mismos y así no exista impunidad. Si bien esta temática aún es bastante desconocida, novedosa, debemos empezar a aplicarla por constituir la mejor herramienta para utilizarla contra la ciberdelincuencia, por lo que resulta importante tener una normativa específica, clara y

detallada sobre la prueba electrónica que esté acorde a la Constitución, a lo que disponen los instrumentos internacionales y a la ley.

En una entrevista con el Cap. de policía Carlos Osorio, señaló que son contados los profesionales que están capacitados sobre la prueba electrónica, por lo que falta capacitación de todos quienes integran el sistema de justicia; adicional manifestó que en el campo forense se requiere de un licenciamiento y existen limitaciones por los costos que son elevados, por lo que se necesita contar con una tecnología actualizada y con licenciamientos de última como son los Premium, siendo esta también una debilidad que presenta nuestro país para la investigación.

Por lo expuesto, resulta importante y recomendable que el Ecuador se adhiera al Convenio de Budapest que es el primer tratado internacional que hace frente a todas las actividades delictivas que son cometidas a través de medios informáticos, permite que todos los Estados miembros armonicen sus leyes para mejorar la cooperación internacional debido a que esta es la que permite combatir los delitos informáticos que en muchas ocasiones los medios empleados o los propios atacantes pueden encontrarse en países distintos o los resultados de los delitos se producen en otros Estados.

El convenio aborda varios delitos cibernéticos como acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines; al adherirse al convenio los Estados miembros se comprometen a implementar medidas para prevenir y para combatir estos delitos lo que traería como resultado que se aborde de manera más eficiente los desafíos que trae la ciberdelincuencia como producto del mal uso de la tecnología, el combate de la ciberdelincuencia ya no sería exclusiva del país, sino de todos los asociados.

Conclusiones y recomendaciones

Conclusiones

- El Ecuador siempre ha reaccionado con lentitud normativamente frente a los avances tecnológicos y nuevas formas de comisión de delitos, esto ha generado el crecimiento de la delincuencia e inseguridad para sus habitantes.

- Es a partir de la reforma de fecha 29 de marzo del año 2023 que cuenta con una base normativa sobre la prueba electrónica la que le permitirá materializar el derecho sustantivo, no solo los ciberdelitos, sino aquellos que pueden ser demostrados a base de pericias informáticas.
- En el Código Orgánico Integral Penal no existe un apartado específico para la prueba electrónica, la prueba documental la subsume; las actuaciones especiales relativas a contenido digital se encuentra dentro de las actuaciones especiales de investigación.
- Al desarrollarnos en un entorno digital, la prueba electrónica es la base para la investigación y posterior demostración de un hecho dentro de un juicio penal.
- Las reformas al Código Orgánico Integral Penal referentes a actuaciones especiales relativas a contenido digital son el complemento de las normas establecidas en el artículo 500 ibídem, lo que permitirá su mejor aplicación en la investigación y probanza de delitos cometidos con dispositivos electrónicos como medio y como fin.
- Las actuaciones especiales relativas a contenido digital deben ser cumplidas y observadas a cabalidad y en forma estricta al momento de asegurar o buscar datos informáticos, su incumplimiento puede causar riesgos de que se violenten derechos constitucionales como la intimidad, el secreto de las comunicaciones y la protección de datos personales.
- Se ha otorgado al agente encubierto varias facultades, pueden realizar vigilancias, patrullajes, investigaciones, por lo que la persona que sea designada tiene que ser calificada y contar con formación amplia en sistemas informáticos, ética al hacking, conocimientos jurídicos, sobre todo que posea valores para no agredir derechos fundamentales.
- Al ser el Ecuador uno de los países que más ciberataques ha recibido en los últimos años necesita de la cooperación internacional para enfrentar esta problemática, siendo indispensable que forme parte del Convenio de Budapest.

Recomendaciones

- El cambio de la cultura jurídica, el uso de la tecnología lleva consigo el desplazamiento del documento. Los peritos, a pedido de los sujetos procesales, tienen que presentar junto a la pericia electrónica solicitada su respaldo en documentos, se cree todavía en el papel.

- Que el Ecuador se adhiera al Convenio de Budapest ya que los altos índices de delitos informáticos exigen de la cooperación internacional. El suscribirse permitirá contar con un marco normativo consistente fruto de la experiencia de los países miembros para abordar la ciberdelincuencia.
- Capacitaciones para todos los que integran el sistema de justicia, jueces, fiscales, incluido el personal policial, en lo que es la prueba electrónica, ya que en la actualidad es el medio principal para el desarrollo de una investigación y el elemento de convicción para un juicio.
- Creación de puntos permanentes de contacto para la cooperación internacional, que operen en todas las provincias del país, en especial para las fronterizas que son víctimas de extorsión por parte de grupos irregulares de los países vecinos, que esta cumpla con los principios de inmediatez y celeridad.
- Que por el principio de taxatividad se explique en las reformas: contenidos, alcances, detalles o formas de cumplir las acciones que se facultan, así se hace referencia a acciones que permitan hacer inaccesibles los datos informáticos o eliminar los mismos, sin indicar en qué circunstancias, cuándo y cómo hacerlo; la falta de definición genera que sean interpretadas y aplicadas de distinta forma.

Referencia y bibliografía

Armenta, T. (2018). *Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre*. IDP. Revista de Internet, Derecho y Política. Obtenido de https://doi.org/10.7238/idp.v0i27.3149

Asociación por los Derechos Civiles. (2018). *La Convención de Cibercrimen de Budapest y América Latina. Breve guía acerca de su impacto en los derechos y garantías de las personas.* Volumen 1. Buenos Aires, Argentina. Obtenido de 035-la-convencion-de-cibercrimen-de-budapest-y-america-latina-vol-1-03-2018.pdf (adc.org.ar)|

Cabanellas, G. (2006). Diccionario Jurídico Elemental. Edición 2006. (pág. 394). Obtenido de https://unidaddegenerosgg.edomex.gob.mx/sites/unidaddegenerosgg.edomex.gob.mx/files/files/Biblioteca%202022/G%C3%A9nero%2C%20Sociedad%20y%20Justicia/GSJ-11%20Diccionario%20juri%CC%81dico%20elemental.%20Guillermo%20Cabanellas%20de%20Torres.pdf

Calaza, S., & Muinelo, J. (2020). *La digitalización y custodia de la prueba pericial electrónica sobre evidencias virtuales.* La prueba pericial a examen: propuestas de lege ferenda. Obtenido de https://vlex.es/vid/digitalizacion-custodia-prueba-pericial-876405904

Castillero, O. (2017, marzo 17). *¿Cuál es la diferencia entre indicio, prueba y evidencia?* Obtenido de https://psicologiaymente.com/forense/diferencia-indicio-prueba-evidencia.

Chinchay, A., &. Dávila, L. (2015). *Elucidación sobre la prueba preconstituida.* Doctrina Práctica Vol 17.

CIDH. (27 de enero de 2009). Corte Interamericana de Derechos Humanos, Caso Tristán Donoso vs. Panamá. Obtenido de https://www.corteidh.or.cr/docs/casos/articulos/seriec_193_esp.pdf

COIP. (10 de febrero de 2014). *Código Orgánico Integral Penal*. RO. 180 de 10 de febrero de 2014. Obtenido de https://www.lexis.com.ec/biblioteca/coip

Comisión de Soberanía, Integración y Seguridad Integral. (18 de abril de 2023). Ayuda memoria y líneas argumentales

Consejo de Europa. (2001). Convenio Sobre la Ciberdelincuencia. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Consejo de Europa. (2022). *Informe explicativo al Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas.* Obtenido de https://rm.coe.int/1680a83723

Constante, G. (2018). *El secuestro de bienes inmuebles en el nuevo Código Orgánico General de Procesos y el principio de seguridad jurídica.* (Tesis de grado). Universidad Regional Autónoma de los Andes: Ambato, Ecuador. Recuperado de

https://dspace.uniandes.edu.ec/bitstream/123456789/8171/1/TUAEXCOMAB011-2018.pdf

Corte Constitucional del Ecuador, Caso No. 2064-14-EP, 27-enero. (2021). Obtenido de http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOic1MDM5NmI5Ny1hZmFiLTQ1OWEtYWRlMC1jNjdmNzM1NTMzYjAucGRmJ30=

Corte Constitucional del Ecuador, Caso No. 77-16-IN, 27 de enero. (2022). Obtenido de https://www.corteconstitucional.gob.ec/sentencia-77-16-in-22/

Corte Nacional de Justicia. (03 de febrero de 2020). Absolución de consultas. Prueba por medio de documentos electrónicos (WhatsApp). Obtenido de https://www.cortenacional.gob.ec/cnj/images/pdf/consultas_absueltas/No_Penales/Civil/127.pdf

CRE, Registro Oficial 449, 20-oct. (2008, Octubre 1). *Constitución de la República del Ecuador*. Montecristi, Ecuador. Obtenido de https://www.ambiente.gob.ec/wp-content/uploads/downloads/2018/09/Constitucion-de-la-Republica-del-Ecuador.pdf

De Aguilar Gualda, S. (2019). *La Prueba Digital en el proceso judicial: Ámbito civil y penal* (1st ed.). J.M Bosch. https://doi.org/10.2307/j.ctvwcjgj0

Delgado, J. (2018). *Investigación tecnológica y prueba digital en todas las jurisdicciones (2. ª Edición).* Editorial La Ley.

El PAcCTO. Delgado, S., Salt, M., Pinho, C., & Verdelho, P. (2022). *La prueba electrónica en el marco nacional y en el internacional en Latinoamerica.* Obtenido de https://www.elpaccto.eu/wp-content/uploads/2022/08/Publicacion-prueba-electronica-EL-PAcCTO.pdf

Enciclopedia Jurídica Omeba. (2009). Prueba documental. Tomo XXIII, "PRES-RAZO".

Enríquez, L. (2023). *Descifrando el rol del Agente Encubierto Informático.* Universidad Andina Simón Bolívar. Obtenido de https://www.uasb.edu.ec/ciberderechos/2023/04/03/descifrando-el-rol-del-agente-encubierto-informatico/

Espinoza, V. (2022). *Delitos informáticos y nuevas modalidades delictivas.* (págs. 127-137). Lima: Instituto Pacífico.

Fernández, J. (2016). *Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente.* Revista Española de Derecho Constitucional, 108, 93-122. doi:http://dx.doi.org/10.18042/cepc/redc.108.03

Forouzan, B. A. (2013). *Data Communications and Networking*. (5th ed.). McGraw-Hill.

Gaibor, M. (2022). Prueba Documental según el COIP. Universidad Regional Autónoma de los Andes.

Gómez, C, (13 de agosto de 2022). *La prueba electrónica.* [Archivo de video]. Ciclo de conferencias de Actualización Judicial 2019. Obtenido de https://www.youtube.com/watch?v=S2NVDBTaElw

Gozaini, O. (2015). *Pruebas Científicas y Verdad. El mito del razonamiento incuestionable*. Obtenido de http://www.derecho.uba.ar/institucional/deinteres/2015-gozaini-pruebas-cientificas-y-verdad.pdf

INEC. (julio, 2022). *Tecnologías de la información y comunicación.*

Jiménez, C. (2017). *Manual de Derecho Penal Informático.* Lima: Jurista Editores

Jiménez, E. (2000), Derecho Constitucional Argentino. Tomo II. Buenos Aires, Argentina: Editorial Ediar.

LOC. (25 de junio de 2013). *Ley Orgánica de Comunicación.* RO. 3er. S. 22 de 25 de junio de 2013. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2020/01/Ley-Organica-de-Comunicaci%C3%B3n.pdf

LOPDP. (26 de mayo de 2021). *Ley Orgánica de Protección de Datos Personales.* RO. 5to. S. 26 de mayo de 2021. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Montoya, M. (2010). *La informática forense como herramienta para la aplicación de la prueba electrónica.* Revista CES Derecho.

Ortego, F. (2022). *Investigación y prueba digital de los ciberdelitos.* Justicia: revista de derecho procesal, ISSN 0211-7754, N°2, 2022.

Petrone, D. (2014). *Prueba Informática.* Buenos Aires: Didot.

Punguil, J. (16 de julio de 2019). *Validez y eficacia de la prueba electrónica como medio probatorio en los procesos judiciales.* (Tesis de maestría). Universidad Católica Santiago de Guayaquil: Guayaquil, Ecuador.

Real Academia Española. (s.f.). En Diccionario de la lengua española. Recuperado el 27 de marzo, 2023, de https://dle.rae.es/inform%C3%A1tico

Rodríguez, F. (2023). *Tratado de Derecho Procesal Penal Tomo I. Introducción al Derecho Procesal Penal & Principios Fundamentales.* 3ª edición. Quito, Ecuador: Cevallos Editora Jurídica.

Sergi, N. (2018). *Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina – Vol. 3.* Buenos Aires. Obtenido de https://adc.org.ar/wp-content/uploads/2019/06/038-analisis-juridico-de-la-situacion-de-la-evidencia-digital-en-el-proceso-penal-en-argentina-vol-3-04-2018.pdf

Talavera, P. (2021). *La búsqueda de las fuentes de prueba y restricción de derechos fundamentales.* Editorial Instituto Pacífico.

Villalba, A. (21 de febrero de 2021). *Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa*. Revista de Derecho. Obtenido de https://revistas.uasb.edu.ec/index.php/foro/article/view/499/2417

Anexos

Entrevista

Entrevistado	Organización	Fecha
Cap. Carlos Osorio	Servidor Policial Directivo de la Jefatura Zonal del Distrito Metropolitano de Quito, con la función de perito informático forense.	28 de abril de 2023

A continuación, se realiza un seguimiento y recopilación con las respuestas obtenidas en la entrevista realizada.

El Cap. Carlos Osorio como perito informático forense precisó sobre la falta de capacitación existente en los miembros del sistema de justicia, así como la necesidad de contar con tecnología actualizada y licenciamientos de última para las pericias que se requieren para este tipo de pruebas.