INSTITUTO
DE ALTOS ESTUDIOS
NACIONALES
LA UNIVERSIDAD
DE POSGRADO
DEL ESTADO

INSTITUTO DE ALTOS ESTUDIOS NACIONALES – IAEN

CENTRO ACADÉMICO DE DERECHO Y JUSTICIA

MAESTRÍA DE DERECHO CON MENCIÓN EN ESTUDIOS JUDICIALES

TITULO

FACTORES QUE CONTRIBUYEN Y EFECTOS QUE EMERGEN DE LA CADUCIDAD DE LOS PROCESOS JUDICIALES DEL TIPO PENAL "INTERCEPTACIÓN ILEGAL DE DATOS"

AUTORA:

AB. SONIA MARÍA PAZMIÑO MONTERO

TUTOR:

DRA. NATALIA MORA

Quito – Ecuador

Agosto 2017

INSTITUTO
DE ALTOS ESTUDIOS
NACIONALES
LA UNIVERSIDAD
DE POSGRADO
DEL ESTADO

AUTORÍA

Yo, Sonia María Pazmiño Montero, con C. C. 0601891021 , declaro que las ideas, juicios, valoraciones, interpretaciones, consultas bibliográficas, definiciones y conceptualizaciones expuestas en el presente trabajo, así como los procedimientos y herramientas utilizadas en la investigación, son de mi responsabilidad. Asimismo, me acojo a los reglamentos internos del IAEN correspondientes a los temas de honestidad académica.

Firma

CC: 060189102

INSTITUTO
DE ALTOS ESTUDIOS
NACIONALES
LA UNIVERSIDAD
DE POSGRADO
DEL ESTADO

AUTORIZACiÓN DE PUBLICACiÓN

Autorizo al Instituto de Altos Estudios Nacionales (IAEN) la publicación de esta Artículo Científico "FACTORES QUE CONTRIBUYEN Y EFECTOS QUE EMERGEN DE LA CADUCIDAD DE LOS PROCESOS JUDICIALES DEL TIPO PENAL "INTERCEPTACIÓN ILEGAL DE DATOS", de su bibliografía y anexos, como artículo en publicaciones para lectura seleccionada o fuente de investigación, siempre dando a conocer el nombre del autor y respetando la propiedad intelectual del mismo.

Quito, agosto 2017

Ab. Sonia M. Pazmiño Montero

0601891021

INSTITUTO
DE ALTOS ESTUDIOS
NACIONALES
LA UNIVERSIDAD
DE POSGRADO
DEL ESTADO

DOCENTE TUTORA DE LA MAESTRÍA EN DERECHO CON MENCIÓN EN ESTUDIOS JUDICIALES

CERTIFICA:

QUE EL ARTÍCULO CIENTÍFICO: "FACTORES QUE CONTRIBUYEN Y EFECTOS QUE EMERGEN DE LA CADUCIDAD DE LOS PROCESOS JUDICIALES DEL TIPO PENAL "INTERCEPTACIÓN ILEGAL DE DATOS"; DE AUTORÍA DE LA AB. SONIA MARÍA PAZMIÑO MONTERO, ESTUDIANTE DE LA MAESTRÍA DE DERECHO CON MENCIÓN EN ESTUDIOS JUDICIALES, HA SIDO REVISADO, ASESORADO EN TODAS SUS PARTES DE ACUERDO A LO NORMADO POR EL INSTITUTO DE ALTOS ESTUDIOS NACIONALES, POR LO QUE AUTORIZO SU PRESENTACIÓN Y SUSTENTACIÓN ANTE LAS INSTANCIAS CORRESPONDIENTES.

Quito, agosto del 2017.

Atentamente,

Dra. Natalia Mora

DOCENTE DEL IAEN

RESUMEN

El tema del presente artículo es harto complejo por tratarse de un delito internacional que abarca nuevas formas de delincuencia común y organizada que pone en riesgo la información privada posiblemente en situaciones fuera de la ética, la moral y la legalidad, partiendo de la lesión que se podría dar a la información (datos informáticos) como bien jurídico protegido, utilizando para ello el internet como medio de comisión del delito.

En el caso de nuestra legislación, en el artículo 29 del Código Orgánico Integral Penal, contempla la incorporación de valores inmateriales como bienes jurídicos protegidos, la información es uno de ellos ya sea como un valor económico o un valor intrínseco de la persona por su fluidez y tráfico jurídico.

Estos actos delictivos presentan grandes dificultades para su comprobación que en su mayoría son dolosos y a pesar de ser denunciados en la Fiscalía General del Estado, no pueden llegar a ser judicializados debido principalmente a la falta de capacitación o especialización del personal encargado de la procuración, administración e impartición de la justicia en materia informática, la falta de colaboración de otros países en lo que a asistencias internacionales concierne, contribuyendo de esta manera a la caducidad, por ende al atropello los derechos del titular del bien jurídico protegido.

Este quizá es el patrón factico que nos estaría llevando a la no judicialización del delito informático de *interceptación ilegal de datos*, dando lugar a la afectación de ciertos derechos de los ciudadanos como es la reserva o intimidad y confidencialidad de los datos, la fiabilidad del tráfico jurídico y probatorio, el derecho de propiedad.

En la provincia de Pichincha, si bien existen alrededor de 74 denuncias en la fiscalía por el delito de interceptación ilegal de datos, a partir de la fecha que entró en vigencia el COIP (setiembre 2014) hasta diciembre de 2016, todas permanecen en la etapa de investigación según registros y estadísticas de la Fiscalía General del Estado; es decir, no existe sentencia ejecutoriada alguna.

Esta investigación se propone determinar los factores que contribuyen a la caducidad de los procesos judiciales del tipo penal *interceptación ilegal de datos*, los efectos que acarrea la falta de su judicialización y los hechos caóticos y confusos en cuanto a la praxis normativa jurisprudencial en la provincia de Pichincha de la República del Ecuador desde que entro en vigencia el COIP hasta diciembre 2016.

ABSTRACT

The subject of this article is very complicated because it is an international crime that covers new forms of common and organized crime that puts at risk private information, security in the navigation of the internet, using such information in situations outside of ethics, moral And legal.

In the case of our legislation (COIP, Art. 29), information, as a protected legal right, contemplates the incorporation of immaterial values such as information itself; Considered in different forms, either as an economic value or as an intrinsic value of the person because of its fluidity and legal traffic.

The crime of illegal interception of data is contained in article 230 of COIP, it punishes with three to five years imprisonment for those who use this data and disseminate it.

These criminal acts, despite being denounced in the Attorney General's Office, can not be prosecuted due to the lack of training or specialization of personnel in charge of procurement, administration and administration of justice in computer science, lack Of collaboration of other countries in what has international assistance concerns, thus contributing to the expiration, therefore to violate the rights of the owner of the protected legal good.

This is perhaps the factual pattern that would lead us to the non-judicialization of computer crime of illegal interception of data, resulting in the affectation of certain rights of citizens such as reservation or privacy and confidentiality of data, reliability of traffic Legal and probative, the right to property.

In our country and specifically in the province of Pichincha, although there are about 74 complaints in the public prosecutor's office for the crime of illegal interception of data, from the date COIP (September 2014) entered into force until December 2016, All are in the research stage according to records and statistics of the Attorney General's Office; That is, there is no enforced judgment.

This investigation intends to determine the factors that contribute to the expiration of the judicial processes of the criminal type illegal interception of data in the province of Pichincha from the validity of the COIP until December 2015 and to analyze the effects that entails the lack of its judicialization.

PALABRAS CLAVE

No judicialización del delito informático *interceptación ilegal de datos*

INSTITUTO
DE ALTOS ESTUDIOS
NACIONALES
LA UNIVERSIDAD
DE POSGRADO
DEL ESTADO

Contenido

INTRODUCCIÓN

El desarrollo del presente Artículo Científico además de brindar una ilustración, crítica y analítica de la procuración y administración de la justicia en materia de delito informático "interceptación ilegal de datos", pretende demostrar cuántos casos por este tipo penal han sido o no judicializados, qué factores han contribuido a su caducidad y la afectación causada por este motivo a ciertos derechos de los ciudadanos.

En nuestra legislación, la penalización de esta conducta es aplicada en el marco del principio de lesividad. Al ser un trabajo eminentemente penal se pretende abordar aspectos en la investigación establecidos en las etapas pre procesal y procesal del Código Orgánico Integral Penal - COIP a través de la ejecución de la justicia ordinaria en todas sus instancias. Así mismo se busca determinar la relevancia de la intervención de la Fiscalía General del Estado e inclusive de los jueces, en su contexto y competencia, como agentes administradores de la justicia y el papel que influye por intermedio de sus resoluciones.

En nuestro país existe impunidad de este tipo de delitos y esto se puede explicar por la dificultad que hay en ubicar a nivel internacional a los delincuentes informáticos dispersos en todo el mundo, existe una posibilidad muy grande que el agresor y la víctima estén sujetos a leyes diferentes. Por otro lado, los acuerdos de cooperación internacional remedian algunas infracciones ocasionadas por los delincuentes informáticos, sus posibilidades son limitadas porque en algunos países asiáticos, arábicos o en la India todavía no existe legislación para sancionar esta clase de conducta ilícita.

Esta persecución de «delitos informáticos» en la que se ven involucrados dos o más países se complican enormemente puesto que es necesario hacer uso de los convenios de colaboración suscritos entre ambos países (caso de haberlos).

El derecho generalmente es territorial, esto es, el Estado establece qué conductas son susceptibles de reproche penal y tiene la limitación territorial de sus fronteras, lo que deriva en que, si no existe la conveniente armonización entre las legislaciones de distintos países, lo que es delito en uno de ellos no lo será en el segundo y por lo tanto, no podrá ser perseguido.

Posibles problemas que rodean a la cooperación internacional son los siguientes:

- Falta de acuerdos globales acerca de la tipificación de qué tipo de conductas deben constituirse delitos informáticos.
- Falta de capacitación o especialización de los fiscales y otros funcionarios judiciales en el área informática.
- Ausencia de tratados de extradición y de mecanismos sincronizados que permitan la puesta en vigencia la cooperación internacional.

El presente trabajo investigativo se encuentra plenamente relacionado con las líneas y sublineas de investigación del Centro de Derechos y Justicia del IAEN, el derecho en la cultura jurídica en el Ecuador, *habitus* de los funcionarios públicos, actores jurídicos, uso del derecho y, articulado con el Plan Nacional del Buen Vivir en su objetivo de "*consolidar la transformación de la justicia y fortalecer la seguridad integral, en estricto respeto a los derechos humanos. Garantizar los derechos de la naturaleza y promover la sostenibilidad territorial y global"* (PNBV, 2013- 2017)

El procedimiento a utilizar será la revisión bibliográfica en torno a las dificultades existentes en relación con la investigación del delito informático, que permitirá construir un escenario teórico para un análisis jurisprudencial. En la investigación del presente artículo, analizaremos los hechos caóticos y confusos en cuanto a la praxis normativa jurisprudencial del delito penal "interceptación ilegal de datos". Para ello, utilizaré el enfoque mixto (cualitativo y cuantitativo), modo jurisprudencial. Es decir, la narración de la problemática, la recolección de datos que me permitirá explorar y analizar cuáles son los factores que impiden la judicialización del delito, para luego probar una teoría o hipótesis que resulte de este estudio. Las técnicas comunes al modo jurisprudencial de investigación para la

aprehensión de los hechos, que aplicaré son las siguientes: (i) la observación jurisprudencial consuetudinaria; (ii) la entrevista jurisprudencia al grupo focal jurisprudencial y social, esto es: a los señores agentes de Criminalística Forense Informático de la Policía Nacional del Distrito Metropolitano de Quito, a los señores Fiscales de la Fiscalía Provincial de Pichincha y a las presuntas víctimas; (iii) la documental jurisprudencial que permitirá construir un escenario teórico y que se encuentran a disposición en la Fiscalía General del Estado. La delimitación espacial de la investigación se fija en las Unidades Especializadas de crimen organizado.

DESARROLLO

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos a saber; un sujeto activo y otro pasivo. Estos, a su vez, pueden ser uno o varias personas naturales o jurídicas, de tal suerte que el bien jurídico protegido será en elemento localizador de los sujetos y de su posición frente al delito, así el titular del bien jurídico lesionado será el sujeto pasivo, "quien puede diferir del sujeto perjudicado, quien eventualmente puede ser un tercero. De otra parte, quien lesionó el bien que se protege a través de la realización del tipo penal será el ofensor o sujeto activo" (Ocurio, 2010, p.14).

La generalización de internet ha supuesto una supresión de fronteras, aunque no de una forma universal para los estamentos policiales y judiciales, las fronteras siguen existiendo. La concepción de los códigos penales tradicionales se basa en la capacidad de los estados para poder ejercitar la persecución de los delitos cometidos dentro de su territorio.

> En lo que tiene que ver con la formulación de pericias informáticas, se advierte un gran problema, cual es la falta de capacitación en el orden técnico-informático de los Fiscales que dirigen la investigación "Es necesario contar no solo con leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los estados para luchar contra la delincuencia informática, sino también con la

> infraestructura tanto técnica como con el recurso humano calificado para hacerle frente a este nuevo tipo de delito transnacional" *(*Acurio, 2010, p. 54*).*

En el mundo de las nuevas tecnologías de la información en el que se circunscriben nuestras pesquisas, se puede llegar en determinadas ocasiones a localizar el ordenador desde el que se realizó la conducta ilícita. Ahora bien, cosa distinta es individualizar al usuario que controlaba la máquina en el momento de cometerse el delito.

Esta dificultad de identificación está dado por varios aspectos que, debidamente combinados entre sí, imposibilitan que se pueda poner nombre y dos apellidos al autor de una conducta, inclusive existen sistemas que facilitan el anonimato permitiendo ocultar o disfrazar una comunicación haciéndola muy difícil de rastrear.

> Estos sistemas pueden haber sido diseñados por sus autores para ocultar la navegación de forma consciente o simplemente consisten en utilizar sistemas informáticos mal configurados a los que se puede tener acceso, y que sirven como trampolines entre los que ir saltando para tratar de despistar a las Autoridades que deseen investigar determinada actividad con la investigación. (Ortiz Márquez José Manuel et al., 2007, pp. 13-15).

> La libertad informática "ya no se trataría, simplemente del derecho a excluir a los demás de un determinado ámbito que el titular considera reservado, y que se protege frente a intromisiones indeseadas, sino de un poder positivo de control sobre la información personal que los demás tienen de cada uno y sobre el uso que hacen de la misma. Ese es el sentido de la llamada libertad informática, habeas data" (González Rus Juan Jose at al., 2007, pp. 32-34).

La Libertad informática, se plantea también como bien jurídico autónomo. El contenido central del mismo vendría dado por el derecho del individuo a decidir qué información personal se podrá difundir sobre él y su familia y el destino de la misma. Se trata de un derecho a la intimidad y tendría que ver fundamentalmente con los peligros que para esta supone el desarrollo de la informática.

Las conductas de los delitos informáticos y cibernéticos.-. "Comprende lo que es la delincuencia que pretende únicamente atentar contra los derechos derivados de los procesos de innovación informática o de gestión de determinados derechos digitales". (De la Mata Barranco Norberto J., 2007, pp. 44-49).

Engloban todas las conductas que sirven para facilitar la actuación delictiva, ya sea de un tercero contra el titular o el beneficiario del sistema, ya sea de éste contra un tercero, que favorecen nuevas formas de ataque a bienes tradicionales o al menos facilitan la extensión de la lesividad, la peligrosidad o la proliferación de los ataques a tales bienes.

Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.- La preocupación grave que por el uso que de internet puedan hacer organizaciones criminales, en particular, a la amenaza de la delincuencia organizada, reclaman medidas legislativas contra este tipo de delincuencia, lo que implica definiciones, tipificaciones y sanciones comunes. "Teniendo en cuenta el marco general descrito que ha presidido el nacimiento de esta normativa, procede concentrarse en el examen de algunos de esos elementos objeto de armonización" (Lerma Esther Morón, 2007, pp. 94-108).

> En relación con la intervención penal en Internet y en las redes de transmisión de datos, se mantienen actualmente dos criterios. Uno, partidario de incorporar a la tutela penal los «nuevos» bienes jurídicos que habrían nacido como consecuencia de la generalización y consolidación de los medios y procedimientos informáticos y que tendrían la suficiente importancia para merecer la intervención penal (González Rus Juan Jose at al., 2007) (Mata y Martín Ricardo M. at al., 2007, pp. 137-141)**.**

Dentro de la gran diversidad de tipos penales de la parte especial del Código Penal aparece la informática como factor que permite el acceso y el manejo de bases de datos con ingentes cantidades de datos, realización de operaciones desde lugares lejanos y no visibles directamente a una gran velocidad y sobre un número potencial de víctimas enorme en muchos casos, siendo más costosa y compleja técnicamente la averiguación del autor y la prueba de los hechos.

> La posibilidad de realizar comportamientos criminales al margen del espacio físico se hace presente con el desarrollo de las nuevas tecnologías, y se crea de este modo una compleja problemática en el ámbito jurisdiccional.
>
> En esta línea, para hacer frente a esta nueva ola de comportamientos atípicos, se hace necesaria la adopción y entrada en vigor de normativas adecuadas indispensable para su prevención, cuya esencia descansa en la cooperación internacional. (Aguilar, 2015, pág. 123).

Estos delitos en comparación con otras tipologías penales que no tienen internet como medio de comisión del delito o de lesión del bien jurídico son más complejos, pues la ubicación es una particularidad relativa a la del ilícito lo cual hace que su persecución más compleja, su característica fundamental del modus radiaría en el anonimato del sujeto activo, pues es más fácil que pase inadvertido.

La delincuencia cibernética constituye uno de los mayores retos de la sociedad actual, objetivo ambicioso si no es por la cooperación y colaboración internacional de diversos organismos gubernamentales y privados.

El patrón fáctico del problema está identificado por el máximo personero de la Fiscalía Provincial de Pichincha Dr. Wilson Toainga, quien expresa que:

> "(…) las investigaciones referentes a los delitos informáticos se realizan de forma técnica y demanda tiempo para establecer la responsabilidad de aquellos que quebrantan la ley sentados frente a un monitor. En el Ecuador existen dificultades durante la investigación de delitos propiciados por el uso de la tecnología, por cuanto la información cruzada a nivel de redes sociales o cuentas de correos electrónicos no se encuentra en el país, los grandes proveedores de las redes sociales y generadores de los sistemas informáticos como Google, Facebook, Yahoo, entre otros, tienen los bancos de datos de sus usuarios en Estados Unidos, y solicitar esa información puede demorar meses (…)". (Ecuador, 2015, p.01).

Cuestiones de jurisdicción y competencia**.-** El carácter transnacional de estos comportamientos delictivos se debe a la facilidad que para el autor supone operar vía internet.

El ciberespacio provoca una relativización de los parámetros espacio temporales característicos del mundo físico. Las fronteras penales se resienten ante la facilidad de su traspaso mediante la Red. En materia de estafa informática desde el territorio de un primer país el sujeto activo de este delito puede incidir en activos situados en un segundo país y colocarlos, a su vez, en un tercer sitio, dando lugar no sólo a problemas de identificación del autor sino de jurisdicción de los Tribunales nacionales.

Tales problemas de jurisdicción internacional pasarán a ser meramente de competencia territorial cuando la actividad y el resultado se produzcan en diferentes lugares de un mismo país.

De acuerdo con el principio de universalidad (art. 23.4 LOPJ) España puede perseguir conductas ilícitas sin tener en cuenta la nacionalidad del autor ni el lugar de comisión del hecho delictivo cuando se trate El problema, como ha señalado Marchena, se plantea por cuanto referirse a delitos que utilizan la Red como instrumento ejecutivo, supone poner el acento en el formato, más que en el bien jurídico cuya defensa se trata de garantizar. La ordenación de delitos sometidos al principio de universalidad presupone un catálogo de bienes jurídicos cuya propia naturaleza impone esa persecución reforzada. Desde este punto de vista, parece claro que no toda ofensa a cualquier bien jurídico, ejecutada aquélla mediante tecnología telemática, podría justificar el acogimiento de un criterio de justicia universal. De ahí que la reformulación del principio de universalidad a partir de un criterio puramente instrumental, supondría un verdadero peligro para la coherencia del sistema de delimitación jurisdiccional. La fijación de los límites jurisdiccionales de un Estado no puede inspirarse en pautas puramente formales, ligadas al modus operandi del autor del delito, sino que exige una atención ponderativa centrada en el bien jurídico afectable por el delito.

Ahora bien, es claro que, sin recurrir al principio de universalidad en su persecución, son muchas las causas que suponen un claro interés supranacional en dificultar la utilización de la red con fines puramente delictivos.

El principio de ubicuidad es válido tanto para determinar el lugar de comisión delictiva tanto a efectos de decidir entre jurisdiccionales nacionales cuanto entre juzgados nacionales de diferentes territorios.

No debe olvidarse que entre el lugar de la acción y el lugar del resultado pueden existir idas y venidas que afecten a los límites jurisdiccionales de otros Estados. La ubicación de los nodos conlleva como efecto ciertos saltos territoriales que podrían plantear la duda acerca de si en cualquiera de los Estados en que se sitúa uno de aquellos, podría también estimarse cometido el delito. No cabe duda de que en esos terceros lugares radica una prueba del delito.

> No parece, sin embargo que la respuesta positiva encuentre fundado apoyo. El recorrido telemático a través del cual discurre el sofisticado medio ejecutivo, no puede aspirar a definir una pretensión de jurisdiccionalidad. Sólo el lugar en el que se despliega la acción y el lugar en el que se ejecuta el resultad o pueden aportar los elementos necesarios para su ponderación. La irrelevancia jurídica de esa ruta telemática a los efectos de afirmar o negar la propia jurisdicción, parece consecuencia obligada de la ausencia de bien jurídico ofendido en los llamados «lugares de tránsito». (Moreno Verdeja Jaime et. al., 2007, pp. 177-226).

El ciberdelito al ser transnacional, conlleva a la persecución al autor o responsable del un delito informático como un problema de tiempo y espacio teniendo en cuenta que el lugar de comisión de estos delitos es el ciberespacio, un lugar donde no hay fronteras físicas, y tratar de encontrar el derecho aplicable y los tribunales competentes entre los estados y aplicar el ius puniendi.

AFECTACIÓN DE DERECHOS CONSTITUCIONALES

Constitución de la República del Ecuador

La Constitución con referencia a algunos de los bienes jurídicos protegidos y los derechos que tiene el sujeto pasivo.

Derecho a la Libertad Art. 66.- Se reconoce y garantizará a las personas:

> "18. El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona
>
> 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.
>
> 20. El derecho a la intimidad personal y familiar.
>
> 21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en 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. Este derecho protege cualquier otro tipo o forma de comunicación". (Constituyente, 2008, Art. 29).

El bien jurídico a la intimidad personal es el derecho a que todo individuo tiene al querer precautelar su información privada y no sea difundida por personas ajenas y a exigir a que no se revele y peor permitir intromisiones en varios aspectos de su vida.

El bien jurídico de la información y la violación a la confidencialidad, es un derecho fundamental.

La importancia de delimitar el bien jurídico protegido, es reconocer el bien jurídico que lesiona el sujeto activo a la víctima en la apropiación ilícita de redes sociales y la información que se encuentre en ella y la vida privada de cada persona afectando al patrimonio al descubrir dentro de los datos claves de cuentas bancarias, y la intimidad de los datos.

La realidad tecnológica que vivimos hoy en día se ha venido desarrollando en este

mundo cada vez más globalizado, el novedoso comportamiento de los delincuentes al delinquir por medio de las computadoras y del internet; viéndose varios bienes jurídicos lesionados por el delito de la apropiación ilícita de redes sociales siendo vulnerados los derechos de una persona víctima del delito.

El bien jurídico protegido de la información contenida en la base de datos de las computadoras es la que está peligrando, se mantiene como algo privado siendo intangible y de mucho valor económico, hablando de las claves para acceder a una cuenta de redes sociales o correo electrónico, banco o contraseña de un computador que contenga secretos profesionales, intelectuales e industriales. Andrés J. Fíjoli Pacheco manifiesta que: "(…) no toda la información merece protección penal, sólo aquellos que revisten una nota de "extrañeidad", cuya naturaleza sea de importancia. Como por ejemplo, los datos personales merecen protección por tener que tutelarse tanto a la intimidad de las personas como a su libertad, seguridad y dignidad." (Disponible en URL: http://www.buscalegis.ufsc.br/revistas/files/anexos/2778-2772-1-PB.html) (12 de noviembre de 2013*)*

 Derecho al P**atrimonio o propiedad privada:** es el ilícito de abuso de confianza, fraude y daño a la propiedad violando el derecho privado lucrando de lo hurtado.

 Derecho a la intimidad: cuando se apoderan y revelan datos difundiendo secretos que pueden poner en dificultades al propietario de los datos guardados en documentos digitales en la computadora es toda conducta típica, antijurídica y culpable que tiene como finalidad la violación de la reserva u obligación de secreto de la información contenida en un sistema de tratamiento de la información. Ejemplo: el espionaje informático, en virtud de lo cual se produce la violación de la reserva o secreto de información de un sistema de tratamiento automatizado de la misma.

 Derecho a la seguridad pública: es toda conducta antijurídica típica y culpable que muestra clara evidencia de peligrosidad e inseguridad hacia las personas o bienes y lesión del bien jurídico protegido.

DELITO INFORMÁTICO "INTERCEPTACIÓN ILEGAL DE DATOS"

La Asamblea Nacional aprobó el Código Orgánico Integral Penal, en segundo debate el último el 17 de noviembre de 2014, y objeción parcial del Presidente de la República el 28 de enero de 2014 y el 3 de febrero de 2014 se envió al Director del Registro Oficial para que se publique en el registro oficial, se imprime el lunes 10 de febrero de 2014 y entró en vigencia el 10 de agosto de 2014.

Se incorporaron más tipificaciones delictivas al Código Orgánico Integral Penal referentes a delitos informáticos, como por ejemplo el siguiente tipo penal materia del presente estudio:

> **"**Artículo 230.- Interceptación ilegal de datos**.-** Será sancionada con pena privativa de libertad de tres a cinco años, la persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. (…) 4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior**".** (COIP, 2014)

ENTIDADES ENCARGADAS DE LA INVESTIGACIÓN

Fiscalía General del Estado

Conforme al Artículo 444 del Código Orgánico Integral Penal COIP., la Fiscalía lleva adelante la investigación de la infracción penal, para lo cual cuenta con el apoyo de la Policía Judicial (Artículo 449 y 500 del COIP.) quienes realizarán la investigación de los delitos de acción pública; en tal virtud, cualquier resultado de dichas investigaciones y pericias, se incorporaran en las etapas pre procesales y procesales como parte de los elementos de convicción.

Ante la investigación de un delito, la policía pueda recabar de los proveedores de servicio de Internet, de compañías telefónicas y cuantos servicios se hallen implicados en la comisión de este delito en concreto aquellos datos necesarios para la identificación del autor.

El sistema especializado integral de investigación, de medicina legal y ciencias forenses contará con el apoyo del organismo especializado de la Policía Nacional y personal civil de investigación, quienes llevarán a cabo las diligencias necesarias para cumplir los fines previstos en este Código, ejecutarán sus tareas bajo la dirección de la Fiscalía y dependerán administrativamente del ministerio del ramo.

La fiscalía encargada de investigar delitos informáticos y, en caso de encontrar elementos de convicción suficientes, acusar ante los jueces de Garantías Penales sobre delito cometidos en contra de garantías y libertades constitucionales es la Fiscalía Especializada en Personas y Garantías haciendo efectiva la tutela judicial de los nuevos tipos penales establecidos en nuestra legislación.

Unidad de Crimen Cibernético de la Policía Nacional del Ecuador.

La Unidad de Crimen Cibernético de la Policía Nacional Investigación del Cibercrimen de la Policía Judicial del Ecuador es la unidad encargada de detectar, investigar y neutralizar las conductas ilícitas en la utilización de las tecnologías de información y comunicación en todas sus formas, mediante herramientas tecnológicas que capture, recupere y preserve la evidencia digital para apoyar el desarrollo de la administración de justicia y garantizar la seguridad. Esta unidad cuenta con 16 efectivos policiales.

Unidad de Criminalística de la Policía Judicial

La Unidad de Criminalística sirve de apoyo a la función judicial con la cadena de

custodia, y trabaja en relaciones conjuntas para prevenir el delito. La unidad se encarga de análisis informático telecomunicaciones.

Peritaje informático

La informática forense nació por la necesidad de auxiliar a la justicia ante los nuevos delitos derivados de la tecnología que violentan los sistemas informáticos, correos electrónicos, redes sociales, etc.

> El FBI plantea un concepto sobre la informática forense (2007) "(…) La informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional" (P. 117).

El objetivo de la informática forense es detectar la vulnerabilidad de la seguridad de los sistemas informáticos, obtener vestigios probatorios para averiguar el origen del ataque, siguiendo las evidencia electrónicas y encontrar las posibles alteraciones, manipulaciones, destrucción de información para poder determinar las actividades realizadas en los equipos.

LEGISLACIÓN O DERECHO COMPARADO

Convenio de Ciber criminalidad de la Unión Europea

Convenio de Budapest promovido por el Consejo de la Unión Europea, Japón y Estados.- Este tratado internacional busca enfrentar los delitos informáticos y los de internet, mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y la cooperación entre las naciones, lo que está en trámite para que Ecuador suscriba este convenio.

El delito informático, su problemática y la cooperación internacional.

La globalización y las transformaciones económicas que la explican han hecho posible la aparición, desarrollo y masificación de las nuevas tecnologías de la información. Paralelamente, el desarrollo tecnológico ha traído de la mano nuevas formas delictuales que tienen por medio o finalidad los sistemas informáticos e Internet. Las peculiaridades de estos nuevos tipos de delitos informáticos, exigen un tratamiento conjunto y coherente, y del mismo modo, su problemática particular involucra a elementos transnacionales, lo que obliga a la utilización de la cooperación internacional para la adopción de medidas globales. Mediante esta técnica es posible lograr una armonización del Derecho sustantivo; así como, en el ámbito procesal, que redunda definitivamente en un alivio de la singular incertidumbre que rodea los tipos ciberdelictuales. Para lograrlo, la cooperación internacional, que se materializa principalmente a través de convenios internacionales, deberá reunir unos requisitos mínimos cualitativos. "El Convenio sobre la Cibercriminalidad del Consejo de Europa, se presenta como la única solución internacional existente para el tratamiento de la cuestión ciberdelictual. A pesar de sus deficiencias, se convierte en una adecuada herramienta para la armonización legislativa interestatal y la lucha contra el ciberdelito (DÍAZ, 2010, p. 169).

Los fiscales asignados a estos delitos carecen de una formación específica en cuanto a conocimientos técnicos y particulares sobre el área de los delitos informáticos, siendo esta una de las principales dificultades, debido a que la unidad especializada del CTI, tiene que hacer un mayor esfuerzo para apoyar a los fiscales designados para la investigación de estos hechos punibles.

> "Acogiéndonos a lo expuesto por el CTI, en cuanto a que los fiscales que han sido signados no tienen la responsabilidad de que no estén capacitados, sino que debería existir una mayor inversión en la capacitación de los mismos y en la creación de fiscales especializados para estos delitos, sujetos con conocimientos técnicos de áreas informáticas y similares, que permitan conjugar el derecho con las tecnologías". Respecto de este resultado puedo sostener que aun en Colombia, nuestros fiscales con

> gran esfuerzo están enfrentando estos flagelos, pues su preparación ha sido progresiva pero no suficiente, muestra de ello es que en Colombia existe un alto índice de impunidad en cuanto a los delitos informáticos, como lo evidencia El periódico el Tiempo (Plan Colombia para la Ciberseguridad, 2014*)* (Montes, 2013, p.13).

FRANCIA

Francia es uno de los Estados que ha regulado con mayor profusión las conductas vinculadas a los abusos informáticos. En 1988, se aprobó la Ley n.º 88-19, de 5 de enero, sobre el fraude informático, en cuya virtud se introdujo, en el Código Penal entonces vigente, el acceso fraudulento a un sistema de tratamiento automático de datos, la alteración indebida de datos, los daños informáticos y la falsificación de documentos informáticos.

En la actualidad, el Código Penal francés de 1992 en vigor desde el 1 de marzo de 1994 ha mantenido básicamente dicha regulación.

Esas conductas se hallan contempladas en un capítulo autónomo, rubricado "De los atentados contra los sistemas de tratamiento automatizado de datos" (Capítulo III), ubicado en el Título II (Otros atentados contra los bienes), del Libro III (Crímenes y delitos contra los bienes).

Las principales novedades del Código Penal de 1992 se cifraron en el incremento de las penas de los diversos delitos, la introducción, en este ámbito, de la responsabilidad de las personas jurídicas y la inclusión de nuevos ilícitos, como, por ejemplo, el delito de tenencia, importación, ofrecimiento, venta o puesta a disposición de instrumentos concebidos específicamente para la comisión de las conductas reguladas en este capítulo.

Así pues, la conducta de acceso ilícito, tipificada en el art. 323-1 CP, establece lo siguiente:

> "El acceso o mantenimiento, fraudulentamente, en todo o en parte de un sistema de tratamiento automatizado de datos se castigará con pena de dos años de cárcel y multa de 30.000 euros.
>
> Cuando como resultado se produzca la supresión o la modificación de datos contenidos en ese sistema o una alteración del funcionamiento del sistema, la pena será de tres años de cárcel y multa de 45.000 euros 28".

Se castiga, pues, la conducta de acceso ilícito y únicamente se exige que el acceso sea fraudulento, entendiéndose por tal cualquier modo de penetración irregular en un sistema automático de datos. Sin embargo, no se requiere ni la presencia de tendencias subjetivas en el ánimo del sujeto ni tampoco la vulneración de especiales medidas de seguridad.

Además, se sanciona la producción de daños contra los datos contenidos en ese sistema o contra el propio sistema al que se accede.

> "En este caso, se sanciona la conducta más gravemente cuando quien lleva a cabo el acceso ocasiona de forma sobrevenida daños sobre los datos o el sistema. Éste parece ser el ámbito de vigencia del art. 323-1, segundo inciso CP, dado que el castigo autónomo de tales conductas, llevadas a cabo de forma intencionada, se prevé en preceptos posteriores" (Lerma Esther Morón, 2007, pp. 85-126).

Procesamiento de la investigación

Los resultados que arrojó la recolección de datos, están representados estadísticamente de forma cuantitativa a través de cuadros estadísticos con porcentajes y cantidades para posteriormente realizar un análisis e interpretación, esto permitirá visualizar los resultados obtenidos (anexos 2 y 3).

CONCLUSIONES

- Luego de haber realizado esta investigación, se detectó un problema socio jurídico real y que persiste en el tiempo. El problema es complejo y las respuestas que se ofrecen tampoco serían simples. El acto delictivo informático interceptación ilegal de datos, a pesar de ser denunciados en la Fiscalía General del Estado, no llega a ser judicializado, debido principalmente a la falta de elementos de convicción y agotamiento del tiempo para la investigación, a la poca o nada colaboración internacional en las etapas pre procesal y procesal contribuyendo a la caducidad y por ende atropellando los derechos del titular del bien jurídico protegido.

- La FGE a través de asistencias internacionales y en base a acuerdos de cooperación internacional, solicita información que pudiera esclarecer la responsabilidad del presunto delincuente informático, pero sus posibilidades son escasas, pues no se pronuncian sobre la persona jurídica ni física del que hubiera cometido la infracción, inclusive en algunos países todavía no existe legislación para sancionar esta clase de conducta ilicitica, hace necesario para dar solución a este problema, se desarrolle un régimen jurídico internacional paralelo, donde se establezcan las normas jurídicas que garanticen la compatibilidad, la armonización entre las legislaciones y aplicación adecuada.

- Se requiere urgentemente capacitar a los tutelares de la acción punible en este tema.

FUENTES BIBLIOGRÁFICAS

Aguilar, M. (2015). *Cibercrimen y cibervictimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido*. *Criminalidad*, 123.

Acurio, S. (14 de 11 de 2011). *Historia de los delitos informaticos.* Obtenido de URL: http://delitosinformaticoslaschecks.blogspot.com/2011/11/historia-de-los-delitos-informaticos.html

Acurio, S. (2011). *Perfil Sobre los Delitos Informáticos en el Ecuador*. Recuperado de http://app. ute. edu. ec/content/3254-42-10-1-6-7/Perfil% 20de% 20los.

Arroyo Jácome, R. P. (2016). *Análisis de los delitos informáticos por ataque y acceso no autorizado a sistemas electrónicos, tipificados en los artículos 232 y 234 del Código Orgánico Integral Penal en el Ecuador*. Recuperado a partir de http://www.dspace.uce.edu.ec/handle/25000/5953.

Cárdenas Aravena, C. (2008). El *lugar de comisión de los denominados ciberdelitos*. Recuperado a partir de http://repositorio.uchile.cl/handle/2250/126580.

De la Mata Barranco Norberto J. (2007). *Conductas que afectan al correcto desarrollo de los contextos* . En L. J. María, *Los cuadernos penales* (págs. 41-81). España: Universidad de Deusto.

Delitos informaticos. (s.f.). Recuperado el 11 de 03 de 2917, de https://es.slideshare.net/osmavences/clasificacin-de-los-delitos-informaticos.

Diaz, A. (2010). *Revista electrónica del departamento de derecho de la Universidad de La Rioja, REDUR.* Recuperado el 25 de 05 de 2016, de https://dialnet.unirioja.es/serviet/revista.

Duncan Ormaza, J. A. (2015). *Falta de aplicabilidad de las normas jurídicas referentes a los delitos informáticos en el Ecuador*. Recuperado a partir de http://www.dspace.uce.edu.ec:8080/handle/25000/5693.

De la Mata Barranco Norberto J. (2007). *Conductas que afectan al correcto desarrollo de los contextos* . En L. J. María, *Los cuadernos penales* (págs. 41-81). España: Universidad de Deusto.

Delitos informaticos. (s.f.). Recuperado el 11 de 03 de 2917, de https://es.slideshare.net/osmavences/clasificacin-de-los-delitos-informaticos

Ecuador, F. G. (13 de 06 de 2015). *Fiscalía General del Estado.- Los delitos informáticos.* Recuperado el 20 de 05 de 2016, de www.fiscalia.gob.ec/.

Espinoza Villamar, J. J., & Verdezoto Acuña, R. G. (2015). *El rol de la auditoría forense ante los nuevos delitos informáticos tipificados en el actual código orgánico integral penal del Ecuador COIP, metodologías y herramientas a usar ante una evidencia digital.* Recuperado a partir de http://www.dspace.ups.edu.ec/handle/123456789/10348.

FGE. (13 de 11 de 2015). *Los delitos informáticos van desde el fraude hasta el espinaje.* Obtenido de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html.

Gamba, J. (2010). *Panorama del derecho informático en América Latina y el Caribe*. Recuperado a partir de http://repositorio.cepal.org/handle/11362/3744.

González Rus Juan Jose at al. (2007). *La intervención penal en internet. En L. J.* María, *Los cuadernos penales* (págs. 13-35). Universidad de Deusto.

HAKER , 008-2013 (02 de 11 de 2013).

Lerma Esther Morón. (2007). *Delitos contra la confidencialidad, integridad* . En L. J. Maria, *Los cuadernos penales* (págs. 85-126). España: Universidad de Deusto.

Mata y Martín Ricardo M. at al. (2007). *Criminalidad informática*. . En L. J. María, *Los cuadernos penales* (págs. 130-171). España: Universidad de Deusto.

Moestre Manuel Viota et el. (2007). Problemas relacionados con la investigación de los denominados delitos informáticos. En J. M. Lidón, *Los cuadros penales* (págs. 238-257). Estaña: Universidad de Duesto.

Montes, B. R. (26 de 05 de 2013). *Retos de la administración de justica frente a los delitos informáticos. Recu*perado el 2016, de http://fiadi.org/wp-content/uploads/2015/08/Rodrigo-Cortes-Borrero.pdf

Moreno Verdeja Jaime et. al. (2007). *Cuestión de jurisdicción y competencia. En L.* J. María, *Los cuadernos penales* (págs. 177-226). España: Universidad de Deusto.

Ortiz Márquez José Manuel et al. (2007). *Problemas relacionados con la investigación de los denominados delitos informáticos* . En L. J. María, *Los cuadernos penales* (págs. 260-300). España: Universidad de Deusto.

Salamea, D. (2012). El Delito *Informático y la Prueba Pericial Informática. Ecuador: Editorial Jurídica del Ecuador*.

Salazar Andrade, O. R. (2008). *Análisis del delito de fraude informática. Editorial Universidad Andina Simón Bolívar Sede Ecuador*.

Santiago, A. (2011). *Perfil sobre los delitos informáticos en el Ecuador-Alfa-Redi: Políticas de la Sociedad de la Información*.

Temperini, M. G. I. (2013). *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado.* 1ra. Parte. En *1er. Congreso Nacional de Ingeniería Informática/Sistemas de Información*. Recuperado a partir de http://conaiisi.unsl.edu.ar/ingles/2013/82-553-1-DR.pdf.

Torres, R., & Xavier, D. (2010). Delitos cometidos a través de sistemas informáticos.

Trejo, C. A., Alvarez, G. A. D., & Chimbo, K. M. O. (2016). La seguridad jurídica frente a los delitos informáticos. *AVANCES*, *10*(12), 41.

Ureta, L. (2009). Retos a Superar en la Administración de Justicia ante los Delitos Informáticos en el Ecuador. *Obtenido de http://www. dspace. espol. edu. ec/bitstream/123456789/5792/5/TESIS*.

Vallejo Delgado, V. E. (2009). *El delito informático en la legislación ecuatoriana*. Recuperado a partir de http://dspace.ucuenca.edu.ec/handle/123456789/17028.

Vallejo, V. (2010). *El Delito Informático en la Legislación Ecuatoriana*. *Ecuador: Corporación de Estudios y Publicaciones*.

Vargas, S. (2011). *Estudio Técnico de la Ciberdelincuencia y su Incidencia en el Ecuador*. UNITA-QUITO.

Villalva Fonseca, D. G. (2011). *La inexistencia de la tipificación de los delitos informáticos en la ley de comercio electrónico. firmas y mensajes de datos vulneran al derecho de propiedad.* Recuperado a partir de http://repo.uta.edu.ec/handle/123456789/4898.

Vizueta Ronquillo, J. (2010). *Delitos Informáticos en el Ecuador*. Guayaquil–Ecuador. Ediciones Edino.

Zambrano-Mendieta, J. E., & Dueñas-Zambrano, K. I. (2016). Delito Informático. Procedimiento Penal en Ecuador. *Dominio de las Ciencias*, *2*(2), 204–215.

ANEXOS

ANEXO 1

DEFINICIONES

Delito informático.-

Delito informático es todo acto o conducta ilícita e ilegal que puede ser considerada como criminal, dirigida a alterar, socavar, destruir o manipular la información depositada en las bases de datos, utilizando para ello cualquier sistema informático teniendo como finalidad poner en peligro un bien jurídico cualquiera que éste fuera.

Sujeto activo

El sujeto activo de esta tipo de infracciones puede ser anónimo y usar este anonimato como forma de evadir su responsabilidad, y a que este no necesariamente puede usar su propio sistema informático, " puede valer de un tercero, como por ejemplo, en el caso del envío de correo no deseado o SPAM, en el cual se puede usar a una maquina zombi, es decir una computadora que está bajo el control del SPAMER y que le permite usarla como una estación de trabajo de su propi a red de m á quinas zombis, las cuales pertenecen a usuarios que no tienen al día sus medidas de seguridad y que son fácil presa de los hackers y crakers para cometer este tipo de infracciones infracciones. También, existen programas de enmascaramiento o que no permiten ver la verdadera dirección ya sea de correo electrónico o del número I P" (Ocurio, 2010, P.15).

Sujeto pasivo

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo, en el caso de los delitos informáticos. "Las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etc., todos aquellos que usan sistemas automatizados de información generalmente conectados a otros.El sujeto

pasivo del delito que nos ocupa, es sumamente importante, pues a través de él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos y su modus operandi" (Ocurio 2010, P.18).

Dolo

Como un conocimiento a los elementos del tipo objetivo y la voluntad de realizarlo, nos referimos a que la persona conoce de todos los elementos y quiera ejecutarlo.

Dolo directo (quiere y lo hace), dolo indirecto (planificación global donde intervienen varias personas), dolo eventual (probabilidad o la representación, se refiere al elemento del conocimiento y voluntad, representado en el conocimiento que lo quiera hacer y y que se representa.

Culpa

Como una falta del deber objetivo de cuidado, la persona tiene un deber objetivo de actuar por medio de reglas, protocolos, la Ley Artix, culpa con representación.

Términos informáticos

Hackers

Hacker nombre en inglés que significa *cortador* y que se les dio esta denominación a los delincuentes interesados en violentar la información con un estilo distinto a los delincuentes comunes hacerlo en silencio y ayudados por la tecnología.

Crackers

Cracker significa *romper* utilizada para referirse a la persona que rompe algún sistema de seguridad. Su objetivo es el de crear virus e introducirlos en otro sistema para dañarlo y en general a causar problemas, esta clase de infractor se subdivide en el que se introduce en un sistema informático y se apropia de la información.

El cracker es aquel individuo que tiene la capacidad para romper sistemas y

difundirlos mediante el internet, y se puede encontrar en el internet de forma fácil y gratuita como romper los software.

Dirección IP

Una dirección IP (internet Protocol, Protocolo de internet) es un conjunto de cuatro números separados por puntos con un valor que puede oscilar entre el 0 y el 255. Suelen adoptar la forma 192.168.12.77.

Estas direcciones IP son imprescindibles para que dos ordenadores o sistemas informáticos se comuniquen en una red. Los ordenador es se identifican entre sí a partir de esa dirección IP, que a la postre se puede asimilar con una dirección física en el mundo real. Por ello, en una red determinada no pueden coincidir dos IPs iguales, en el mismo momento.
Esto es debido a que los ordenadores envían sus informaciones mediante paquetes y utilizan determinados protocolos para esos envíos.

En esos paquetes de información se anotan en sus cabeceras, entre otros datos, las direcciones IP del emisor y del receptor, para que la comunicación pueda llevarse a efecto.

Si en una misma red coexistiesen más de una dirección IP idéntica, no podría discernirse a cuál de las dos se dirigiría un paquete de datos, de la misma forma que un cartero se volvería loco si en la misma calle existiesen dos portales 5 con el mismo número de pisos, y en la carta no constase el nombre del destinatario.

Asignación de direcciones IP

Por su definición, el número de direcciones IP, aunque muy amplio, es limitado y por lo tanto tiene que estar sometido a alguna regulación para que se puedan repartir entre los usuarios de una forma efectiva.

Con este objetivo se creó la IANA (Internet Assigned Numbers Authority), cuyas funciones fueron posteriormente asumidas por la ICANN (Internet Corporation for Assigned Names and Numbers) que se encarga, entre otras cosas, de distribuir las limitadas direcciones IP entre los solicitantes.

Cuando un proveedor de servicios de Internet (PSI) desea establecerse, lo que tiene que hacer es ponerse en contacto con el RIR de su demarcación y solicitarle el número de direcciones IP que necesite para su negocio.

Generalmente hacen una estimación a la baja, alquilando únicamente aquel número de las mismas que puedan ser utilizadas a la vez por sus clientes.

Cuando un usuario perteneciente a este PSI desea «navegar por Internet» su ordenador se pone en contacto con el PSI y le informa (utilizando determinados protocolos) de sus intenciones. El proveedor, tras verificar que se trata de su cliente (mediante usuarios y contraseñas u otros métodos de autenticación) revisa su listado de direcciones IP para ver cuál de ellas está libre. Una vez localizada una disponible se la asigna al cliente.

Hasta el momento en el que el cliente cierre la comunicación esa dirección IP seguirá siendo la misma, identificándole en todos y cada uno de los servicios que utilice en Internet. Una vez finalizada la navegación el cliente devolverá su dirección IP al proveedor, quien la tendrá nuevamente disponible para nuevos clientes.

Según lo visto, es perfectamente factible que una misma dirección IP pueda ser asignada consecutivamente a dos clientes completamente distintos. Por ello la fecha y la hora de asignación de una IP es fundamental de cara a identificar qué ordenador estaba detrás de determinada comunicación

Rastros en internet

Como se ha apuntado anteriormente, cuando un equipo informático realiza cualquier acción en Internet, se identifica mediante su dirección IP, y por lo tanto los distintos servicios que se prestan, desde enviar un correo electrónico hasta consultar una página web pasando por el compartir archivos en las redes P2P, hacen un uso intensivo de esta dirección IP, quedando almacenada en varios lugares de los cuales puede ser recuperada.

El primero de ellos es el PSI, otro las páginas web que se visita, otra son los mensajes de correo electrónico enviados, y así para casi todas las acciones que se lleven a cabo en Internet. Por lo tanto nuestra actividad en la Red deja rastro.

No obstante existen métodos, más o menos sofisticados de soslayar este control o al menos de disfrazarlo de tal forma que su identificación sea costosa. (Moestre Manuel Viota et el., 2007, pp. 238-257).

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

ANEXO 2

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

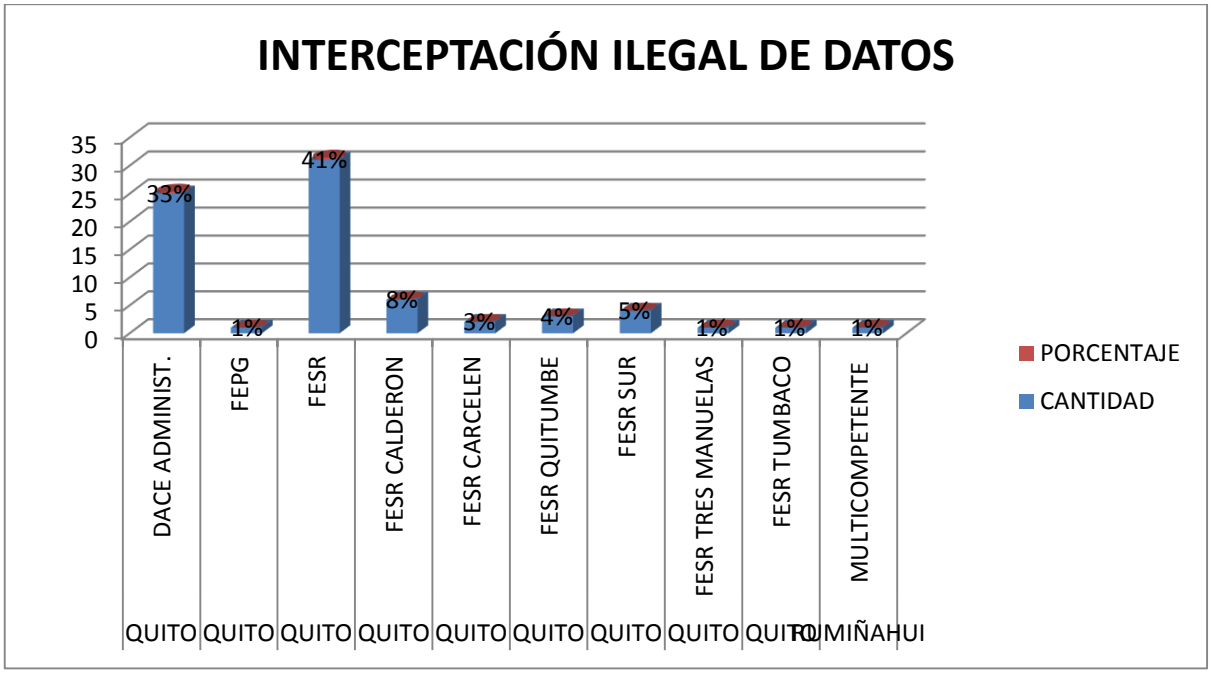
CUADRO DEMOSTRATIVO N ° 1

NUMERO DE CAUSAS POR EL DELITO: INTERCEPTACIÓN ILEGAL DE DATOS QUE MANTIENEN EN LAS DIFERENTES FISCALÍAS

DE AGOSTO 2014 A DICIEMBRE 2016 PROVINCIA DE PICHINCHA

CANTONES	FISCALIAS	DENUNCIAS	PORCENTAJE
QUITO	Fiscalía DACE ADMINIST.	25	33%
QUITO	Fiscalia especializada de personas y garantías	1	1%
QUITO	Fiscalía especializada de soluciones rápidas	31	41%
QUITO	Fiscalía especializada de soluciones rápidas de con sede en CALDERON	6	8%
QUITO	Fiscalía especializada de soluciones rápidas de CARCELEN	2	3%
QUITO	Fiscalía especializada de soluciones rápidas de QUITUMBE	3	4%
QUITO	Fiscalía especializada de soluciones rápidas del SUR de Quito	4	5%
QUITO	Fiscalía especializada de soluciones rápidas TRES MANUELAS (centro de Quito)	1	1%
QUITO	Ffiscalía especializada de soluciones rápidas de TUMBACO	1	1%
RUMIÑAHUI	Fiscalía MULTICOMPETENTE, cantón Rumiñahui	1	1%

FUENTE: GESTIÓN PROCESAL – FGE.
Elaborado por: Ab. Sonia Pazmiño Montero



INTERPRETACIÓN

En el cuadro estadístico se representa las variables: cantones de la provincia de Pichincha, fiscalías especializadas y el número de casos o denuncias que tienen a su haber cada fiscalía.

ANÁLISIS

Se muestra que las fiscalías especializadas a las cuales fueron asignadas la investigación del delito interceptación ilegal de datos, tienen acumulados estos casos en la etapa pre procesal de investigación por falta de elementos de convicción sin poder avanzar a la etapa intermedia de instrucción.

ANEXO 3

CUADRO DEMOSTRATIVO N ° 2

FECHA DE LA DENUNCIA Y TIEMPO TRASCURRIDO A DICIEMBRE 2016

CANTON	FISCALIA	NUMERO DENUNCIA	FECHA INGRESO	Tiempo transcurrido (años)
QUITO	FESR	170101814083663	27/08/14	2 a 7 m
QUITO	FESRQUITUMBE	170101814092429	18/09/14	2 a 6 m
QUITO	FESRCALDERON	170101814093555	19/09/14	2 a 6 m
QUITO	FESR	170101814095414	07/10/14	2 a 6 m
QUITO	FESR	170101814100564	13/10/14	2 a 6 m
QUITO	FESRQUITUMBE	170101814103442	24/10/14	2 a 5 m
QUITO	FESR	170101814100150	12/11/14	2 a 5 m
QUITO	FESR	170101814110864	12/11/14	2 a 5 m
QUITO	FESR	170101814114281	28/11/14	2 a 4 m
QUITO	FESR	170101814114827	04/12/14	2 a 4 m
QUITO	FESR	170101814122666	15/12/14	2 a 3 m
QUITO	FESR	170101814122494	20/12/14	2 a 3 m
QUITO	FESR	170101814122824	20/12/14	2 a 3 m
QUITO	FESR	170101814122496	20/12/14	2 a 3 m
QUITO	FESR	170101814123057	20/12/14	2 a 3 m
QUITO	FESRCALDERON	170101814123667	31/12/14	2 a 3 m
QUITO	FEPG	170101813072437	09/01/15	2 a 3 m
QUITO	FESR	170101815012668	19/01/15	2 a 2 m
QUITO	FESR	170101815014276	28/01/15	2 a 2 m
QUITO	FESRCALDERON	170101814105088	31/01/15	2 a 2 m
QUITO	FESR	170101814092429	02/02/15	2 a 2 m
RUMIÑAHUI	MULTICOMPETENTE	170501815020040	04/02/15	2 a 2 m
QUITO	FESR	170101815023512	19/02/15	2 a 2 m
QUITO	DACE ADMINISTRATIVA	170101815033469	13/03/15	2 a 1 m
QUITO	FESR	170101815033124	23/03/15	2 a 1 m
QUITO	DACE ADMINISTRATIVA	170101815042703	13/04/15	2 a 0 m
QUITO	DACE ADMINISTRATIVA	170101815046302	28/04/15	1 a 11 m
QUITO	DACE ADMINISTRATIVA	170101815055914	28/05/15	1 a 10 m

QUITO	FESR	170101815055469	28/05/15	1 a 10 m
QUITO	FESRCALDERON	170101815065870	01/07/15	1 a 9 m
QUITO	FESR	170101815075133	28/07/15	1 a 8 m
QUITO	DACE ADMINISTRATIVA	170101815080908	05/08/15	1 a 8 m
QUITO	FESR	170101815083391	20/08/15	1 a 7 m
QUITO	FESRCALDERON	170101815080509	01/09/15	1 a 7 m
QUITO	DACE ADMINISTRATIVA	170101815092285	10/09/15	1 a 7 m
QUITO	DACE ADMINISTRATIVA	170101815055469	15/09/15	1 a 6 m
QUITO	DACE ADMINISTRATIVA	170101815103486	27/10/15	1 a 5 m
QUITO	DACE ADMINISTRATIVA	170101815113331	17/11/15	1 a 4 m
QUITO	DACE ADMINISTRATIVA	170101815124210	18/12/15	1 a 3 m
QUITO	FESRCARCELEN	170101815123442	21/12/15	1 a 3 m
QUITO	FESR	170101815080908	22/01/16	1 a 2 m
QUITO	FESRSURORDINARIO	170101816014646	29/01/16	1 a 2 m
QUITO	DACE ADMINISTRATIVA	170101816033028	15/03/16	1 a 1 m
QUITO	FESRSURORDINARIO	170101816032376	15/03/16	1 a 1 m
QUITO	DACE ADMINISTRATIVA	170101816035137	23/03/16	1 a 0 m
QUITO	DACE ADMINISTRATIVA	170101816035137	23/03/16	1 a 0 m
QUITO	FESRVALLEDETUMBACO		23/03/16	1 a 0 m
QUITO	FESR	170101816035137	04/04/16	1 a 0 m
QUITO	FESR	170101816040792	07/04/16	1 a 0 m
QUITO	FESR	170101816040959	07/04/16	1 a 0 m
QUITO	FESR	170101816043728	21/04/16	11 m
QUITO	DACE ADMINISTRATIVA	170101816050629	04/05/16	11 m
QUITO	FESR	170101816051827	11/05/16	11 m
QUITO	DACE ADMINISTRATIVA		12/05/16	11 m
QUITO	FESRSURORDINARIO	170101816054213	20/05/16	10 m
QUITO	DACE ADMINISTRATIVA	170101816061980	10/06/16	10 m
QUITO	FESRCALDERON	170101816064209	26/06/16	9 m
QUITO	DACE ADMINISTRATIVA		11/07/16	9 m
QUITO	FESRQUITUMBE	170101816074637	25/07/16	8 m
QUITO	DACE ADMINISTRATIVA	170101816061513	26/07/16	8 m
QUITO	FESR	170101816074626	26/07/16	8 m
QUITO	FESR	170101816074644	26/07/16	8 m
QUITO	DACE ADMINISTRATIVA	170101816080259	01/08/16	8 m
QUITO	FESR	170101816084784	29/08/16	7 m
QUITO	DACE ADMINISTRATIVA	170101816090092	01/09/16	7 m
QUITO	FESRCARCELEN	170101816091660	14/09/16	6 m
QUITO	FESRSURORDINARIO	170101816092270	16/09/16	6 m
QUITO	DACE ADMINISTRATIVA	170101816101875	11/10/16	6 m
QUITO	DACE ADMINISTRATIVA	170101816104466	25/10/16	5 m

QUITO	DACE ADMINISTRATIVA		28/10/16	5 m
QUITO	FESRTRESMANUELAS	170101816114054	05/12/16	4 m
QUITO	FESR	170101816090092	08/12/16	4 m
QUITO	FESR	170101816124011	23/12/16	3 m
QUITO	DACE ADMINISTRATIVA	170101816123866	27/12/16	3 m
QUITO	DACE ADMINISTRATIVA	170101816125178	29/12/16	3 m

FUENTE: GESTIÓN PROCESAL – FGE.
Elaborado por: Ab. Sonia Pazmiño Montero

INTERPRETACIÓN

En el cuadro estadístico se representa 5 variables: el cantón, las diferentes fiscalías, la denuncia, fecha que ingresa la denuncia y el tiempo que ha trascurrido desde su presentación hasta la presente fecha.

ANÁLISIS

La Fiscalía General del Estado registró 75 denuncias por el delito informático de "interceptación ilegal de datos (Art. 230 COIP) a partir de su tipificación en el COIP, 10 de agosto del 2014 hasta el 31 de diciembre del 2016.

De la información obtenida hemos podido diagnosticar que en efecto de las 75 denuncias presentadas en la FGE, 50 (67%) se encuentran prescritas según en el Art. 417 del COIP, dejando en la impunidad derechos violentados de las víctimas.