



UNIVERSIDAD GERARDO BARRIOS

FACULTAD DE POSTGRADO

MAESTRÍA EN DERECHO PENAL

TRABAJO PARA OPTAR AL GRADO DE MAESTRO (A) EN:

DERECHO PENAL

NOMBRE DEL TRABAJO:

**“ALCANCES DE LA FIGURA DEL AGENTE ENCUBIERTO DIGITAL
Y SUS IMPLICACIONES EN LA INVESTIGACIÓN DE LOS DELITOS
INFORMÁTICOS FRENTE AL DERECHO DE DEFENSA DEL
IMPUTADO.”**

PRESENTADO POR:

LICENCIADO: SIMEÓN ARISTIDES CENTENO BATRES.

LICENCIADA: CLAUDIA MARIA SURA AVILES.

LICENCIADA: CLAUDIA MARIELOS REYES DE SERRANO.

ASESOR:

MAESTRA MIRTALA TERESA PORTILLO

SAN MIGUEL, 21 DE SEPTIEMBRE DE 2022

AUTORIDADES

Msc. Licdo. José Salvador Alvarenga Rivera
RECTOR

Msc. Licda. Yaneth Rubidia Campos de Rivas
FISCAL

Msc. Licdo. Jorge Luis Zelaya Garay
VICERRECTOR ACADÉMICO

Msc. Licdo. Miguel Antonio Flores Castro
DECANO DE LA FACULTAD DE POSTGRADO

Decano: MDF. Miguel Flores Castro.
Facultad de Postgrado.
Universidad Gerardo Barrios, San Miguel.
Presente.

Por este medio se hace constar que los abajo firmantes remitimos la documentación del informe final de la tesis para optar al grado de Máster en Derecho Penal, bajo el tema: “**ALCANCES DE LA FIGURA DEL AGENTE ENCUBIERTO DIGITAL Y SUS IMPLICACIONES EN LA INVESTIGACIÓN DE LOS DELITOS INFORMÁTICOS FRENTE AL DERECHO DE DEFENSA DEL IMPUTADO**”, según lo estipula el protocolo de requisitos de graduación, con el siguiente detalle:


- 1 informe final de tesis.
-

Sin otro particular.

San Miguel, 17 de octubre de 2022.

F. 

Simeón Arístides Centeno Batres.

F. 

Claudia María Sura Avilés

F. 

Claudia Marielos Reyes de Serrano.

F. 

Máster Mirtala Teresa Portillo de C.

Asesora.

A Dios todopoderoso creador de los cielos y la tierra, quien me otorgó un poco de inteligencia y sabiduría para realizar esta gesta.

En Memoria de mis padres Manuel y Gloria, que en Dios en gloria los tenga.

En Memoria de Tina, mi segunda madre

Agradezco a mi esposa Angela Verónica Flores de Centeno y mis hijos: Lucas Enrique y Rebeca Haydeé porque tuvieron que sacrificar su tiempo conmigo.

A mi "tía chita", (Mercedes Calderón de Batres) por haberme cuidado por mucho tiempo

A mis compañeras de tesis por todo el esfuerzo y sacrificio que compartimos.

A la maestra Mirtala Cruz por sus sabios consejos durante la realización de la presente tesis.

A todos mis docentes que me impartieron clases durante toda la carrera.

A todos, mis sinceras gracias.

Simeón Arístides Centeno Batres.

Mi máxima gratitud a Dios por la vida, por ser siempre mi esfuerzo en todo momento, por haberme permitido iniciar y culminar una más de mis metas propuestas, sin su voluntad nada sería posible; y sobre todo por su amor y su bondad.

A mi amada madre, por su apoyo y amor incondicional, por siempre estar a mi lado con sus valiosos consejos y orientación, por haber compartido mi sentir y mi anhelo de superación; gracias por creer en mí, gracias por nunca soltar mi mamo. A mi amado y siempre recordado padre, quien me enseñó que para triunfar se debe de luchar; y aunque ya no está a mi lado su amor seguirá intacto todos los días de mi vida.

A mi querido y amado hijo Luis Sura, por ser el motor que impulsa mi vida día a día, mi fuente de inspiración; por todo su apoyo brindado a través de sus conocimientos y por toda su comprensión, y aún más, por el sacrificio de las horas que le he robado en el transcurso de esta maestría. A él y a mi madre se los dedico.

A mis compañeros de tesis, por emprender juntos este reto que ahora estamos culminando.

Un agradecimiento general a todos los maestros/as, que de una forma profesional compartieron y transmitieron sus conocimientos y consejos durante el desarrollo de la maestría, dejando así un bagaje para emprender este trabajo. Y sin faltar un especial agradecimiento a mi asesora de tesis, Msc. Mirthala Cruz de Portillo, por aceptar la responsabilidad de ser guía y apoyo para la realización de este arduo trabajo.

A todas las personas que de una u otra forma, han estado en este proceso de formación.

A todos, gracias sinceras.

Claudia María Sura Avilés.-

Agradecimientos

Primeramente, agradecerle a Dios todo poderoso, por ser mi guía en cada paso importante de mi vida, por darme fortaleza en los momentos que más lo necesito y la sabiduría, para alcanzar la meta deseada.

A mis padres, Cecilio y Lidia Reyes, por darme la vida y por estar presentes en cada paso que doy y su apoyo incondicional, en las metas propuestas y de esa manera alcanzar mis sueños,, darme sus consejos, porque son las primeras personas en creer en mí y en mi capacidad de seguir aprendiendo, así mismo, superarme en todos los ámbitos de mi vida, especialmente en lo profesional, haciéndome una persona de provecho para la sociedad.

A mis hermanos, porque han sido fundamentales en mi crecimiento como ser humano y dar lo mejor de mi misma, por su amor y su apoyo en cada paso que doy en mi vida, lo que me ha permitido, desarrollarme profesional y espiritualmente.

A mi hija, Lauren Reyes, porque es la persona que me ha impulsado a seguir creciendo, así mismo, es quien no me permite decir, la palabra no, porque mi meta es darle un mejor futuro, en pocas palabras, es mi motor, para seguir aspirando a llegar alto dentro de esta carrera profesional del Derecho y prepararme cada día para cualquier reto.

A mi familia, porque están presentes en cada momento de mi vida y comparten mis alegrías, por brindarme sus consejos oportunos, que me han llevado por caminos de lucha constante, pero sin duda, donde puedo alcanzar el éxito en mi vida personal como profesional.

A mi esposo, Hirving Serrano, por la dedicación a su familia, por su paciencia y su apoyo total, en el transcurso de mi estudio, por sus ánimos en cada momento de flaqueza, porque nunca me permitió rendirme, por lo cual, culmine mis estudios de forma exitosa.

A los docentes, porque fueron pare fundamental en mi formación profesional, por sus sabios consejos, los cuales, pondré en práctica, permitiéndome seguir avanzando en el ámbito laboral y ser una excelente profesional.

A mi asesora de tesis, por haber dedicado tiempo y su guía en el proceso de tesis, ha sido un pilar de importancia, ya que su orientación en el proceso de tesis fue siempre oportuna, que me permitió salir de forma exitosa.

A mis compañeros de tesis, por acompañarme en este trayecto, que iniciamos al mismo tiempo y también ahora culminamos.

A las personas que de una u otra forma me brindaron apoyo incondicional en el transcurso de mi estudio de maestría.

Claudia Marielos Reyes de Serrano

Tabla de contenido

Introducción.	11
CAPÍTULO I. PROBLEMA DE INVESTIGACIÓN.	14
1.1. Situación problemática	14
1.2. Delimitación.	19
1.2.1. Delimitación temporal:.....	19
1.2.2. Delimitación Espacial.	19
1.2.2. Delimitación Temática:	19
1.3. Enunciado del problema.	20
1.4. Justificación.	20
1.5. Objetivos:.....	22
1.5.1. Objetivo general.....	22
1.5.2. Objetivos específicos	22
CAPÍTULO II MARCO TEÓRICO.	23
2.1. Antecedentes históricos.	23
2.1.1. Evolución de las tecnologías en lo jurídico.....	25
2.2. Evolución normativa de la figura del agente encubierto digital en El Salvador.....	29
2.2.1. Constitución 1983.	29
2.2.2. Ley Reguladora de Actividades Relativas a las Drogas (1993).....	29
2.2.4. Código Procesal Penal 1998.	30
2.3. Marco conceptual.	32
2.3.1. Derechos fundamentales.	33
2.3.2. Garantías Procesales.....	33
2.3.3. Garantías Constitucionales.....	33
2.3.4. <i>Debido proceso</i>	34
2.3.5. Derecho de defensa	34
2.3.6. Defensa técnica.....	35
2.3.7. Defensa material.	35
2.3.8. Delitos informáticos.....	35
2.3.9. Técnica de Investigación del delito	36

2.3.10.	Agente encubierto.	36
2.3.11.	El agente provocador.	37
2.3.12.	Agente encubierto digital.	38
2.3.13.	El ciber patrullador.	40
2.3.14.	Canales cerrados. (PEER TO PEER o P2P).	40
2.3.15.	Internet abierta.	40
2.3.16.	Surface web.	41
2.3.17.	Motor de Búsqueda.	42
2.3.18.	Deep web.	43
2.3.19.	Dark web.	43
2.3.20.	Canales abiertos.	43
2.3.21.	Evidencia digital.	44
2.3.22.	Clasificación de la tipología de la información en las redes (red oscura, red pública y red privada)	46
2.4.	Bases doctrinarias.	49
2.4.1.	Autorización judicial.	49
2.4.2.	Supuesto de aplicación.	50
2.4.3.	Objetivo del agente digital encubierto.	51
2.4.4.	Requisitos jurídicos para la admisibilidad de la evidencia digital según doctrina.	51
2.4.5.	Uso de engaño en el agente encubierto digital en relación con el derecho de no autoincriminación y no declararse culpable.	54
2.4.6.	Derecho de defensa del imputado en relación con la prueba en la evidencia digital	55
2.4.7.	Proceso penal: eficacia versus garantía.	58
2.4.8.	Reconocimiento constitucional del derecho de defensa dentro del proceso penal.	60
2.4.9.	El derecho de defensa	64
2.4.10.	El derecho de defensa como mecanismo de protección.	65
2.4.11.	El Derecho de defensa en la Investigación del delito.	68
2.4.12.	El rol del juez en los actos de investigación con control judicial	71

2.4.13. La información extraída al acusado, en la investigación frente a la prohibición de la utilización del engaño como método de recolección de información. [art.93. CPP]	73
2.4.14. Valor de las diligencias de investigación en el juicio. [Art. 311CPP] 74	
2.4.15. Exclusión de medios de prueba obtenidos en las conversaciones entre el agente encubierto y el investigado.....	76
2.4.16. La prueba digital y los derechos fundamentales.....	79
2.4.17. Tratamiento de la técnica de investigación del agente encubierto digital en el derecho comparado.	80
2.4.18. Derecho de defensa del imputado en la investigación de los delitos informáticos.....	81
2.4.18. Agente encubierto digital en El Salvador y la investigación.	82
2.4.18.1. Fundamentos	82
2.4.19. Investigación criminal y tecnología.	84
2.5. Bases legales.	85
2.5.1. Legislación.	85
2.5.2. Configuración normativa del uso de la técnica de agente encubierto digital.	86
2.5.3. Análisis comparado de la figura del agente encubierto digital.	88
2.5.4. Agente encubierto en El Salvador	88
2.5.5. <i>Tratamiento de la evidencia digital en el proceso penal salvadoreño.</i>	91
2.5.6. Ámbito internacional.	91
2.5.7. Análisis comparativo del Art 24 Cn. y la regulación de la técnica del agente encubierto digital.....	92
2.5.8. Análisis jurisprudencial.....	95
2.6. Agente encubierto informático en España.	103
2.6.1. Legislación.	103
2.6.2. Funciones.....	104
2.6.3. Evidencia digital en delitos informáticos en la investigación.	105
2.6.4. Convenio de Budapest sobre la cibercriminalidad.	105

2.6.4.1. Análisis Comparativo: Ventajas y Desventajas.	107
2.6.4.1.1. Beneficio.	107
2.6.4.1.2. Desventaja.	109
CAPITULO III. METODOLOGÍA DE LA INVESTIGACIÓN	110
3.1. Método.	110
3.2. Tipo de estudio.	110
3.3. Técnicas.	111
3.4. Instrumentos.	112
4. CAPITULO IV. HALLAZGOS DE LA INVESTIGACIÓN.	114
4.1. Análisis hermenéutico Jurídico.	114
4.1.1. Agente encubierto digital.	115
4.1.2. Campo de aplicación. Inciso. 1°	116
4.1.3. Autoridad competente.	116
4.1.4. Órgano ejecutor.	117
4.1.5. Campo de aplicación. Inciso 2°	117
4.1.6. Acuerdos de cooperación internacional. Inciso 3°	117
4.2. Análisis de entrevistas a fiscales.	119
4.3. Análisis de entrevistas a operadores judiciales. ¡Error! Marcador no definido.	
4.4. Entrevista a defensores	138
4.5. Análisis de entrevista. Entrevista 1	139
CAPÍTULO V. CONCLUSIONES.Y RECOMENDACIONES.	147
5.1. Conclusiones.	147
5.2. Recomendaciones.	149
Bibliografía	157
Anexos.	164

Introducción.

La concepción antropocéntrica en nuestra Constitución dentro del proceso penal la encontramos en los artículos del 12 al 28, pues son postulados referidos protección de la persona frente al ejercicio del poder punitivo del Estado, ya que frente a una acusación, hay reglas básicas que los operadores -creador/ aplicadores- deben de tener en cuenta para el juzgamiento de las persona, tiene que ser juzgada por un juez competente, imparcial, cuya competencia haya sido atribuida con anterioridad, a través de un procedimiento previamente establecido, el cual debe ser de carácter oral, público, y contradictorio donde se garanticen iguales posibilidades de intervención y defensa, reconociéndosele una situación jurídica de inocencia, mientras no exista un fallo condenatorio de culpabilidad que tenga como base una actividad probatoria de cargo derivada del juicio.

Siendo que un eje central de la presente investigación es el derecho de defensa, resulta fundamental centrar la mirada, cómo frente a las nuevas tecnologías, derechos reconocidos en la constitución deben ser interpretados; de tal forma que métodos de investigación como la figura del agente encubierto digital, no produzcan disfunciones de los derechos y las garantías que la persona que enfrenta el proceso penal tiene por mandato constitucional. Dentro de la presente investigación se realizó un análisis, respecto a qué, si la configuración de la técnica de investigación antes mencionada se ajusta al estándar constitucional que el derecho de defensa reconoce en el artículo 12 de nuestro ordenamiento fundamental.

A partir del reconocimiento del derecho de defensa en nuestra Constitución, el desarrollo de este se convierte en una garantía fundamental para enfrentar un proceso penal, y su materialización, no es propio del proceso judicial, pues el mismo según la configuración normativa, no hace distinción, debiendo entenderse que dicha protección debe ser trasladada en todos los aspectos, en el caso que nos atañe a la investigación del delito relacionado a los entornos digitales, por lo que la obligación no solo recae en el juzgador, sino también en el ente acusador.

No podemos desconocer que la era digital cada vez toma mayor fuerza, cada vez dependemos más de la tecnología, la inteligencia artificial está presente en nuestra vida de manera imperceptible. El crecimiento de este nuevo aspecto de la realidad hace posible el

surgimiento de nuevos espacios para el cometimiento de delitos. Los delitos informáticos son relativamente nuevos ya que el lugar donde se comete también lo es.

La técnica del agente digital encubierto es de reciente creación, la cual tiene su origen en la necesidad de una investigación del delito eficiente; pues la dinámica en que se desarrolla la vida cotidiana de las sociedades, exige que los instrumentos normativos, tanto de corte sustantivo como adjetivos, permitan la protección de bienes jurídicos, y, que además permitan ajustar los ordenamientos jurídicos al momento actual que la sociedad atraviesa; de tal forma que a pesar de los avances tecnológicos el derecho sea el instrumento mediante el cual se garantice el tratamiento de los conflictos con herramientas jurídicas efectivas, completas y actualizadas a las necesidades del momento.

Sin embargo, la modalidad de la técnica, no obstante, su utilización en el entorno de la virtualidad encontramos que la misma, ha sido utilizada para la investigación del delito y su antecedente es la técnica específica del agente encubierto, que es la base bajo la cual se desarrolló el agente digital encubierto.

Es importante dar una hojeadá de las bases históricas que permitieron el surgimiento del agente digital encubierto; además de estudiar el derecho comparado que informa a nuestra legislación y sus diferencias específicas, con el objetivo claro de lograr un contenido jurídico, sustancioso y útil para la comunidad jurídica.

El avance que han presentado las tecnologías de la información y comunicación, han generado una necesidad real de legislar y crear políticas criminales, para enfrentar el fenómeno de la cibercriminalidad; para ello, se adapta a los nuevos entornos utilizados para la comisión de hechos delictivos, la técnica de operación encubierta para la investigación de delitos informáticos y conexos; la cual se regula bajo la denominación de agente encubierto digital. En esa misma línea, dentro del marco teórico se establece la injerencia de este, dentro de la investigación del delito, quien actuará de forma infiltrada en la investigación de los delitos cometidos a través de la informática.

De conformidad a lo prescrito en los arts. 259-D, 201 y 175 del Código Procesal Penal, será procedente la implementación de operaciones encubiertas digitales, siempre que resulten necesarias realizar indagaciones por medio de programas informáticos en las

tecnologías de la información y comunicación, sean estas de carácter abierto o público, con el propósito de potenciar la seguridad de aquellos derechos intangibles que las personas han adquirido y continúan adquiriendo con la utilización e interacción en el internet; dicha investigación estará bajo el cargo de la policía, con la previa autorización de la Fiscalía General de la República. Resultando que la información obtenida durante la investigación por parte del agente encubierto digital tendrá carácter de prueba y podrá ser incorporada al proceso penal como evidencia digital.

El derecho de defensa es una esfera, donde el sujeto investigado forma parte de la carpeta investigativa desde el inicio de la investigación y participa en ellas, y que, junto a su defensa técnica, componen una defensa integral al en el proceso judicial, bajo garantías que le asisten; no obstante, es lo contrario en la investigación de los delitos informáticos cuando se autoriza un agente digital encubierto, donde se declara reserva desde el inicio de la investigación.

El agente encubierto digital es una figura donde por no tener control judicial, sino solo un control funcional, es decir de la Policía Nacional Civil, pero autorizado por la Fiscalía General de la República, procede con la investigación, pudiendo interpretarse como una vulneración al derecho de defensa, habiéndose examinado a través de esta investigación dicha figura, frente al derecho de defensa.

Respecto al derecho de defensa frente a la investigación de los delitos informáticos, con la entrada en vigor de la figura del agente encubierto digital, supone una desventaja para el sujeto investigado, puesto que únicamente intervienen en ella, el ente investigador (Fiscalía y Policía), sin mediar actuación jurisdiccional que garantice el estricto respeto y cumplimiento de las garantías judiciales y derechos fundamentales del sujeto investigado.

CAPÍTULO I. PROBLEMA DE INVESTIGACIÓN.

1.1. Situación problemática

El surgimiento del agente digital encubierto, con la entrada en vigencia del decreto número 280 de fecha 01 de febrero de 2022; publicado en el Diario Oficial Tomo 434 de fecha 04 de marzo de 2022, con el cual se adicionó el artículo 259 – D, del Código Procesal Penal, trae a la sociedad nuevas herramientas para la investigación del delito informático, por lo cual el agente digital encubierto es una técnica en la investigación del delito.

Las técnicas de investigación del delito son las herramientas con las que cuenta el Estado para descubrir la verdad, cuando se tiene indicios que se cometió un ilícito penal.

Existen una gran cantidad de ellas que se pueden utilizar dependiendo de la clase de delito o las personas a investigar; sin ellas no se tendría posibilidad alguna de lograr una “pronta y efectiva justicia”, en consecuencia el Estado debe garantizar a la población a través de los distintos órganos persecutores del delito, que tienen los elementos necesarios para la averiguación de la verdad, dada la obligación de asegurar la seguridad jurídica que debe tener tanto la víctima, como la persona a quien se atribuye un delito.

Del desarrollo del estudio, se infiere que dicha figura será importante en la investigación del delito digital, porque supone un avance cualitativo en la investigación del delito. No obstante, su importancia, la regulación actual presenta indicios de posibles vulneraciones a garantías constitucionales, ya que para su utilización no se requiere autorización judicial, lo cual, en otros países, como España, es un requisito habilitante.

A medida que la humanidad logra avances en el desarrollo, a nivel científico como social, esto conlleva al apareamiento de nuevas formas de cometer el delito en ese nuevo campo. Por ello en cada escalón que sube la humanidad, así sube el nivel de delitos y, por lo tanto, los medios que el Estado tiene que construir y desarrollar para evitar, prevenir y sancionar a aquellos individuos que los cometan.

Ese desarrollo jurídico a pesar de ser novedoso debe ser también respetuoso de los derechos y garantías fundamentales de la persona investigada, dichos alcances han sido objeto de estudio de la presente investigación.

Por ello debemos tener en cuenta el pasado de la investigación del delito para tener un enfoque acertado y comprensivo del mismo. La investigación en tiempos bíblicos pasó de una venganza total, a una limitación punitiva “ojo por ojo, diente por diente”, allá por el año 2,000 antes de Cristo. (Cabezas Esteban, 2010, p. 19), debemos reconocer que técnicamente no representan una “investigación del delito”

Luego en la Edad Media surgen diversos métodos de torturas, que básicamente buscaban la “verdad” lesionando hasta la muerte al presunto culpable; con la tortura se pretendía llegar a la confesión del imputado-víctima, esto porque la confesión era la “reina de las pruebas”.

Sin embargo la existencia de la investigación como hoy la entendemos no se puso en práctica, ya que no era necesaria la existencia de pruebas materiales para la imputación de un hecho criminal, aunque en casi todos los Estados europeos, durante la Edad Media y Moderna, se relatan casos en los que se tiene en cuenta algún tipo de procedimiento o la aplicación de formas que, tienen como finalidad el esclarecimiento práctico y real de los hechos criminales, pero no hemos de olvidar que son la excepción (Cabezas Esteban, 2010, p. 21)

Luego con la codificación de leyes, encontramos indicios sistematizados de técnicas de investigación del delito.

En nuestro país podemos retrotraernos hasta el Código Procesal Penal de 1973, (derogado) en el cual en el Título III, “COMPROBACIÓN DEL DELITO Y DE LA DELINCUENCIA” a partir del art. 150, podemos encontrar algunas técnicas de investigación adecuadas para la época, tales como: la inspección, art. 152; examen de identificación del cadáver, art. 155; reconocimiento de cadáver, art. 161; análisis químicos y exámenes científicos art. 166, entre otras. Dichas técnicas eran válidas y técnicamente posibles para su época; las cuales han sido recogidas por el Código Procesal Penal del año de 1998.

En el código Procesal Penal de 1998, encontramos un mayor desarrollo de las técnicas de investigación del delito, además de las múltiples reformas que tuvo; en dicho cuerpo legal se consagra el art. 162, que establece lo siguiente:

Los hechos y circunstancias relacionados con el delito podrán ser probados por cualquier medio legal de prueba, respetando las garantías fundamentales de las personas, consagradas en la Constitución de la República, y demás leyes, siempre que se refiera, directa e indirectamente al objeto de la averiguación y sea útil para el descubrimiento de la verdad.

En consonancia con ese desarrollo, se estableció en el art. 171 del mismo código, las denominadas “operaciones técnicas”, donde se establece la base para las distintas técnicas de investigación del delito.

Con relación al agente encubierto en el art. 192 -A), se estableció la declaración de “declaración de agentes, funcionarios y empleados encubiertos”. Cabe aclarar que aún el desarrollo tecnológico de la internet estaba en sus etapas iniciales, a nivel mundial y aún más en nuestro país.

Luego en el Código Procesal Penal del año 2009, se amplía el catálogo de técnicas de investigación del delito, se establecen, por ejemplo, las operaciones técnicas, art. 186; se reconoce la prueba del ADN, art. 187; el agente encubierto, art. 282 literal d); y, actualmente el tema que nos ocupa el agente digital encubierto, art. 259 – D de dicho cuerpo legal.

En ese sentido, con la figura del agente encubierto tradicional el propósito del legislador era contrarrestar delitos complejos, cumpliendo con requisitos establecidos jurisprudencialmente a partir de la sentencia de inconstitucionalidad ref. 147 – 2010, emitida por la Sala de lo Constitucional de la Corte Suprema de Justicia, de fecha 09 de marzo de 2012, entre ellos: i) que sean de criminalidad organizada; ii) ser indispensable; iii) con autorización de la Fiscalía General de la República; iv) la información recabada deberá ser puesta a la brevedad posible a la Fiscalía General de la República; v) respeto a los derechos y garantías constitucionales; vi) que la actividad del agente investigador no se convierta en delito.

El agente digital encubierto es un esfuerzo del legislador de dotar de herramientas adecuadas para la investigación de delitos informáticos y conexos, los cuales son cometidos en uso u ocasión de las tecnologías de la información y la comunicación.

La figura del agente digital encubierto viene a ser una figura especial del agente encubierto “tradicional”, con la diferencia que el primero es exclusivo para delitos informáticos.

Ahora bien, la figura del agente digital encubierto no está configurado en el respeto a dichos requisitos, lo cual plantea una serie de posibles escenarios jurídicos en los cuales se pondría en tela de juicio el respeto a los criterios de validez de dichos agentes.

Por ejemplo, si el agente investigador entra en contacto vía correo electrónico con un posible sospechoso, ¿podría utilizarse esos correos como prueba? consideramos que dicho nivel de acceso requiere autorización judicial, y eso no está regulado por la reforma, ni por ninguna otra ley.

Por todo lo anterior, se ha realizado un escenario investigativo sobre los siguientes puntos:

1. Se efectuó un análisis de los alcances de la figura del agente digital encubierto en la investigación de los delitos informáticos, según el ordenamiento jurídico, jurisprudencial y doctrinario.
2. Se realizó un estudio de la normativa nacional e internacional, así también, doctrinario y jurisprudencial de las funciones del agente digital encubierto, durante la investigación de los delitos informáticos, respecto a los derechos y garantías fundamentales de la persona con calidad de imputada, específicamente al derecho de defensa enfocado en la ausencia de un control judicial.

3. Se analizaron los criterios y puntos de vista de expertos en la materia, entre ellos: operadores del sistema de juzgamiento (jueces), operadores del sistema encargados de la acción (fiscales), y profesionales del derecho en el libre ejercicio (defensores técnicos); sobre los alcances y funciones del agente digital encubierto durante la investigación de delitos informáticos, respecto al derecho de defensa del sujeto investigado frente a la ausencia del control judicial, durante la investigación.

1.2. Delimitación.

1.2.1.

D

Delimitación temporal:

La información tomada a consideración para la realización del presente trabajo de investigación, se enmarcó dentro del periodo del 4 de marzo al 30 de junio del año 2022, por haber entrado en vigencia la figura del agente encubierto digital, del decreto legislativo N° 280, publicado en el Diario Oficial de fecha 4 de marzo del presente año, tomo 434, tiempo en el que se aplicará la técnica de entrevista a operadores del sistema judicial, así también a operadores de la acción (siendo estos agentes fiscales), y profesionales del derecho en el libre ejercicio (defensores técnicos); considerando únicamente los alcances del figura del agente digital encubierto y sus implicaciones en la investigación de los delitos informáticos, respecto al derecho de defensa del imputado, frente a la ausencia del control judicial; retomando además a consideración información jurisprudencial y doctrinal [advirtiendo que el estudio de estas fuentes no comprenden el periodo establecido en el inicio de este párrafo].

1.2.2. Delimitación Espacial.

El presente trabajo de investigación además de haberse analizado información de las fuentes doctrinarias, normativas y jurisprudenciales se realizó, el análisis de la información obtenida a través de las entrevistas efectuadas en las instituciones judiciales, oficinas fiscales y profesionales del derecho en el libre ejercicio, en la ciudad y departamento de San Miguel y Usulután.

1.2.3. Delimitación Temática:

El presente trabajo de investigación se ha desarrollado respecto a los alcances que posee el agente encubierto digital, en la investigación de delitos informáticos, así como la injerencia de este en misma, todo ello frente al derecho de defensa que le asiste a la persona que se le imputa la comisión del ilícito informático, en lo referente a la falta de mediación de una autoridad judicial para la práctica de esta operación.

Lo anterior se realizó, a través del análisis y estudio de forma normativo, jurisprudencial y doctrinal, y a la vez, sobre los criterios de los operadores profesionales del derecho en la progresividad de la protección en cuanto al respeto de las garantías judiciales que le asisten a la persona investigada, respecto a su derecho de defensa durante la investigación, todo ello habiéndose tomado a consideración la situación de la ausencia del control judicial durante la práctica de las diligencias investigativas.

1.3. Enunciado del problema.

¿Cuáles son los alcances de la figura del agente encubierto digital y sus implicaciones en la investigación de los delitos informáticos, frente al derecho de defensa del imputado, debido a la ausencia del control judicial, en la práctica de dicha técnica?

1.4. Justificación.

La importancia de la investigación radica en diferentes niveles, siendo estos los siguientes:

El agente encubierto digital es una figura nueva en nuestro ordenamiento jurídico, que tendrá gran repercusión en la investigación de los delitos informáticos. Las actuaciones que éste realice tendrán repercusiones dentro del proceso penal, dichas repercusiones deben ser analizadas para incrementar el acercamiento jurídico penal, que en el caso en concreto es un tema totalmente nuevo y por lo tanto necesario, que ponga la justicia penal en nivel de avance frente a las nuevas tecnologías.

Dada que la configuración y campo de acción de dicho método de investigación será en la “privacidad de las comunicaciones digitales” de los posibles imputados, sin que medie un control jurisdiccional; puesto que dicha técnica únicamente está bajo la dirección

funcional de la Fiscalía General de la República, de quien es sabido, es el ente acusador y por ende el encargado de recabar las pruebas de cargo sobre la comisión de un delito, lo cual pone en desventaja al investigado, puesto que este no solo desconoce de la investigación realizada en su contra (careciendo además de la asistencia de un defensor), sino aunado a ello, que tampoco cuenta con la seguridad del respeto a las garantías judiciales que le asisten (derecho de defensa, debido proceso, gama de principios procesales, etc.), ni de una seguridad jurídica para el respeto a sus derechos fundamentales, pues todo está a cargo del ente acusador e investigador. Resultando en razón lo anterior necesario investigar, y con ello indagar el grado de vulneración que con esta actividad investigativa se da en los derechos y garantías judiciales, por no cotar con el control de un juez; específicamente el derecho de defensa del imputado, por ser este un derecho y una garantía fundamental de las personas que enfrenta el ejercicio del poder punitivo.

La información ha sido obtenida a través de la utilización de dos métodos: el método cualitativo y el método de la hermenéutica jurídica, los cuales han sido esenciales en el abordaje del tema.

Las variables de la investigación son entonces, el agente encubierto digital, que sería una variable independiente, y el derecho de defensa del imputado, sería la variable dependiente del tema.

Se configura por tanto como objetivo de la investigación el análisis de la figura del agente encubierto digital y las repercusiones que tendrá frente al derecho de defensa del imputado debido a la ausencia de un control judicial.

Por lo tanto, los resultados obtenidos serán importantes herramientas para los estudiosos del derecho, así como la sociedad en general debido a la necesidad de contar con un abordaje científico de tan reciente y novedosa institución del derecho penal.

1.5. Objetivos:

1.5.1. Objetivo general

Determinar los alcances de la figura del agente encubierto digital y las implicaciones en la investigación de los delitos informáticos, frente al derecho de defensa del imputado por la ausencia de control judicial en la autorización de dicha técnica.

1.5.2. Objetivos específicos

- Determinar el alcance normativo de la figura del agente digital encubierto en la investigación de los delitos informáticos.
- Determinar si la falta del control judicial en la utilización de la técnica del agente digital encubierto puede afectar el derecho de defensa.
-
- Identificar soluciones interpretativas, sobre la utilización de la técnica del agente encubierto digital en la investigación de los delitos informáticos frente al derecho de defensa del imputado.
-

CAPÍTULO II MARCO TEÓRICO.

2.1. Antecedentes históricos.

La figura del agente encubierto según las diferentes posturas doctrinarias presenta un origen bíblico y literario, puesto que es relacionado con pasajes de la biblia y obras literarias; no obstante, ya meramente en materia de investigación la cual nos ocupa en la presente investigación, se afirma que esta figura tuvo su surgimiento en Francia, habiéndose creado con fines políticos para el espionaje, atribuyéndola en la figura del “Agente Provocador”.

Para el autor MONTROYA (*La Investigación Del Delito En El Derecho Penal Español - Piva Torres, Gianni Egidio, Ruiz Carrero, Wilmer de Jesús, Lattuf Rodríguez, Williams de Jesús - Google Libros, 2021*) señala que el surgimiento del agente encubierto tiene diversa posturas, ello según autores del derecho esta figura posee orígenes en el pasaje bíblico citado en Genesis capítulo 3: 1-7, el cual alude a la astucia de la serpiente para engañar a Eva (durante la creación del mundo); otra posición adoptada es que el origen de la referida figura, recae en la antigüedad griega, en las fábulas de Esopo; no obstante, presentan una postura diferente a las anteriores, afirmando que el origen de esta figura radica en la expresión francesa “ Agent Provocateur”. Dicha expresión francesa, es relacionada con las actividades políticas de espionaje que se realizadas en Francia, durante los siglos XIV y XVI; en donde personas catalogadas “agentes”, provocaban a otras personas (quienes eran consideradas enemigos del gobierno) para que cometieran delitos políticos, no con el fin de la persecución en la investigación de un delito, si no dirigido directamente contra la persona (víctima) con el propósito de eliminarlos y así dejaran de ser un peligro para el Estado, dándose con ello una persecución política; esta figura tenía fines fundamentalmente políticos. El agente encubierto provocador (como figura de origen) es diferente a la figura del agente encubierto actual, en cuanto a que el segundo es utilizado como una técnica de investigación especial para combatir delitos.

La investigación del delito es una herramienta del proceso penal, por lo tanto, está necesariamente unida a la evolución de este, por ello, así como evolucionó el proceso penal así debe desarrollar la investigación del delito.

Es importante, partir mencionado, que la evolución histórica de la ciencia del derecho penal pertenece propiamente a la historia del derecho, la misma que comienza por así decirlo en la época primitiva, la cual se refiere a la historia general del derecho romano, canónico e italiano.

Que tiene su literatura propia relacionada con el derecho penal alemán, común de los siglos XVI, XVII, XVIII, en el cual la ciencia del derecho penal, se hallaba en las manos de copistas, sin ingenio ni espíritu crítico, por lo cual es entendida como nacida en las sociedades, tras la necesidad de la creación de la propiedad privada, la cual es considerada como uno de los indicios del derecho penal, otro aspecto importante dentro de la época primitiva, es también que se basa en la costumbre es decir es un derecho consuetudinario, que por ende llega a tener características religiosas y otras denominadas místicas o mágicas(CORNEJO A., 2020)

En el desarrollo legislativo, en la constitución de 1824 se estableció la competencia del órgano judicial para conocer de la aplicación de la ley. art. 46, en el art. 62 se estableció una versión previa del debido proceso, cuando establece que: ningún salvadoreño podrá ser preso sin precedente sumario del hecho por el cual deba ser castigado; y sin previo mandamiento del juez por escrito que ordene la prisión. (*Constitución Política de La República de El Salvador de 1824 | Biblioteca Virtual Miguel de Cervantes, 1824*)

En nuestro país, en el Código de Instrucción Criminal, de la República del Salvador, en 1882, en el cual, en relación con la investigación del delito tenía algunas disposiciones propias de su época. Este código es totalmente primitivo y tiene un corte netamente inquisitivo, es decir, que el juez es el impulsor de la investigación. En el mismo la principal prueba es la confesión,

Art. 6. — Corresponde asimismo a los jueces de paz practicar las primeras diligencias de instrucción en todos los delitos comunes que se cometan en sus respectivas jurisdicciones, o instruir todas las mas que los jueces de 1a instancia les cometan.

Art. 7. — Son primeras diligencias, las indagaciones mas (sic) urgentes e indispensables que no pueden diferirse, para la comprobación del cuerpo del delito, por el medio que su naturaleza exija, y para el descubrimiento de los criminales; como el reconocimiento del cadáver en caso de homicidio, de la persona ofendida en el de heridas, golpes ó (sic) cualquiera otra violencia, de la casa ó (sic) heredad quemada, de las fracturas ó (sic) rompimientos en el robo etc., la declaración del ofendido si fuere posible, el examen de los testigos que aparezcan desde luego como presenciales, la detención ó(sic) arresto de las personas sospechosas y la declaración indagatoria de éstas.(Código de Instrucción Criminal de la República de El Salvador - El Salvador - Google Libros, s/f, p. 2)

Asimismo, en cuanto a la investigación dispuso lo siguiente:

Art. 163. — El juez de 1a instancia ó (sic) el de paz, luego que tenga noticia de haberse cometido un delito de los «pie dan lugar á (sic) procedimiento de oficio, procederá á (sic) instruir las diligencias correspondientes para la averiguación del delito, sus autores, cómplices y encubridores. (Código de Instrucción Criminal de la República de El Salvador - El Salvador - Google Libros, s/f, p. 24)

En este artículo podemos ver que la investigación del delito era competencia del juez de lo penal.

Luego tenemos el Código Procesal Penal de 1973, que también estaba enmarcado en el sistema inquisitivo, es decir que la mayoría la función investigativa era dirigida y ejecutada por el juez instructor.

2.1.1. Evolución de las tecnologías en lo jurídico.

Indudablemente el derecho ha usado cada avance tecnológico tiene repercusiones en el mundo jurídico, por ejemplo, crea nuevos escenarios, el surgimiento de la imprenta permitió la impresión masiva de nuevos libros que posteriormente configuró los derechos de autor.

La creación del campo computacional originó un nuevo escenario: el mundo digital; el cual tiene un sin número de aplicaciones con el derecho: propiedad intelectual y todos sus derivados, contratación online.

Asimismo, cada avance tecnológico necesita su debida regulación tanto en las distintas áreas del derecho o creación de nuevas áreas del derecho: derecho informático, informática forense, delitos informáticos, etc.

Por ello se espera que la informática jurídica, sirva para la toma de decisiones en un futuro, es decir que la informática jurídica sirva para la aplicación del supuesto normativo al hecho concreto.

Generaciones de computadoras.

En el mundo de la informática, según el nivel de surgimiento de los procesadores, se tienen la clasificación por “generaciones”, de la manera siguiente:

Primera Generación. (1950)

Estas computadoras trabajaban con tubos al vacío, gigantescas y costosas, la más conocida es la computadora llamada: UNIVAC.

Segunda Generación. (1960)

El tamaño se reduce y se inicia la forma de comunicarse con la computadora, con ello el nacimiento del “lenguaje de programación”, dentro de estas computadoras tenemos: ATLAS.

Tercera Generación. (1964)

Computadoras mucho más pequeñas, del tamaño de 2 archiveros de oficina, utilizaron el sistema de circuitos integrados. El modelo más representativo es la IBM 360.

Cuarta Generación. (1980)

Surgimiento de los procesadores, integración de los circuitos integrados de alta densidad y velocidad impresionante. Acá hay una auténtica revolución: el surgimiento de la computadora personal.

Quinta Generación: (1983 – ?)

Con esta generación se trata de innovar en el manejo del lenguaje natural y sistemas de inteligencia artificial.

Aquí tenemos todas las computadoras que conocemos hoy en día tanto las de uso personal como las de uso científico.

Desde esa época el avance en el poder de procesamiento es alucinante, se pasó de unos cuantos kilobits de memoria y procesamiento que es medido por petabits

Computadoras Cuánticas.

El concepto surge en 1980, con y utilizan Richard Feynman quien propuso la utilización de fenómenos cuánticos para uso computacional. La idea revolucionaria de este tipo de computadora es el uso del estado cuántico de la materia, en el cual un átomo puede estar en dos lugares al mismo tiempo, es decir, la computadora cuántica puede hacer muchas más cosas mucho más rápido que los supercomputadores actuales, su unidad de medida es el "qubit", como se le ha venido a llamar en abreviación de "quantum bit", puede estar no sólo en uno de los estados 0 o 1, sino que también puede estar en una superposición de ambos. (Saniz Balderrama, 2001)

El surgimiento de las computadoras necesariamente supuso la regulación de la propiedad de las mismas, (hardware) así como también los programas utilizados para su funcionamiento (software).

Por lo tanto, la intersección entre el derecho y la informática es conocida como "informática jurídica; y se puede definir como: "es una rama de las ciencias jurídicas que

contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática.” (Aguilar, 2015, p. 2)

La tecnología informática basada en sistema de software aparece con la primera computadora llamada

El derecho informático, como una nueva rama del conocimiento jurídico, es una disciplina en continuo desarrollo, que tiene en su haber (al menos hasta esta fecha) nuevos antecedentes a nivel histórico; empero, podemos decir que las alusiones más específicas sobre esta interrelación existen a partir de 1949 con la obra de Norbert Wiener, en cuyo capítulo 4, dedicado al derecho y las comunicaciones, expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico. Dicha interrelación se da a través de las comunicaciones, a lo que habría que agregar que, si bien estos postulados tienen cerca de 40 años, en la actualidad han adquirido matices que probablemente ni el mismo Wiener hubiera imaginado. Así, esta ciencia de entrelazamiento interdisciplinario sugería una conjunción aparentemente imposible entre los mundos del ser y del deber ser.(Téllez Valdéz, 2009, p. 32)

Inteligencia artificial y el derecho.

El autor Pino Diez, (2001) citado por Navas Navarro, define la inteligencia artificial como:

“es un campo de la ciencia y la ingeniería que se ocupa de la comprensión, desde el punto de vista informático, de lo que se denomina comúnmente comportamiento inteligente. También se ocupa de la creación de artefactos que exhiben este comportamiento” (Navas Navarro, 2017, pp. 23, 24)

En la actualidad tenemos un avance enorme en la tecnología, la inteligencia artificial está creciendo a pasos agigantados, y por ese desarrollo, se debe regular a efecto de proteger los derechos de los ciudadanos.

Hasta la fecha se conocen dos modelos computacionales aplicados al razonamiento jurídico: i) los sistemas expertos basados en la lógica formal mediante el suministro de una

serie de reglas (1.); ii) los sistemas expertos de extracción de información conceptual y el Cognitive. Computing: (Navas Navarro, 2017, p. 27)

Por tanto, la evolución de la tecnología en lo jurídico llevó a la regulación de derechos de sobre el software y el hardware, a nivel de derecho patrimonial y derecho penal, así como la utilización de las tecnologías en el derecho.

2.2. Evolución normativa de la figura del agente encubierto digital en El Salvador.

2.2.1. Constitución 1983.

En la reforma constitucional se estableció por primera vez la separación de funciones del órgano investigador del órgano juzgador, cuando se estableció que era el Fiscal General de la República quien monopolizaría la acción penal, según la reforma al ordinal 4° del art. 191: 4°- “PROMOVER LA ACCION PENAL DE OFICIO O A PETICIÓN DE PARTE”;(1).

A pesar de su reforma, dicha disposición no fue operativa sino hasta el año de 1998 con la entrada en vigencia del entonces nuevo Código Procesal Penal de dicho año.

2.2.2. Ley Reguladora de Actividades Relativas a las Drogas (1993)

En esta ley fue la primera que en El Salvador se reguló la figura del agente encubierto en el art. 4 de la misma de la manera siguiente:

2.2.3. Agente encubierto

Todo miembro de la corporación policial, independientemente de su rango institucional, que haya sido nombrado por escrito como tal por el director general de la policía, o por agente de autoridad en la que él delegare dicha función, y que fuere autorizado por escrito por la Fiscalía General de la República para el uso de

medios engañosos con el exclusivo objeto de detectar, investigar y probar conductas delincuenciales contempladas en la presente ley.

La figura del agente encubierto es de capital importancia ya que del mismo se deriva la figura del agente digital encubierto digital. El surgimiento de esta figura es debido al nivel de complejidad que muestran las organizaciones que se dedican al tráfico ilícito de drogas. En este artículo se establece que tanto el director de la Policía Nacional Civil como la Fiscalía General de la República, podían autorizar su funcionamiento.

2.2.4. Código Procesal Penal 1998.

Este código cambió los paradigmas en la administración de justicia penal, que desde la fundación del estado había tenido un corte inquisitivo, pasaba a tener un corte acusatorio. Donde el órgano investigador es diferente del órgano juzgador y se establece la preponderancia del sistema de audiencias versus el sistema escritural, aunque debemos admitir que tenemos un sistema mixto.

En cuanto a las técnicas de investigación del delito, este código procesal admitió nuevas técnicas propias del desarrollo tecnológico de su época.

Operaciones Técnicas.

Art. 171.- Para mayor eficacia de las inspecciones y reconstrucciones, y en cualquier caso cuando sea conveniente, se podrán ordenar operaciones técnicas y científicas convenientes, tales como exámenes serológicos, químicos, microscópicos, microfotografía, macrofotografía, pruebas ópticas, biogenéticas, antropométricas, fonográficas, grafoscópicas, electrónicas, acústicas, de rayos X y las demás disponibles por la ciencia y la técnica. (8) (el subrayado es nuestro)

declaración de agentes, funcionarios y empleados encubiertos

Art. 192.-A.- La declaración de los agentes, funcionarios y empleados que hayan participado en operaciones encubiertas de la Policía Nacional Civil, con

autorización por escrito del fiscal general de la República tendrá la validez de prueba testimonial. (6)

Este código era tachado de “excesivamente garantista” por ello, también el cambio de normativa imponía una restricción a las facultades policiales reconocidas en la Ley Reguladora de Actividades Relativas a las Drogas, que tácitamente reconocía la utilización de agentes encubiertos y provocadores para la investigación de narcotráfico, situación que el régimen probatorio del proceso vigente no reconocía en un inicio. Esta situación ha sido modificada legislativamente permitiendo, dentro del CPP el uso de agentes provocadores y encubiertos bajo el control de la fiscalía, los que pueden actuar en cualquier tipo de delincuencia organizada (Fundación de Estudios para la aplicación del derecho, 2003, p. 45)

Este código sufrió muchísimas reformas las cuales fueron poco a poco flexibilizando los requisitos para la investigación y haciendo más fácil la función investigativa de tanto de la policía nacional civil, como para la Fiscalía General de La República.

En la actualidad este equipo investigador entiende la necesidad de dotar al órgano persecutor del delito de la herramientas que permita, realizar una protección efectiva de la tutela que el derecho sustantivo ofrece respecto de los bienes jurídicos, en tanto es necesario realizar estudios a cada técnica implementada, en razón de que nuestro proceso es un conjunto de derecho y garantías, en el cual se ha determinado que cualquier información que se recopile dentro de una investigación o en el proceso penal con infracción o vulneración de derechos individuales, -derecho de defensa- se considera como prohibida y que por lo tanto es ilícita. En consecuencia, cuando la prueba se obtiene violando un derecho fundamental como la vida, la libertad, la integridad, a través de tortura, desaparición forzada, amenazas y engaños [que es donde podríamos ubicar la técnica de investigación objeto de estudio] se torna de pleno derecho en ilícita y no puede ser tenida en cuenta en ninguna actuación judicial.

2.3. Marco conceptual.

En la presente investigación para una mejor comprensión, de los ejes temáticos desarrollados en la misma, se desplegarán en este apartado el contenido de los conceptos importantes, que permitirán lograr una identificación de forma clara y precisa la temática.

Dentro de las funciones del Estado se encuentra investigación del delito, la cual tiene razón de ser, pues el proceso penal es el mecanismo de protección que se ha instaurado como mecanismo de protección frente a la lesión o puesta en peligro de un bien jurídico tutelado por el derecho penal.

Si bien dentro de la presente investigación no tiene como finalidad estudiar la estructura de normas sustantivas o tipos penales, si es necesario reconocer que la dinámica en que se mueve la delincuencia lleva a la regulación de conductas por medio del derecho penal, conducta que constituyen supuesto de hechos, en tanto frente a esa regulación de conducta, requiere que se disponga de métodos mediante los cuales se determine la investigación y determinación de responsabilidad penal, en tanto la función punitiva del Estado debe evolucionar y tecnificarse para poder realizar su deber.

En ese sentido, el surgimiento de las tecnologías de la información y comunicación abrió un nuevo espacio para el surgimiento y desarrollo de nuevas figuras delictivas.

Por lo tanto, al surgir el delito informático, el Estado debe dotarse de herramientas tecnológicas que sean pertinentes, eficaces y conducentes para la investigación del delito informático. Esto debido a que con técnicas tradicionales poco se podría hacer para la investigación de este. Por lo que es necesario desarrollar conceptualmente la terminología e instituciones jurídicas vinculadas a la presente investigación, los cuales nos permitan comprender las temáticas contenidas.

2.3.1. Derechos fundamentales.

Son todos aquellos derechos que constituyen el asiento o fundamento de protección de la vida o actividades esenciales de las personas, permitiendo el desarrollo de estas y el ejercicio de libertades públicas.(de Silva Gutiérrez, 2021, p. 78)

Para Ferrajoli, los derechos fundamentales: “ son todos aquellos derechos subjetivos que corresponden universalmente a todos los seres humanos en cuanto dotados del status de personas o ciudadanos, con capacidad de obrar; entendiendo por derecho subjetivo cualquier expectativa positiva (de prestación) o negativa (de no sufrir lesiones) adscrita a un sujeto por una norma jurídica; y por status la condición de un sujeto, prevista así mismo por una norma jurídica; y por status la condición de un sujeto, prevista así mismo por su idoneidad para ser titular de situaciones y/o autor de los actos que son ejercicio de estas”.(Aguilera Portales & López Sánchez, 2007, p. 5)

2.3.2. Garantías Procesales.

Las garantías judiciales o garantías procesales, hace referencia a todos aquellos derechos que tienen como finalidad la protección de la persona que se encuentra sometida a un procedimiento legal ante una autoridad competente, que puede ser de orden civil, laboral, fiscal, o cualquier otro carácter (Villavicencio Macías, s/f, p. 17)

2.3.3. Garantías Constitucionales.

Como garantías constitucionales del proceso penal, se entiende “el cumulo de principios, derechos y libertades fundamentales reconocidas por la constitución y “*lato sensu*”, por los tratados internacionales que tienen por finalidad otorgar al imputado un marco de seguridad jurídica, y en última instancia, mantener un equilibrio entre la llamada búsqueda de la verdad material y los derechos fundamentales del imputado”. (Caro Coria, 2007, p. 1028)

El autor Pablo Lucas Verdú, define desde un criterio sociológico las garantías constitucionales “como instrumentos jurídicos-formales que tutelan el libre y seguro desenvolvimiento del individuo en una estructura social”, citado por el autor Louis Alain

Benavides Monterrosa en “El debido proceso en la jurisprudencia constitucional”. (Benavides Monterrosa, 2010, p. 3)

2.3.4. Debido proceso.

La Corte Interamericana de Derechos Humanos, señala que el derecho al debido proceso se refiere: “al conjunto de requisitos que deben observarse en las instancias procesales a efectos de que las personas estén en condiciones de defender adecuadamente sus derechos ante cualquier acto del Estado, adoptado por cualquier autoridad pública, sea administrativa, legislativa o judicial, que pueda afectarlos. (Corte Interamericana de Derechos Humanos, 2018, p. 35)

La Sala de lo Penal de la Corte Suprema de Justicia, de El Salvador, en sentencia con referencia número 67C2014, retoma la definición sobre el debido proceso: “ como aquel conjunto de garantías en virtud del cual se asegura a las partes en todo proceso legalmente establecido y sin dilaciones injustificadas, la oportunidad razonable de ser oídas por un tribunal competente predeterminado por la ley independiente e imparcial, de pronunciarse respecto a las pretensiones y manifestaciones de aportar pruebas lícitas relacionadas con el objeto del proceso y contradecir las proporcionadas por la contraparte, de hacer uso de los medios de impugnación consagrados por la ley contra resoluciones judiciales motivadas y conforme a derecho, de tal manera que las personas puedan defender efectivamente sus derechos” (Sala de lo Penal, 2015, p. 4)

2.3.5. Derecho de defensa

El derecho de toda persona a ser oída con las debidas garantías y dentro de un plazo razonable por un juez o tribunal competente, independiente e imparcial, establecido con anterioridad por la ley en la sustanciación de cualquier acusación penal en su contra o para la determinación de sus derechos de carácter civil, laboral, fiscal u otro cualquiera (Montero & Salazar, 2013, p. 101)

2.3.6. Defensa técnica.

Aquella actividad que se ejercita durante todo el proceso con el fin de eliminar toda duda que el ejercicio de la acción penal ha producido con relación a una persona determinada. (Robleto Gutiérrez, 2013, p. 24)

2.3.7. Defensa material.

La directa intervención del inculpado en el proceso es la facultad de este de bregar a favor de su inocencia por sí mismo. Se trata de la parte del ejercicio de la defensa que lleva a cabo personalmente el propio imputado y que se manifiesta en diferentes formas y oportunidades. Consiste en sus propias expresiones defensivas, volcadas en las explicaciones que vierta cuando declare en las sucesivas etapas del proceso; cuando se confronte con la víctima, un testigo o coimputado en un careo; cuando ejerza la facultad de interrogar personalmente a un testigo (Mouriño, 2020, p. 3)

2.3.8. Delitos informáticos

Delitos informáticos computer crimes, comprenden todas las acciones típicamente antijurídicas para cuya consumación se utiliza o se afecta perjudicialmente una computadora o sus accesorios y se incluyen las acciones de uso indebido del software, apropiación o comunicación ilícita de datos, interferencias de bancos electrónicos ajenos de datos, y muchas otras conductas antijurídicas relacionadas con la informática, dichas figuras delictivas tipificadas en el Código Penal y en leyes especiales pueden ser cometidas con los sistemas electrónicos de elaboración de datos, o contra ellos, dañándolos. (Flores Salgado, 2015)

Es el derecho a la intimidad del artículo 18.1 de la norma suprema. Este derecho implica “la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura para mantener una calidad mínima de la vida humana (Ascencio Mellado & Fernández López, 2017, p. 105); derecho fundamental a la autodeterminación informativa que se recoge el artículo 18.4 de la norma suprema.

Este derecho supone un reforzamiento de la autonomía individual de la persona en el contexto de las nuevas tecnologías de la información (Ascencio Mellado & Fernández López, 2017, p. 106)

2.3.9. Técnica de Investigación del delito.

Se define como aquellos métodos y procedimientos realizados por los operadores del sistema, con la finalidad de determinar la ocurrencia de un hecho penalmente relevante y presentarlo en los estrados judiciales-

Dentro de las técnicas de investigación del delito existe una modalidad de investigación, que es de interés dentro de la presente investigación, debido a que la misma pudiera estar produciendo alguna afectación a la garantía fundamental del derecho de defensa del acusado, debido a la ausencia de control judicial, por lo que es necesario esgrimir sobre la misma, así como los efectos que esta produce, antes y después de la judicialización de la información; nos referimos al agente digital encubierto.

2.3.10. Agente encubierto.

Debemos partir de la figura conocida y de la cual nace el agente encubierto digital, y es el agente encubierto como tal, del cual se citan algunas definiciones:

El agente encubierto ha sido definido, de modo general, como un funcionario de la policía que se infiltra en una organización criminal, cambiando de identidad, llevando a cabo tareas principalmente de represión y de prevención del delito, con el fin de ganarse la confianza del grupo, identificar a sus integrantes, obtener información en cuanto a su funcionamiento, financiación, etc., recaudar pruebas y, excepcionalmente, presentar testimonio de cargo ante la justicia(Ramírez Jaramillo, 2010, p. 27)

La Sala de lo Constitucional (2002), citada por la Sala de lo Penal, ha establecido lo siguiente:

“el agente encubierto es un miembro de la Policía que realiza funciones de investigación de delitos y que, por lo mismo, la competencia para autorizar este tipo de agentes ha sido otorgada por ley al Fiscal General de la República, en virtud que no se trata de una simple investigación, sino de una autorización a una persona para que delinca a efecto de comprobar la participación delincuencia de otra u otras personas integrantes de una organización delictiva con ello. (Sentencia Casación 9-CAS-2016, 2016, pp. 11, 12).

Es decir, la figura del agente encubierto presupone la existencia de crimen organizado en el cual no existe otra forma de permear su estructura y recabar información que pueda ser prueba en contra de los elementos que conforman dicha estructura.

En nuestro país el nombramiento del agente encubierto depende de la Fiscalía General de la República art. 282 C. Pr. Pn., y está considerada como una técnica de investigación del delito.

2.3.11. El agente provocador.

Es necesario advertir además que no se debe confundir al agente encubierto con el agente provocador.

En ese sentido, la Sala de lo Penal citando a Rey Huidobro (1991) ha establecido que:

El agente provocador (...) podemos definirlo, siguiendo a Muñoz Sánchez, como aquél que provoca a otro a la comisión de un delito con el fin de que el autor provocado sea castigado precisamente a causa de este hecho, sin que tenga voluntad de consumación del delito y poniendo para ello las medidas necesarias (2018, p. 7)

Es alguien que provoca a otro a cometer un delito, aquí el elemento principal es que el instigado en un primer momento no tenía la intención de cometerlo. Dicha figura es totalmente ilegal y no goza de valor probatorio.

En este sentido, la doctrina internacional tiene el mismo pensamiento: “el agente provocador no es tanto una figura diferenciada del AE como una patología, un mal obrar del policía infiltrado que invalida su actuación y descarta la presencia de un delito.” (Lafont Nicuesa, 2022, p. 53)

2.3.12. Agente encubierto digital.

El agente encubierto digital es una derivación necesaria del agente “tradicional” encubierto, como una especialización de este, pero con elementos que le hacen diferente, ya que su campo de acción no es “el mundo real” sino el “mundo informático”.

De lo antes expuesto y para tener una mejor comprensión es necesario citar los siguientes conceptos:

A) Concepto de agente encubierto informático.

El concepto de agente encubierto informático se construye como una especialización de la figura del agente encubierto, por lo que comenzaremos diciendo qué debe entenderse por este último. ”.(Sanchis Crespo & Velasco Núñez, 2019, p. 514)

Como el miembro de policía judicial que debidamente autorizado por el juez de Instrucción para investigar delitos castigados con pena superior a un año de prisión, estén o no relacionados con actividad de crimen organizado, se le habilita para interactuar mediante una identidad ficticia en un canal cerrado de comunicación con el fin de ganarse la confianza de investigado, incluso a través del envío o intercambio de material ilícito.(Lafont Nicuesa, 2022, p. 427)

Esta definición proviene de un autor español, país donde se legisló por primera vez esta figura, y en este país es requisito indispensable la autorización judicial para que lo recolectado por el agente investigador encubierto tenga validez, preceda autorización judicial.

La necesidad de dicho agente encubierto surgió con el apareamiento de nuevos escenarios para cometer delitos, en el mundo informático, en cuyo entorno las regulaciones para un mundo físico no se adecuaban y que por lo tanto generaban impunidad para los hechos que allí se cometieran.

Este medio de investigación aprovecha la infiltración de policías especializados en los grupos criminales. se trata de “(...) enfrentarse, desde dentro de la trama delincinencial a los crímenes más graves que nuestra sociedad conoce en el tiempo presente y, se justifica en la necesidad de establecer nuevas fórmulas o mecanismos que faciliten una óptima averiguación de los hechos delictivos investigados, así como las circunstancias organizativas y estructurales de la organización criminal investigada”.(Sanchis Crespo & Velasco Núñez, 2019, p. 514)

La razón se puede entender debido a que las personas que, por ejemplo, comparten cualquier clase de contenido ilícito, por regla general operan ya sea en la “Deep Web” o en la “dark web”, cuyo contenido no es asequible con navegadores normales como Google, Mozilla Firefox, entre otros.

Por lo tanto, es muy difícil permear esos grupos delictivos, por ello:

La nota definitoria del agente encubierto informático, la que principalmente lo distingue del agente encubierto es, como dice el art. 288 bis núm. 6 LECrim, su actuación “(...) en comunicaciones mantenidas en canales cerrados de comunicación (...)”. Junto con esa nota existen otras dos diferencias. Por un lado, su autorización es competencia exclusiva del juez instructor y por otro, su actuación se extiende no solo a los delitos del núm. 4 del art. 288 bis, sino también a los delitos típicos de las medidas de investigación tecnológica, como inmediatamente tendremos ocasión de ver. (Sanchis Crespo & Velasco Núñez, 2019, p. 516)

Entonces en España, dado el nivel de intrusión que se tiene en la intimidad de la persona investigada, se hace necesario la aprobación judicial de dicha medida de investigación.

En el art. 282 bis.6) de la LECrim regula la figura del agente encubierto informático, que consiste en la actuación bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación, con la oportuna autorización judicial para el descubrimiento de los delitos enumerados en el art. 282 bis.4, o de los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación, o a través de un servicio de comunicación. (Cortéz Domínguez & Moreno Catena, 2019, p. 274)

2.3.13. El ciber patrullador.

Es el policía que ocultando que lo es, interacciona con terceros en canales abiertos de comunicación con el propósito de detectar y prevenir delitos sin que tenga indicios concretos sobre su comisión. No necesita autorización judicial o del Fiscal. (Lafont Nicuesa, 2022, p. 430)

2.3.14. Canales cerrados. (PEER TO PEER o P2P).

González, 2008, citado en Mellado, define estos canales como: las comunicaciones mantenidas en un canal cerrado de comunicación son aquellas que se caracterizan por la expresa voluntad del comunicante de excluir a terceros del proceso de comunicación. (2017, p. 103)

Resulta fundamental precisar la noción del canal cerrado de comunicación. Para la STS nº 249/2008, de 20 de mayo dichos canales “se caracterizan por la expresa voluntad del comunicante de excluir a terceros del proceso de comunicación”(Lafont Nicuesa, 2022, p. 428)

2.3.15. Internet abierta.

Para entender lo que significa lo que es internet abierta, es necesario tener claro qué significa “*internet*”, por ello en una definición técnica significa:

Técnicamente, internet es un sistema global de dispositivos interconectados que utiliza la familia de protocolos TCP/IP para dar servicio a varios miles de millones de usuarios en todo el mundo. Después de tres décadas de evolución y adopción, Internet se ha convertido en una red de redes diversificada y en evolución que consta de millones de conexiones privadas, públicas, académicas, empresariales y de administraciones, de un alcance que va desde local a mundial, y que se gestiona a través de una amplia gama de tecnologías con cable e inalámbricas (UNESCO, 2013, p. 2)

Es decir, internet es la intercomunicación de computadoras, teléfonos inteligentes, o cualquier otro mecanismo que tenga la capacidad de conectarse, y por medio de los cuales se puede compartir información.

En el proceso de evolución de Internet, surgió un momento crítico que marcó para siempre la historia de la red y de la sociedad en general, este hito ocurrió en marzo de 1989 con la propuesta por parte de Tim Berners-Lee⁸ de lo que sería la World Wide Web -desde ahora- (www) y sus conceptos de hipertexto e indexación del contenido, para que pudiera estar disponible a todo el público. Esta tecnología se convierte en la piedra angular para entender la diferencia entre la Surface Web y la Deep Web.(Romero, 2018, p. 8)

2.3.16. Surface web.

Teniendo en claro lo que internet significa debemos pasar entonces a lo que significa "*internet abierta*", para ello el sistema interamericano de derechos humanos, a través de la Comisión, ha establecido lo siguiente:

Esta nueva necesidad trajo consigo la creación de un nuevo término, motor de búsqueda: "*Archie*", para muchos se instauró como el primer motor de búsqueda en la historia, o por lo menos el primero usado masivamente, indexaba archivos descargables vía FTP y guardaba sus vínculos en una base de datos que permitía la consulta para los usuarios interesados. Los primeros motores de búsqueda seguían el principio de buscar palabras clave dentro de los sitios almacenados, guardarlas, clasificarlas de acuerdo con la cantidad de veces que se repetía esta palabra, y ofrecer una interfaz amigable para que

el usuario pudiera encontrar lo que deseaba de acuerdo a esos criterios. (Romero, 2018, p. 9) este motor de búsqueda fue el primero en existir.

2.3.17. Motor de Búsqueda.

Existe un parámetro claro para establecer lo que es internet pública y lo que es Deep web y Dark Web: si las páginas pueden ser visitadas por motores de búsqueda, éstos pertenecen a la internet pública, pero si los motores de búsqueda no pueden tener acceso a esas páginas, contenido archivos, etc. Estas páginas pertenecen ya sea a la Deep Web o a la Dark Web.

La “navegación” al inicio del internet, implicaba que el usuario debía conocer la dirección de la página web a visitar.

Las ventajas que conlleva el apareamiento de la internet es innegable: permitió compartir archivos, de manera remota, supuso la muerte de algunos medio de comunicación clásicos: como la carta, educación a distancia por correspondencia, etc; además en esta época de pandemia Covid- 19, la internet permitió la potencialización de la educación online, a través de plataformas educativas. Por ello, el acceso a la internet se está configurando como un elemento necesario de las personas, el cual permite su desenvolvimiento en el nuevo mundo digital.

El concepto de apertura y libertad en la red se explica a partir del desarrollo de estándares técnicos, como la interoperabilidad, las interfaces de aplicación abierta, los documentos, texto y data abiertos, así como en la ausencia de limitaciones o trabas que favorezcan artificialmente monopolios o plataformas arcaicas.(COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, 2017, p. 17)

Como ya se dijo anteriormente, esta herramienta surgió como una necesidad para hacer frente al crimen organizado de pornografía infantil, ya que éste utiliza sofisticados mecanismos de DEEP WEB.

Definimos como Deep Web todo aquel contenido de Internet: redes, sitios, bases de datos, mensajería, sistemas de intercambio de ficheros, etc. Que por voluntad propia o como consecuencia de alguna tecnología aplicada, no permite que sus contenidos sean indexados en los motores de búsqueda de la Surface Web. La Deep Web no es una red física separada, si no una capa de aplicación y protocolos montada sobre las redes existentes. La Deep Web también es parte de Internet. (Romero, 2018, p. 10)

2.3.18. Deep web.

Definimos como Deep Web todo aquel contenido de Internet: redes, sitios, bases de datos, mensajería, sistemas de intercambio de ficheros, etc. que por voluntad propia o como consecuencia de alguna tecnología aplicada, no permite que sus contenidos sean indexados en los motores de búsqueda de la Surface Web. La Deep Web no es una red física separada, si no una capa de aplicación y protocolos montada sobre las redes existentes¹². La Deep Web también es parte de Internet. (Romero, 2018, p. 10)

2.3.19. Dark web.

Un concepto que es necesario clarificar en este escenario es el de las Dark Nets. Aunque es parte de la Deep Web, la Dark Web está formada por redes exclusivas cuyo acceso se encuentra restringido a aplicaciones específicas creadas para cada una de ellas, estas redes son conocidas como Dark Nets. Se deben diferenciar estos dos conceptos que, si bien son cercanos, no son iguales. Tor, I2P, Free Net, Resilio, GnuNet, etc. son Dark Nets. (Romero, 2018, p. 39)

2.3.20. Canales abiertos.

Ahora veremos el punto más álgido de diferencia entre la normativa española y la normativa salvadoreña, en ese sentido en España, en relación a los canales abiertos (Surface internet, común), se dice:

En estos casos cabría señalar, que es posible que en los canales de comunicación abiertos, no era necesaria parece la autorización del Juez o del Ministerio Fiscal, así por ejemplo lo entiende la Sentencia del Tribunal Supremo 767/2007, de 3 de Octubre, pues explica que el uso del nickname se llevó a cabo en espacios públicos y en funciones de prevención. De modo que, en los canales abiertos donde además no es precisa la identificación previa personal, no habría conveniente en que el funcionario policial actuara con ese nickname, más aún cuando en esos escenarios es normal el uso de estos, los cuales nunca corresponden a nominaciones reales, sino fantasías y apodos.(María de las Nieves Jiménez López et al., 2017, p. 591)

En nuestro país la redacción, establece el agente encubierto digital se establece para la Surface internet, lo cual para los españoles no tiene ningún sentido, porque no se necesita entrar a ningún círculo restringido, sino que cualquier policía lo podría realizar encriptación y seguridad para poder operar impunemente, en ese sentido Cruz Yagué, (2013) citado por Nicuesa, establece que se podría equiparar a una especie de pirámide, en la cual tenemos una base en la cual hay gran cantidad de usuarios que no toman muchas medidas de seguridad en cuanto a la difusión pero que el contenido que intercambian tampoco es de excesiva gravedad o es contenido poco actual o ya muy difundido... Según vamos subiendo la pirámide, los usuarios toman más medidas de seguridad y el material es más violento, con contenido más grave, o incluso material que se produce ya por redes organizadas que mueven dinero por intercambiar este material. En estos sistemas de intercambio ya entrarían...incluso en foros cerrados, a los cuales para acceder es necesaria la invitación de uno de los miembros, y el contenido está cifrado. al pedir invitación de alguna de las personas que ya componen ese grupo, se garantizan que nosotros no vamos a poder acceder. (2022, p. 421,422)

2.3.21. Evidencia digital.

Definición

Se considera evidencia digital: los documentos digitales, mensajes electrónicos, imágenes, videos, datos y cualquier tipo de información que sea almacenada, recibida o transmitida a través de las tecnologías de la información y comunicación o por medio de

cualquier dispositivo electrónico, serán admisibles como prueba y valorados conforme a la sana crítica establecidas en este código y en el Código Penal. (*Decreto Legislativo 280*, 2022). El Código Penal es claro y específico al establecer la información que será considerada como evidencia digital, esto para efectos de producción de prueba dentro de todo proceso penal.

El autor Raúl Velarde, la define como todo registro informático almacenado en un dispositivo informático o que se transmite a través de una red informática y que pudiera tener valor probatorio para una investigación. Se considera evidencia digital a cualquier información que, sujeta a una intervención humana, electrónica, y/o informática, ha sido extraída de cualquier clase de medio tecnológico informático –computadoras, etc. Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas técnicas especiales. (Velarde Callirgos, 2017, pág. 15); con ello es de hacer notar, que la doctrina esta acorde a lo establecido con la normativa de nuestro país, en cuanto a la evidencia digital, dando una definición mas amplia y explicativa.

Principios de la Evidencia Digital

La evidencia digital se rige por tres principios fundamentales: relevancia, fiabilidad y suficiencia. Estos tres principios son importantes para todas las investigaciones, no sólo para que las pruebas digitales sean admisibles en los tribunales. La evidencia digital es relevante cuando se trata de probar o refutar un elemento del caso específico que se está investigando. Aunque la definición detallada de “confiable” varía entre las jurisdicciones, el significado general del principio, “para asegurar la evidencia digital es lo que pretende ser” es ampliamente celebrado. el concepto de suficiencia significa que necesita reunir suficiente evidencia digital potencial para permitir que los elementos de la materia sean examinados o investigados adecuadamente. (Mesa Elneser, n.d.), pag.15

2.3.22. Clasificación de la tipología de la información en las redes (red oscura, red pública y red privada)

Red Pública

Una red pública es un tipo de red en la que cualquier persona, es decir, el público en general tiene acceso y, a través de ella, puede conectarse a otras redes o a Internet. Esto contrasta con una red privada, donde se establecen restricciones y reglas de acceso para relegar el acceso a unos pocos seleccionados. Dado que una red pública tiene pocas o ninguna restricción, los usuarios deben tener cuidado con los posibles riesgos de seguridad al acceder a ella, los navegadores que se utilizan para acceder a los sitios de la red pública se encuentran: Google Chrome, Firefox, internet explore, safari; y suelen identificarse como operadores de registro como: (.com) y (.org). (techopedia, 2022b)

Red Privada

Una red privada es cualquier conexión dentro de una red específica en la que se establecen restricciones para promover un entorno seguro. Este tipo de red se puede configurar de tal manera que los dispositivos fuera de la red no puedan acceder a ella. Solo un conjunto seleccionado de dispositivos puede acceder a este tipo de red dependiendo de la configuración codificada en los enrutadores de red y puntos de acceso. (techopedia, 2022a)

Red Oscura

La web oscura se refiere al contenido que los buscadores no indexan y que requiere una autorización o algún software especial para acceder a él. El contenido de la web oscura se encuentra en la Internet oscura: una parte de la red que solo es accesible mediante ciertos navegadores o configuraciones de red determinadas.

La Internet oscura está diseñada para proporcionar anonimato, ya que garantiza la privacidad de las comunicaciones cifrando y enrutando el contenido en línea a través de varios servidores web. Aquí es donde entra la parte «oscura»: acceder a la web oscura requiere utilizar software específico que le proporciona anonimato.

Si bien la web oscura suele describirse como un foro anárquico para la actividad delictiva, no es necesariamente cierto. La red oscura se trata simplemente de un espacio anónimo de la red al que se puede dar un uso inadecuado o un uso útil.

La forma más rápida de acceder a la web oscura es descargar e instalar el navegador Tor, que dirigirá su tráfico a través de la red Tor y le dará acceso a la web oscura. En Tor, puede escribir cualquier URL que le gustaría visitar, incluidos dominios. *unión de la web oscura.*(Belcic & Nelson, 2020)

RED PUBLICA	DEEP WEB.	RED OSCURA
<p>SURFACE WEB</p> <p>Aquí están todos los sitios que están indexados y que se pueden acceso con cualquier navegador (Mozilla, Chrome, Firefox, etc.)</p> <p>Se le conoce como canales abiertos.</p>	<p>CANALES CERRADOS (comunicación que se utiliza para excluir terceros)</p> <p>Aquí tenemos las bases de datos de los bancos, universidades, bibliotecas de paga virtuales, archivos Bit torrent, etc.</p>	<p>DARK WEB</p> <p>(red oscura, en el que se puede navegar de forma invisible, existen buscadores como Tor, que permiten su navegación de forma anónima. Esta se caracteriza: por no tener indexación de páginas web, por parte de los motores de búsqueda de la red superficial (Google); tiene túnel de tráfico virtual con infraestructura de red aleatoria; es inaccesible para los navegadores tradicionales).</p> <p>Se aquí se encuentran las redes de comunicación de los gobiernos e intercambio de material ilegal (pornografía infantil, armas, tráfico de drogas, etc.)</p>

Relación con los derechos fundamentales y necesidad de control judicial.

Con relación a la red pública, está por ser una web abierta o también llamada red superficial, en la que los sitios web que esta contiene son disponibles para el público, es por ello que se puede acceder por medio de cualquier buscador común o tradicional (Google chrome, Firefox, internet explore, safari), y sin restricciones; por lo cual resulta posible inferir con relación al tema de investigación, que en los casos de tener acceso a este tipo de red, ya sea por una persona particular o bien así que medie una investigación judicial, en este caso por parte del agente encubierto digital, no resulta necesario e indispensable que se cuente con una autorización judicial puesto que no se recae en una intervención a los derechos fundamentales del propietario de la información contenida en esta red, ya que desde el momento que se tiene acceso o se introduce información en ella se tiene en claro conocimiento que es de índole público.

Definimos como Deep Web todo aquel contenido de Internet: redes, sitios, bases de datos, mensajería, sistemas de intercambio de ficheros, etc. que por voluntad propia o como consecuencia de alguna tecnología aplicada, no permite que sus contenidos sean indexados en los motores de búsqueda de la Surface Web. La Deep Web no es una red física separada, si no una capa de aplicación y protocolos montada sobre las redes existentes. La Deep Web también es parte de Internet. (Romero, 2018, p. 10)

La red oscura inicialmente fue utilizado por los usuarios conocidos como hackers y los delincuentes, con el propósito de hacer un uso de ella en cuanto a información ilícita; como bien es sabido en este sitio es donde se encuentra información relacionada con la pornografía, la venta y tráfico de órganos y así otros tipos de ilícitos sancionados ahora en la Ley Especial de Delitos Informáticos y Conexos; en esta web los usuarios pretenden mantenerse en anonimato, tener información en sitios que resultan imposible de rastrear o de acceder; y que puede ser utilizados tanto por usuarios como por sus proveedores para actividades ilícitas; puesto que en este existe una restricción para su acceso, ya que únicamente se puede acceder a través de navegadores especializados (no así los comunes o tradicionales); no obstante esta red oscura no es ilegal en términos generales, ya que existe la posibilidad que usuarios la utilicen ya sea para mantenerse en anonimato o por la

máxima seguridad de la información que en esta se pueda tener, pero también por estas características puede ser utilizada para fines ilícitos, por lo cual depende del fin de su utilización si resulta ilegal o no su uso, en ese orden de ideas, se puede establecer que debido al nivel de seguridad y de restricción para el acceso a este sitio web, las probabilidades del cometimiento de actividades lícitas, son mayores, por lo que no resultaría necesario, en caso de requerirse a acceder a la información de un sitio de este tipo, atendiendo a su característica y fines (puesto que se presta al cometimiento de delitos) no sería necesario para su investigación y acceso autorización de un juez, puesto que en esta esfera no vulneraría derechos fundamentales.

2.4. Bases doctrinarias.

2.4.1. Autorización judicial.

En España, dado el nivel de invasión en los derechos fundamentales del investigado, se hace imprescindible autorización judicial para su utilización, el artículo 282 bis LECrim, establece la necesidad de autorización judicial para que un agente encubierto actúe bajo identidad supuesta en actividades propias de la delincuencia organizada y exige nueva habilitación del órgano judicial competente para aquellas actuaciones investigadoras que afecten a derechos fundamentales (Arrabal Platero, 2019, p. 203)

Esa figura desde el año 2015 se ha añadido (art. 282 bis. 6 y 7) que el juez de instrucción, podrá autorizar a funcionarios de la policía judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a), el agente encubierto informático podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los algoritmos asociados a dichos archivos ilícitos si tiene autorización específica para ello. (Esparza Leibar et al., 2019, p. 193)

Su surgimiento se explica por el abundante contenido pornográfico que circulaba en aquel entonces por las redes y que no existía forma de investigarlo de manera eficiente,

por ello, el agente encubierto informático (AEI) fue introducido por reforma de la LO 13/2015671 como una figura necesaria para combatir de manera más efectiva el delito de pornografía infantil.(Lafont Nicuesa, 2022, p. 421)

Esta autorización previa actúa como hecho habilitante, requisito ineludible sin el cual no podría operar un miembro de la policía judicial con documentación supuesta, el objeto de esa autorización es proporcionar cobertura personal de su responsabilidad, actividad que sería imposible llevarla a cabo bajo autorización gubernativa, ni siquiera del máximo responsable de la investigación(López - Muñoz, 2019, p. 181)

Para la legislación española la autorización judicial es requisito habilitante, caso contrario la prueba recolectada carecería de valor alguno.

Resulta imprescindible un control judicial sobre la actuación del agente que vulnera el derecho fundamental a la intimidad de los investigados, en primer lugar, porque se trata de una medida que se extiende en el tiempo y por tanto la acción perniciosa sobre el derecho es más dilatada, sin solución de continuidad y abarcando todo un espectro que engloba numerosos aspectos de la vida del individuo, comunicaciones, relaciones con personas, aficiones, domicilio, necesidades íntimas físicas y de credo y un largo etcétera; también porque los titulares de los derechos afectados ignoran la aplicación de ese medio de investigación.(López - Muñoz, 2019, p. 185)

2.4.2. Supuesto de aplicación.

Para la legislación española, tiene tipos penales específicos en los cuales se aplica el agente digital encubierto: los delitos del núm. 4 del art. 282 bis LECrim, son especialmente graves. Deben ser siempre realizados como delincuencia organizada en asociación de tres o más personas, para su realización permanente o reiterada. Se trata de los siguientes:

a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal.

b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal.

c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal.

d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal. (Sanchis Crespo & Velasco Núñez, 2019, p. 522)

En este punto inicial de la exposición, resulta conveniente señalar que el agente encubierto informático participa de un sustrato común básico que es idéntico al que inspira la regulación del agente encubierto presencial. De esta manera, la noción de agente encubierto en internet toma como punto de partida la construcción conceptual del agente encubierto presencial, habida cuenta de que, como se ha señalado, esta figura no constituye una creación ex novo del ordenamiento jurídico procesal actual. (Ascencio Mellado & Fernández López, 2017, p. 100)

2.4.3. Objetivo del agente digital encubierto.

El objetivo, por tanto, que cumple esta figura, es la de garantizar el éxito de la investigación penal, esto es, la averiguación del hecho delictivo, de su autoría... y de recabar toda la información susceptible de constituir prueba suficiente para enervar la presunción de inocencia. Se trata, como se ha puesto de manifiesto de una nueva medida de investigación tecnológica frente a la proliferación de delitos cometidos a través de internet. (Ascencio Mellado & Fernández López, 2017, p. 101)

2.4.4. Requisitos jurídicos para la admisibilidad de la evidencia digital según doctrina.

La doctrina expresa que es importante manejar la evidencia digital en tenor del criterio de la debida diligencia, que en nuestro ordenamiento jurídico se encuentra regulado en el Art. 83 del C. Pr. P., la Sala de lo Penal de referencia 17CAS2018, de fecha ocho de mayo de dos mil diecinueve, establece a través de jurisprudencia Internacional de Colombia, la Figura de la debida diligencia “sentencia marcada con la referencia No. 17001

11 02 000 2013 00024 01, emitida por el Consejo Superior de la Judicatura de Bogotá, Colombia, de fecha veintitrés de marzo del año dos mil diecisiete, que en lo pertinente, dice: "... cuando un abogado asume un compromiso profesional, se obliga a realizar todas las actividades en procura de cumplir las gestiones a él encomendadas, cobrando a partir de este momento vigencia el deber de hacer oportunamente las diligencias propias de la actuación profesional, compromiso que lleva consigo un actuar positivo al requerir prontitud y celeridad en el mismo, por tanto cuando el litigante se aparta injustificadamente de este deber, queda incurso en la infracción a la debida diligencia profesional ... se incurre en esta falta cuando se omite la gestión encomendada, igualmente cuando se demora en instaurarla, o cuando en su curso se quebrantan términos o se pierden oportunidades legales; cuando se desatiende el asunto, se atiende de manera ineficiente o de manera esporádica ... "(sic)".(7CAS2018., 2019, pág. 4)

La autora Ana Maria, establece que deben ser tomadas en cuenta las siguientes circunstancias para los requisitos:

- El aseguramiento seguro de la evidencia y de los datos del caso en el final del caso de la Corte si así que requerido. En nuestro país la reforma ha establecido la cadena de custodia para el aseguramiento de dichas evidencias.

- Preservación segura de los medios y de los dispositivos que sostienen la evidencia digital potencial por lo que posible, la preservación segura de la evidencia digital sí mismo y la preservación segura de los resultados de la investigación para la referencia futura posible.

- La notificación al tema de los resultados de la investigación.

El conocimiento científico, técnico u otro especializado ayudará al juzgado a entender las pruebas o a determinar un hecho en cuestión, un testigo aceptado como experto en virtud de su experiencia, conocimiento, destreza, la formación, o la educación,

puede atestiguarlo en la forma de una opinión. para ayudar a asegurar la admisibilidad de la opinión experta, se deben considerar los siguientes factores:

- Si las teorías y técnicas empleadas por el experto científico han sido probadas;
- Si han sido objeto de revisión por pares y publicación;
- Si se conoce una tasa de error para la técnica, debe reportarse;
- Si están sujetos a normas que rigen su aplicación;
- Si las teorías y técnicas empleadas por el experto disfrutan de una aceptación generalizada.

La admisibilidad de la evidencia misma y la admisibilidad de la opinión experta sobre la interpretación de las pruebas son, dos cuestiones diferentes a considerar. Por ejemplo, un testigo técnico puede ser capaz de testificar acerca de cómo se adquirió, preservaba, etc., la evidencia para abordar la idoneidad de esos procesos sin la necesidad de calificar como experto. En otras palabras, el experto también puede testificar de hechos técnicos. Consulte también ISO/IEC 27042: (Organización Internacional para la Estandarización, 2015).

Los requisitos de admisibilidad pueden variar considerablemente entre las jurisdicciones, por lo que es muy recomendable obtener asesoramiento jurídico competente en relación con los requisitos específicos. Sin embargo, muchas jurisdicciones incluirán al menos lo siguiente en sus requisitos de admisibilidad para evidencia:

- Relevancia: las pruebas deben tener cierta relevancia para los hechos en disputa.

- Autenticidad: la evidencia debe ser demostrada como lo que pretende ser. Por ejemplo, si una imagen JPEG particular extraída del disco duro de un servidor en particular es relevante para una cuestión de hecho en disputa, el Trier de hecho exigirá la garantía demostrable de que la unidad es de hecho de ese servidor en particular, que no ha sido modificado de cualquier manera desde su colección, que el proceso utilizado para extraer la imagen JPEG es digno de confianza, etc.

Es importante que se apliquen cuestiones jurídicas durante todo el proceso de investigación. Para todos y cada uno de los subprocesos, se debe realizar un control legal para determinar si se cumplen las leyes y reglamentos legales dentro de la jurisdicción particular. (Mesa Elneser, n.d. pag.16-17)

2.4.5. Uso de engaño en el agente encubierto digital en relación con el derecho de no autoincriminación y no declararse culpable.

El uso de engaño en el agente encubierto se manifiesta cuando comienza la investigación sin que el investigado tenga conocimiento de ella, en conclusión, puede verse afectado el derecho a la no incriminación en dos aspectos, el primero que durante la investigación se consigue prueba incriminatoria y en segundo lugar cuando el investigado no tiene conocimiento de la carpeta investigativa, así como también, siendo afectado el derecho de defensa del imputado.

En estas situaciones, considera López Barja de Quiroga, afectan al derecho de defensa, pues en ninguno de estos dos casos se informó previamente al investigado ni se le advirtió de que su declaración iba a ser utilizada en su perjuicio. A favor de admitir estos métodos, sin embargo, se arguye que es el investigado el que opta por no guardar silencio, pero ciertamente no estamos ante la prestación de una declaración espontánea, libre y voluntaria, sino mediante la utilización de engaño. Al ser los derechos a guardar silencio y a no declarar contra sí mismo "*derechos básicos que descansan en el corazón del concepto de juicio justo del art. 6 del Convenio Europeo de Derechos Humanos*"¹, el investigado debe

estar protegido contra procedimientos intimidantes o engañosos que alteren su voluntad.(Ascencio Gallego, 2017)

2.4.6. Derecho de defensa del imputado en relación con la prueba en la evidencia digital

En la resolución de la Corte Interamericana de Derechos Humanos en el caso Ruano Torres y otros vs. El Salvador, sentencia de 5 de octubre de 2015, manifiesta sobre el derecho de defensa: “el derecho a la defensa es un componente central del debido proceso que obliga al Estado a tratar al individuo en todo momento como un verdadero sujeto del proceso, en el más amplio sentido de este concepto, y no simplemente como objeto del mismo. El derecho a la defensa debe necesariamente poder ejercerse desde que se señala a una persona como posible autor o partícipe de un hecho punible y sólo culmina cuando finaliza el proceso, incluyendo, en su caso, la etapa de ejecución de la pena. (Antonio Sierra Porto et al., 2015, Pág. 45).

El derecho de defensa del imputado en relación con la prueba en torno a la evidencia digital, consiste en la legalidad del procedimiento realizado en la información sustraída de cualquier plataforma o dispositivo informático, confiable para la averiguación de la verdad y que se garantice el acceso a dichas evidencias, una vez terminada la investigación al imputado junto con su defensa técnica, en los delitos informáticos, como en cualquier delito, la importancia del derecho de defensa es que el imputado tenga conocimiento no solo de los hechos atribuidos sino también de la pruebas que se presentan en su contra, en contrario de los delitos informáticos en relación al agente encubierto digital el cual supone el retraso de dicho conocimiento.

En la sentencia de la Sala de lo Constitucional, de fecha diez de junio del dos mil once con referencia 94-2007, manifiesta que el derecho de defensa en términos generales implica, que toda persona objeto de imputación ante una autoridad judicial o administrativa, se presume inocente y debe asegurarse que el proceso se instruya con todas las garantías necesarias para ejercer su defensa. Asimismo, garantiza al detenido la asistencia de defensor en las diligencias de los órganos auxiliares de la administración de justicia y en los procesos judiciales, lo que se remite a la legislación secundaria a efecto de darle

positividad a tal derecho, al enunciar: “en los términos que la ley establezca”. (sentencia 94-2007, 2011, pág. 3)

En la doctrina el funcionamiento general del derecho de defensa en el imputado señala Nicolas González es en cuanto a que “el registro se realizará en presencia del interesado o de la persona que le represente. Dado el nacimiento del derecho a la asistencia letrada del imputado en el mismo momento en que se le atribuya la comisión de un hecho delictivo, debería darse a su abogado la posibilidad de asistir a la diligencia, cuando la entrada se haya producido y la realización del registro no sea urgente”. (González-Cuellar Serrano, 2008, pág.8)

Se considera que toda la evidencia digital recolectada, se lleve a cabo en reserva total en toda la investigación, porque la participación de ellos constituiría la destrucción de la prueba o desaparición de ella, para constituir la veracidad de la prueba recolectada en la investigación, el agente encubierto digital redacta informes, donde una vez iniciado el juicio inicia la defensa integral del imputado sin violaciones a sus derechos fundamentales como es la intimidad, el agente encubierto digital mundialmente fue creado para las investigaciones de organizaciones delictivas, delitos graves como secuestro, drogas, entre otros, que tienen complejidad, que necesariamente la intimidad se ve limitada, en este sentido, al momento de la investigación es necesario tener indicios suficientes para proceder a su violación, como una denuncia o un aviso de la víctima, prueba indiciaria del delincuente, para que estén amparados en una investigación justa.

Aunque el sujeto investigado no está en igualdad de condiciones en cuanto a su derecho de defensa, ya que no tiene conocimiento de las diligencias de investigación encubierto, pero que al tener la fiscalía indicios y tenga identificado el sujeto que delinque, inicia una investigación de la cual, el infiltrado bajo reserva respetando los protocolos de investigación y autorización por parte de la Fiscalía, su labor en el procedimiento tendrá valor probatorio, como ejemplo en nuestro país, en los casos de los Delitos de droga, que son delitos complejos, bajo una estructura, donde inicialmente se tiene prevista la figura del agente encubierto, en el caso de apelación de referencia ASDC-273-16, en la Cámara de la Tercera Sección de Occidente, en donde se autorizó un agente encubierto, ante el señalamiento de ilegalidad en el nombramiento del agente encubierto “Daniel”, la Cámara se pronunció “*que no existió evidencia de que el agente policial ejerciera algún tipo de*

fuerza, coacción o medio de presión prohibida para provocar la realización del acto por el cual es procesado el imputado MP, es decir, no se llegó a contaminar su voluntad en ningún momento; puesto que el agente encubierto “Daniel” sólo le llamó y le requirió la venta de la sustancia ilícita, accediendo con libertad el acusado al grado de indicarle el lugar donde le entregaría la droga.

Debe acotarse, que, si bien el agente encubierto se infiltró engañosamente, no encontró resistencia a la comisión del hecho que, con toda certeza, era conocido por el acusado como punible; es decir que el acusado MP actuó con libertad y espontaneidad, por lo que su actuar no puede estimarse como provocadora, ni atentatoria a los derechos fundamentales, en tanto su intervención se mantuvo dentro del ámbito de lo racional”. (sentencia ASDC-273-16, 2017, pág. 35)

En el caso antes relacionado, el agente encubierto, actuó bajo parámetros de legalidad probatoria, por lo tanto, el juzgador, lo valora al momento establecer su resolución, porque es útil para probar su participación en el delito que se le acusa.

El derecho de defensa en los delitos informáticos una vez asegurada la participación del imputado, presentado el requerimiento, debe manifestarse desde el inicio del proceso, pero la doctrina establece, que debe ser lo contrario, en el libro Nicolás González, que dice que “En la labor de recogida, apertura y copia de fuentes de prueba, aparatos, dispositivos o soportes de almacenamiento de información digitalizada la intervención del interesado (y si es posible de su defensa) ha de ser asegurada. También cuando, tras el registro, se procede a la apertura de los instrumentos informáticos aprehendidos y a la obtención de copias, actuación procesal en la que la defensa, al igual que todas las demás partes, tiene derecho a participar”. (González-Cuellar Serrano, 2008)

No obstante, a lo establecido por el autor, no se establece así en nuestro país, una vez que la fiscalía ha autorizado en determinado caso a la Policía Nacional Civil, el agente encubierto digital, se comienza a recolectar la evidencia, que una vez consolidada, con sustento probatorio, se judicializa, lo cual retrasa el conocimiento al imputado y su defensa, en ese sentido establece Nicolás González “cuando se declare el secreto del sumario el imputado y su defensa no tendrán derecho a conocer las actuaciones procesales ni la práctica de la diligencia de registro ni a participar en ellas. Ello supone la posibilidad de

realización de registros «subrepticios» cuya puesta en conocimiento al interesado se retrase.

Así mismo, para establecer y probar la culpabilidad como participación del imputado no basta con los informes realizados por el agente encubierto digital, deben ser corroborados con los técnicos que realizaron dichos informes para mayor veracidad de la información recolectada en el juicio y alcanzar mayor valor probatorio, así lo establece Nicolas González, “la pericia como medio de prueba no consiste sólo en la realización de un análisis y la redacción de un escrito, sino en su presentación, con las explicaciones que se soliciten por el tribunal y las partes, en el acto del juicio oral y público. Si la carga de la prueba de los hechos constitutivos de delito recae sobre la acusación le incumbe a ella solicitar la citación del experto al juicio para que el hecho quede probado mediante la pericia”. (González-Cuellar Serrano, 2008, pág.8)

En la investigación de los delitos informáticos dirigidos por el ente fiscal y realizados por la Policía, agente digital encubierto, deben trabajar acorde a las garantías constitucionales y las leyes secundarias, porque todo Derecho puede ser limitado, en aras de garantizar la pronta y cumplida justicia, haciendo un juicio de respeto a las garantías procesales.

2.4.7. Proceso penal: eficacia versus garantía.

El proceso penal es aquel sistema utilizado para realizar el ius puniendi del Estado, a través del cual se trata de averiguar la comisión de un hecho delictivo, se determina el autor y los demás partícipes, se impone una pena o una medida de seguridad a los indicados y, finalmente, se ejecuta la misma. (Real Academia de la Lengua Española, 2022)

En un estado constitucional de derecho, el proceso penal es una garantía, que regula el poder punitivo del estado, evitando que éste último se exceda en sus funciones afectando los derechos y garantías del acusado. El Estado siempre querrá tener más herramientas, que sean más fáciles de poner en acción, pero dichas herramientas pueden vulnerar derechos fundamentales del acusado, por ello es que encontramos una tensión entre la eficacia de la investigación y las garantías del imputado. Por ello, Ferrajoli establece que:

Según el tipo de derechos para cuya protección se establecen las “garantías”, es decir las técnicas idóneas para asegurar su efectiva tutela o satisfacción, pueden distinguirse aún diversos tipos o significados de garantismo... y específicamente penal, para designar las técnicas establecidas para la defensa de los derechos de libertad, sobre todo la libertad personal, frente a intervenciones policiales o judiciales arbitrarias; de garantismo social para designar el conjunto de garantías, todavía bastante escasas e imperfectas, encaminadas a satisfacer los derechos sociales, como los derechos a la salud, a la educación, al trabajo, etcétera. (Ferrajoli, 2006, p. 10)

Es decir, que las garantías procesales contenidas en la Constitución, en y en las diversas leyes penales vienen a limitar en el poder punitivo del Estado, estableciendo una serie de procedimientos, frenos y contrapesos, limitantes, requisitos y necesidad de autorización judicial para proteger de manera objetiva la persona del acusado quien carece de todo el andamiaje institucional que sí posee el estado.

En otro libro de Ferrajoli, establece un punto de vista necesario sobre la configuración de la necesidad de investigación del estado, y su limitación:

...garantismo penal y democracia política, entre seguridad y libertad, entre defensa social y derechos del imputado, del reo y del detenido, existe de facto una antinomia; que la legitimación del poder judicial, en otras palabras, no es «democrática», si por «democracia» se entiende únicamente voluntad del pueblo, y por tanto de la mayoría. La batalla por el garantismo penal, ha escrito Norberto Bobbio, siempre ha sido una «batalla de la minoría». (Ferrajoli, 2013, p. 191)

Para este autor existe una antinomia entre la necesidad de investigar y la necesidad de protección, dentro del contexto de la democracia, donde la investigación representa la voluntad general versus la protección que representa la voluntad de la minoría.

En el contexto de la investigación del delito, en casos de crimen organizado, para Cardoso Pereira, el estado siempre necesita de herramientas especiales ya que el crimen

organizado cuenta con dinero, logística y recursos que hacen nugatorio la investigación del mismo con las herramientas tradicionales. Por lo tanto, “son necesarias nuevas respuestas en el orden penal, en el plano procesal y en el marco de la cooperación internacional” (2012, p. 23).

Pero la necesidad de nuevas herramientas no puede ser una justificación universal para la violación de los derechos del acusado, sino que dichas herramientas deben estar reguladas por ley. Esto por supuesto como concreción consecuente del principio de seguridad jurídica y debido proceso, de orden constitucional.

En ese orden de ideas debe comportar un detrimento de la plena vigencia de los principios, derechos y garantías constitucionales, y la preservación de los aludidos principios, derechos y garantías exige, siempre que exista conflicto, que el mismo se resuelva en favor de estos últimos, porque ellos constituyen el verdadero fundamento de nuestro sistema democrático (BOE.Es - BOE-A-1999-846 Ley Orgánica 5/1999, de 13 de Enero, de Modificación de La Ley de Enjuiciamiento Criminal en materia de Perfeccionamiento de la acción Investigadora relacionada con el Tráfico Ilegal de Drogas y otras Actividades Ilícitas graves., 1999)

En el caso de la investigación, encontramos que la figura del agente digital encubierto se encuentra dentro del repertorio de herramientas que el Estado tiene para investigar el delito en el ámbito de los delitos digitales, pero dicha figura debe estar adecuadamente regulada por ley para poder tener ese control del mismo, lo que vendrá a ser una relación dialéctica eficacia- garantía de la investigación con los derechos del acusado.

2.4.8. Reconocimiento constitucional del derecho de defensa dentro del proceso penal.

El proceso penal es un campo de conflicto entre derechos individuales fundamentales e intereses sociales; el cual tiene como eje transversal la garantía del juicio previo, dentro de la cual resulta involucrada la inviolabilidad de la defensa siendo esta última, tema de interés en la presente investigación y la cual resulta ser una de las garantías básicas del proceso penal, da vida a la noción al debido proceso.

En ese sentido se entiende que la función de las garantías constitucionales, son como guías en el desenvolvimiento de la actividad procesal. Se trata de normas fundamentales que no van a restringir sus efectos a determinados actos o momentos del proceso penal, sino que su configuración va a permitir que proyecten su fuerza garantista – mecanismo de protección- vinculante a todos los momentos por lo que atraviesa el proceso penal.

Concretamente, la noción expresa que la garantía constitucional es nada menos que la idea plasmada en texto constitucional del ámbito de libertad de los contratantes y su consecuente imposibilidad de vulneración por parte de los órganos del Estado. La razón de la existencia de las garantías constitucionales radica en la necesidad de poner un límite al ejercicio del poder punitivo.

El derecho de defensa es uno de los derechos más antiguos, cuya concreción específica no surgió en un momento determinado, en la edad antigua, “era entendido como la atribución que tenía cada individuo de retribuir el daño que le era causado, ello en el marco de un sistema de justicia privada en el que primaba la ya famosa frase “ojo por ojo, diente por diente, llaga por llaga, tormento por tormento.” (Polo Palacios, 2020, p. 3)

A nivel español, también se ha reconocido la progresividad del derecho de defensa cuando se dice que:

“el derecho de defensa responde a una construcción histórica paulatina, acumulativa y sedimental (sic) en base a la cual, después de siglos de poderes absolutos, tiranías y anarquías, se ha ido abriendo paso el reconocimiento a unos límites básicos que aseguren que se administra la justicia en términos ajustados al progreso de nuestra civilización”.(Martí Mingarro, 2010, p. 23)

La evolución de la sociedad humana ha configurado el derecho de defensa como lo tenemos en la actualidad, los errores y aciertos del pasado estructuran el contenido del presente. Las peores facetas de la humanidad han necesitado soluciones, esas soluciones han estructurado dicho mecanismo de control: el derecho de defensa.

La Sala de lo Constitucional estableció que:

En virtud de ello, la Constitución consagra, en el art. 2 inc. 1° parte final, la protección en la conservación y defensa de los derechos de toda persona. El derecho a la protección en la defensa implica —en términos generales— la creación de mecanismos idóneos para la reacción mediata o inmediata ante vulneraciones de los derechos de las personas. (Corte Suprema de Justicia, s/f-a)

Esa protección se desarrolla en los siguientes niveles: “(i) el acceso a la jurisdicción; (ii) el proceso constitucionalmente configurado o debido proceso; (iii) el derecho a una resolución de fondo motivada y congruente; y (iv) el derecho a la ejecución de las resoluciones.” (Corte Suprema de Justicia, s/f-a)

Por ello la legislación secundaria debe desarrollar todo este sistema constitucional en aras del completo respeto a la dignidad del acusado.

El reconocimiento constitucional de la defensa, como mecanismo de protección, dentro del proceso penal, significa la exigencia que dentro del proceso penal; debe generarse igualdad de armas, que no debe haber nada oculto entre los adversarios, de hecho dentro de las reglas de prueba, existe una fase del descubrimiento en la cual el órgano persecutor; poner a disposición de la parte contraria toda la información recolectada, lo cual se hace inicialmente por medio del requerimiento fiscal y luego por medio del dictamen de acusación.

En ese mismo orden de ideas, cuando El Salvador optó por un sistema de tendencia acusatoria acogió con ello los principios básicos que rigen este sistema, uno de ellos, el de separación de funciones y Adversarial o entre partes, en donde corresponde a las partes probar y al juez decidir con base en la prueba ofrecida y practicada por las partes. Igualmente restringe esta norma el principio constitucional y legal de igualdad de las partes y obliga al juez a ser Imparcial, a ser el moderador del debate entre los intervinientes, a fin de que no desequilibre el proceso a favor de una de ellas. (arts. 4, 5 y 12, 209, 378 C.Pr.Pn.) (Aldana Revelo & Bautista González, 2014, p. 41)

La evolución del derecho penal y procesal penal, a partir de la implementación del sistema, acusatorio, en sustitución del modelo inquisitivo, busca convertir al imputado, de un simple objeto en un auténtico sujeto del proceso y es a partir del principio de inviolabilidad de la defensa que se matizan una serie de reglas que tienden a asegurar un juicio justo mediante el cual el acusado se encuentre en las condiciones de poder refutar y contradecir todo a la información recolectada. El principio de inviolabilidad de la defensa de traduce en una serie de reglas que tienden a asegurar un juicio justo.

Implicando que dicha garantía asegure al acusado:

- a) Conocer los cargos que se le imputan.
- b) Tener oportunidad para rebatirlos ante el Órgano Jurisdiccional.
- c) Poder presentar pruebas.
- d) Poder confrontar las presentadas en su contra, y,

e)

Contar con la asistencia de un abogado, desde el momento en que es citado por la autoridad policial.

Ahora bien teniendo en cuenta la implicancia de la defensa dentro del proceso, habrá que analizar como la utilización de la técnica del agente encubierto digital, colisiona con la garantía de la defensa, siendo que la misma se implementa sin que medie intervención judicial, pues habida cuenta dicha técnica limita derechos fundamentales y que no podría considerarse como un acto de investigación autónomo que no sea controlado por el juez, colocando al imputado en un estado de indefensión, frente a los operadores, quienes pudieran recolectar información incriminatoria, producida por el o personas con vínculos a este; mediante el agente encubierto, el Estado se infiltra en la vida de las personas investigadas, de modo secreto para poder obtener información acerca del iter criminis.

Lo que sucede es que esta práctica se materializa en una mayor injerencia en la esfera de la intimidad de esas personas investigadas, pues el policía infiltrado no sólo mantiene relaciones de confianza con los denominados ciberdelincuentes, sino que lleva a cabo actuaciones que, de conocerse su verdadera identidad, no hubiera podido realizar

Por consiguiente, el eventual problema que suscita la actuación de esta figura reside en la posibilidad de implicar un plus de lesividad en el ejercicio de los derechos fundamentales de esas personas investigadas (García Molina et al., 2017, p. 358)

2.4.9. El derecho de defensa

Se entiende por derecho de defensa a la garantía constitucional que le asiste a toda persona que posea un interés directo en la resolución jurídica del proceso penal para poder comparecer ante los órganos de persecución pertinentes, a lo largo de todo el proceso, a fin de poder resguardar con eficacia sus intereses en juego. (Dino Carlos, 2007, p. 13)

En la jurisprudencia salvadoreña encontramos la siguiente aseveración:

El proceso penal responde a un diseño en el cual las garantías fundamentales de los sujetos intervinientes constituyen la base sobre la cual ha de girar la búsqueda de la verdad y de la justicia en el caso concreto; es en ese contexto donde la defensa del imputado se convierte en una actividad esencial, proyectándose en dos modalidades: la defensa material y la defensa técnica. (Sentencia Casación Ref. 92-CAS-2006, 2006, p. 10)

En ese sentido la concreción del derecho de defensa se estructura en el siguiente desarrollo:

- Derecho a la asistencia de Abogado
-
- Derecho a ser informado de la acusación
-
- Derecho a guardar silencio, no declarar contra sí mismo
-

- Derecho a la confidencialidad y al secreto del abogado
-
- Derecho a ser asistido gratuitamente por un intérprete. (Martí Mingarro, 2010, pp. 23, 24)
-

2.4.10. El derecho de defensa como mecanismo de protección.

El derecho a defenderse es entonces, un mecanismo de protección que permite al acusado: oportunidad de negar, de aportar prueba de controvertir aseveraciones, por lo tanto, es una protección del acusado del poder punitivo del aparato estatal.

El derecho de defensa es un mecanismo de protección puesto que se establecen elementos que permiten controvertir la prueba en contra, aportar elementos de descargo e incluso, recurrir de resoluciones adversas.

En ese sentido la honorable Sala de lo Constitucional estableció que:

“la defensa en juicio se proyecta sobre todo en el proceso, fundamentalmente en el núcleo de su desarrollo, en el cual debe concederse a las partes una protección efectiva a sus derechos y categorías jurídicas protegibles a través de los medios de defensa que éstas consideren convenientes”. (Sala de lo Constitucional, 2007, p. 4)

Es decir, los litigantes deben tener la posibilidad real de poder controvertir las afirmaciones realizadas por la contraparte y en especial en los casos penales donde se juzga la libertad ambulatoria del procesado.

Luego en el año 2007, la misma Sala, estableció la concreción del derecho de la manera siguiente:

“... la defensa en juicio posibilita, mediante la contradicción, la oportunidad de defenderlas correspondientes posiciones en todo proceso,

en el que pudiere resultar afectado cualquier derecho constitucional que forme parte integrante de la esfera jurídica de alguno de los intervinientes, lo cual será posible mediante la aportación y alegación de los hechos que las conforman sustancialmente". (Sala de lo Constitucional, 2009, p. 3)

Por

ello podemos sostener que el derecho de defensa es el presupuesto de para toda la defensa del imputado, sin el cual no habría lógica, además el proceso mismo, como mecanismo de control en un estado constitucional de derecho carecería de legitimidad, por imposibilitar la defensa del imputado; en sentido contrario, entre mayor sea la posibilidad de defensa, mayor será la legitimidad del proceso como mecanismo de control, en todos y cada uno de diferentes estratos jurídicos que se apliquen a la persona procesada por un ilícito penal.

Lue

go la Sala en el año 2010, en sentencia bajo la referencia: 85 – 2008, de fecha 04 de marzo de 2010, establece las concreciones del derecho de defensa en la siguiente manera:

“al efecto, en la sentencia de amparo 714-99 de fecha 19/11/2001, se estableció que las diferentes oportunidades de defensa brindadas a lo largo de las sucesivas etapas de un proceso de cualquier naturaleza no son más que manifestaciones o aplicaciones en extremo del de audiencia, el cual es de naturaleza indisponible a la voluntad de los sujetos procesales, pues sus elementos y manifestaciones deben respetarse forzosamente por su naturaleza constitucional”. (2010, p. 1)

Est

a sentencia llama la atención en razón que es una cita directa de la sentencia de amparo 714-99, (Sala de lo Constitucional de la Corte Suprema de Justicia, 2001b, p. 6) y esta sentencia a su vez no establece como propia dicha aseveración, sino que la retoma de la sentencia del proceso de inconstitucionalidad bajo la referencia 4- 99, de fecha 28 de mayo de 2001, (Sala de lo Constitucional de la Corte Suprema de Justicia, 1999) y esta última, a su vez esta hace referencia a la sentencia bajo la referencia 8-97Ac de fecha 23 de marzo de 2001 (Sala de lo Constitucional de la Corte Suprema de Justicia, 2001a) llama la

atención por la amplia uniformidad de criterio, a pesar del transcurso del tiempo se tuvo a bien configurar el núcleo del derecho de defensa de esa manera: que el justiciable debe tener la capacidad de defenderse en cualquier etapa del proceso.

El derecho de defensa en la jurisprudencia de la Corte Interamericana de Derechos Humanos.

Para la CIDH, existe una importante jurisprudencia que involucra al Estado salvadoreño: el caso de Agapito Ruano, persona que fue detenida únicamente por un alias y que no se le garantizó el derecho de defensa de manera adecuada, por el cual el Estado de El Salvador, fue condenado a indemnizar al señor Agapito Ruano.

Con relación al derecho de defensa visto como mecanismo de protección se estableció en dicha sentencia lo siguiente:

158. el mismo sentido, el perito Binder sostuvo que el derecho de defensa comprende un carácter de defensa eficaz, oportuna, realizada por gente capacitada, que permita fortalecer la defensa del interés concreto del imputado y no como un simple medio para cumplir formalmente con la legitimidad del proceso...

160. En El Salvador, el mandato constitucional de asegurar a “[t]oda persona a quien se impute un delito, [...] todas las garantías necesarias para su defensa” se hace efectivo a través de la asistencia técnica que brinda la Unidad de Defensoría Pública a solicitud de toda persona que esté privada o amenazada de su libertad individual, sin distinción de nacionalidad, sexo, religión o condición económica. Según el artículo 33 de la Ley Orgánica de la Procuraduría General de la República, “[l]a Unidad de Defensoría Pública tiene por función ejercer la defensa técnica de la libertad individual a personas adultas y menores, a quienes se les atribuye la comisión de una infracción penal” (Corte Interamericana de Derechos Humanos, 2015, pp. 46, 47)

2.4.11. El Derecho de defensa en la Investigación del delito.

Durante la etapa de instrucción, en la investigación del delito; es una de las etapas cruciales donde se configura el derecho de defensa; la oportunidad de impugnar elementos de convicción, de exigir parámetros de oportunidad de investigación, el demandar cumplimiento de requisitos legales para la investigación; el oponerse a la realización de prueba donde el acusado actúe de manera activa en la aportación de evidencias; aquí encontramos una de las máximas materializaciones del derecho de defensa.

Dentro del proceso de investigación, el cual le compete al Ministerio Público fiscal, es importante hacer mención de una garantía existente como lo es “la garantía de objetividad del fiscal”, la cual para el doctor Carlos Manuel Romero Berdullas esta es considerada como el reaseguro ante la potencial arbitrariedad, tanto para el imputado como para las víctimas de los delitos, por tanto el contenido del conocimiento viene determinado por las cosas; y no por la voluntad del titular del ejercicio de la acción penal, quien en caso de actuar bajo su subjetividad fácilmente podría tocar a cualquier “inocente” en “presunto culpable” o a la inversa, cubrir a todo delincuente bajo el velo de la impunidad... si no ajustara su actuación a criterios objetivos. (Romero Berdullas, 2021, pág. 42)

El autor Mari Iván Verger Cazadero, hace referencia a esta garantía como uno de los principios que rige al Ministerio Público durante la investigación de un delito, estableciendo “que el principio de objetividad conlleva que la investigación debe referirse tanto a los elementos de cargo como de descargo, procurando recoger con urgencia los elementos de convicción, y actuando en todo momento conforme a un criterio objetivo, con el fin de determinar incluso, el no ejercicio de la acción penal o el sobreseimiento”. (Verger Cazadero, 2022, pág. 63)

El “Debido Proceso” es la base fundamental para una correcta impartición de justicia, requiriéndose el estricto cumplimiento y respeto de las garantías procesales establecidas en el marco legal de ámbito nacional como internacional. Para la Corte Interamericana de Derechos Humanos el derecho al debido proceso, es reconocido y llamado como “el derecho de defensa procesal”, consistiendo este en el derecho que le asiste a toda persona a ser oída con el cumplimiento de las debidas garantías y dentro de un plazo razonable por un juez o tribunal competente, independiente e imparcial, establecido con anterioridad por la ley en la sustanciación de cualquier acusación penal en su contra. (Alonso Salazar, pág. 102)

El derecho de defensa está estrechamente relacionado con la garantía al debido proceso, y consecuentemente con las garantías procesales, puesto que si estas últimas no se cumplen en el desarrollo del proceso, indiscutiblemente se estaría en ausencia del debido proceso y frente al irrespeto del derecho de defensa. Dentro de las garantías procesales que permiten percibir el perfil del derecho de defensa, están: 1) Juez competente, independiente e imparcial; 2) Presunción de inocencia; 3) comunicación previa y detallada al inculpado de la acusación formulada; 4) oportunidad y medios adecuados para preparar la defensa (derecho a interrogar testigos y perito y hacer que comparezcan a estrados judiciales; 5) derecho a ejercer la defensa, sea personalmente o bien mediante defensor técnico; 6) derecho del imputado a no ser obligado a declarar contra si mismo ni a declararse culpable(confesión), siendo esta valida únicamente si se realiza sin coacción; 7) “ne bis in idem” nadie puede ser castigado o sancionado dos veces por el mismo hecho punible; 8) publicidad del proceso penal; todas estas garantías se encuentran establecidas en la Convención americana de Derechos Humanos, en su art. 8.

Referente al derecho de defensa por parte del procesado, deberá ser ejercido desde que se le señala como posible autor de la comisión de un delito, lo que implica que su defensa no la ejercerá desde que inicie el proceso, sino desde la etapa de investigación hasta la ejecución penal, así lo concibe la CIDH en el art. 8.2.b “toda persona inculpada de delito tiene derecho a que se presuma su inocencia mientras no se establezca legalmente su culpabilidad. Durante el proceso, toda persona tiene derecho, en plena igualdad, a las siguientes garantías mínimas: ... comunicación previa y detallada al inculpado de la acusación formulada...”

En ese orden de ideas es necesario precisar, que el derecho de defensa no se activa por decirlo así, desde el momento que a la persona se le acusa formalmente de la comisión de un delito (inicio del proceso penal), sino que esta con base al derecho de defensa que le asiste (siendo este fundamental para el respeto a un debido proceso y así el cumplimiento de las garantías procesales), ejerza su defensa desde el momento en que tiene conocimiento o se le señala de ser presunto autor o participe del cometimiento de un delito, (puesto que le asiste el derecho a que se le informe de manera previa y de forma detallada la acusación en su contra), hasta la culminación del mismo incluyendo la fase de ejecución de la pena; caso contrario se recaería en la vulneración de las garantías convencionales, y con ello una posible afectación al derecho de defensa del imputado.

La Corte Constitucional de la República de Colombia, hace alusión al derecho de defensa en la sentencia bajo referencia Sentencia C-025/09, estableciendo:

“La jurisprudencia constitucional ha destacado la importancia del derecho de defensa en el contexto de las garantías procesales, señalando que con su ejercicio se busca impedir la arbitrariedad de los agentes estatales y evitar la condena injusta, mediante la búsqueda de la verdad, con la activa participación o representación de quien puede ser afectado por las decisiones que se adopten sobre la base de lo actuado. Acorde con ello, ha reconocido igualmente el derecho de defensa es una garantía del debido proceso de aplicación general y universal, que constituyen un presupuesto para la realización de la justicia como valor superior del ordenamiento jurídico” (Corte Constitucional República de Colombia, 2009)

Así también en la misma sentencia citada anteriormente, la Corte Constitucional República de Colombia, señala:

“... la Corte fue contundente en afirmar que, aun cuando la investigación previa es anterior a la existencia formal del proceso penal, la misma es determinante y básica para dar paso a la instrucción y el juicio, ya que en ella se define si la actuación debe continuar o no. Por esta razón, no existe justificación válida para restringir la participación del indagado en ella, pues resulta indispensable su protección desde el momento en que se ha iniciado una investigación en su contra, en procura de que pueda tomar oportunamente todas las medidas que establezca el ordenamiento para proceder a ejercer con equilibrio la defensa de sus derechos”.

La Sala de lo Penal de la Corte Suprema de Justicia de El Salvador, hace referencia a la intervención o participación del procesado o su defensor en los actos iniciales de investigación, citando lo establecido por la misma Sala e sentencia HC. 205-2009 del 30-06-2010, expresado:

“ Por ello se ha sostenido que los actos de investigación puede darse en una etapa anterior al inicio del proceso penal y en tal caso con ellos se pretende recoger elementos cuya eficacia depende de su pronta realización y que, a diferencia de los anticipos de prueba, no en todos los casos necesitan la intermediación judicial, ni el control de las partes, ya que el resultado de los mismos podría inclusive considerarse incierto, razón por la cual en esta fase no es requisito ineludible la presencia de un defensor pues no se puede juzgar anticipadamente que como consecuencia de las referidas diligencias surgirá

ineludiblemente una imputación penal.” (Sala de lo Costitucional de la Corte Suprema de Justicia, 2011)

Así mismo en la misma sentencia de HC. 94-07, la Sala efectúa una valoración en cuanto a la ausencia de la defensa técnica, en la práctica de “enlace de llamadas telefónicas” como diligencias iniciales de investigación, estableciendo:

“ ... se realizaron "actos extrajudiciales" que vulneraron su derecho de defensa por no estar presente defensor en las diligencias iniciales de investigación, específicamente refiere que en el momento en el que "se enlazaban las llamadas telefónicas" ya se le atribuía participación y tenía calidad de imputado; al respecto, es necesario aclarar, que este tipo de actos no revisten las características definidas para aquellos en los que sí se requiere la presencia de defensor. Esto es así porque no se realizan en la persona del procesado y tampoco constituyen actos de prueba definitivos, es decir, aquellos actos que requieren ser reproducidos dentro del proceso con la inmediación de las partes y del juez, para que puedan valorarse en la determinación de la responsabilidad penal del imputado, sino que se trata de actos de indagación que debían ser efectuados de forma inmediata, para determinar la existencia del delito en investigación y la persona posiblemente responsable del mismo; en adición a lo anterior, las diligencias iniciales de investigación sirven para dar origen a una imputación penal, trasladadas con posterioridad al conocimiento de una autoridad judicial, donde pueden ser controvertidas”. (Sala de lo Costitucional de la Corte Suprema de Justicia, 2017)

2.4.12. El rol del juez en los actos de investigación con control judicial

En la sentencia de 24-X-2005 (Inc. 2-2005), la Sala ha señalado que el proceso penal salvadoreño actualmente configurado, supone una relación triangular entre tres sujetos procesales: el *acusador*, el *defensor* y el *juez*. Se trata entonces de una estructura *tríadica* propia de los modelos de enjuiciamiento acusatorio, o próximos a dicho modelo, donde el juez se encuentra distanciado de las partes y su decisión está sujeta a un contradictorio oral y público.

Esta consideración del constituyente establece una nítida separación entre las funciones institucionales de perseguir y acusar, de las de juzgar y sancionar; poniendo cada una de ellas a cargo de distintos órganos diferenciados entre sí. Consecuentemente el legislador acogió tal planteamiento en el ordenamiento Procesal Penal vigente, en la

medida que tanto el requerimiento, la investigación preliminar y la acusación corresponden al ministerio público fiscal, y al juez queda reservada una función de *control y dirección del proceso*, que se acentúa en la fase de instrucción. (Sala de lo Constitucional, 2006, pág. 22)

Ello resulta claramente establecido en el inciso primero del art. 267 del C. Pr. Pn. que dispone: "el juez de Instrucción coordinará la investigación del hecho contenido en el requerimiento, procurando la mayor colaboración posible entre la Fiscalía General de la República, la policía, las partes y las autoridades judiciales".

El rol del Juez en los actos de investigación es fundamental para el esclarecimiento de un hecho, ya que el juez es garante de la legalidad en los actos de investigación, sometidos a inmediación y contradicción entre las partes, lo que en el proceso tiene valor probatorio. En el Habeas Corpus con referencia 13-04-00, se establece que: "El juez no se puede convertir en un receptor inerte frente a las afirmaciones del acusador, el principio acusatorio no significa tal cosa, pues el juez no puede ser un mero otorgante del pase de lo que expone el fiscal y puede añadirse en apoyo a lo anterior, que no basta con lo que afirma el fiscal, si esto no tiene un apoyo; pues si así fuera el mero relato sería eficaz para mantener en detención provisional a una persona".(Casado Pérez & Duran Ramírez y otros, 2018, pág. 359)

Según los estándares de la Constitución y el actual Código Procesal Penal, corresponde a la fiscalía el ejercicio de la acción penal y la dirección de la investigación del delito; pero no de manera independiente sino coordinada, en ese sentido: "la instrucción es la actividad realizada bajo la coordinación del juez competente (el juez de Instrucción), para obtener información que permita decidir si procede o no, efectuar un juicio penal y para asegurar su eficacia, en caso que se decida realizarlo."(Marroquín Galo, 2020, p. 2), por lo tanto se establecen actos de investigación que la fiscalía puede realizar de muto propio, pero existen otros que requieren actividad judicial previo a realizarse. Es aquí donde se maximiza el rol de juez en la investigación del delito: un coordinador y protector de la legalidad y derechos del imputado.

2.4.13. La información extraída al acusado, en la investigación frente a la prohibición de la utilización del engaño como método de recolección de información. [art.93. CPP]

En el artículo 93 del CPP, se establece una serie de restricciones en la investigación por parte del sistema y en beneficio del imputado.

La información extraída por el imputado en ningún momento puede ser bajo amenazas, violencia o incluso, engaño, si algún elemento probatorio es incorporado al proceso bajo estas circunstancias será excluido del elenco probatorio. En ese sentido, el Código Procesal Penal comentado establece que:

“no habiendo exclusiones a la regla, se le impondrá al imputado juramento o promesa de decir verdad, implica con ello que el imputado no ha de verter verdad sobre su dicho, o que diciendo verdad puede llevar inmersa en su declaración una afirmación o negación de los hechos” (Consejo Nacional de la Judicatura, 2018, p. 496)

Asimismo, en cuanto al engaño, para obtener información, tampoco tiene valor probatorio, y aquí es donde nos encontramos con un gran enfrentamiento en relación con el objeto de estudio: el agente digital encubierto utiliza el engaño para obtener información del investigado.

Ahora bien, el inciso 4° el art. 175 del CPP, establece una exclusión de la prohibición del engaño cuando establece que:

“No obstante, tratándose de operaciones encubiertas practicadas por la policía, se permitirá de medios engañosos con el exclusivo objeto de investigar y probar conductas delincuenciales del crimen organizado, delitos de realización compleja, delitos de defraudación al fisco y delitos contenidos en la Ley Especial contra Actos de Terrorismo, la Ley Contra el Lavado de Dinero y de Activos, la Ley Reguladora de las Actividades Relativas a las Drogas y la Ley Especial para Sancionar Infracciones Aduaneras, previa autorización por escrito del fiscal superior”

Es decir, se admite a raja tabla una excepción, pero estas excepciones no deberían ser autorizadas únicamente por el fiscal, sino que por el nivel de invasión en la persona del imputado deberían ser autorizadas por el juez para que tuviera un adecuado control jurisdiccional y no solo administrativo.

2.4.14. Valor de las diligencias de investigación en el juicio. [Art. 311CPP]

La preparación de la prueba comienza desde las diligencias iniciales de investigación que realiza la Policía Nacional Civil o en conjunto con la Fiscalía General de la República, toda prueba incautada o destinada a probar un hecho e incorporarse al proceso, a lo que se conoce como fuente de prueba, que se incorpora al expediente por un medio de prueba, sea documental, testimonial, entre otras, una diferencia de ellas es que La fuente existe con independencia de que llegue a realizarse o no un proceso; mientras que el medio cobra sentido en relación con un proceso y producirá efectos en un proceso concreto.(Lluch, 2012), el Valor de las diligencias de investigación en el juicio, solo pueden tenerlo si se ha efectuado por un medio de prueba regulado en el Código Procesal Penal, así lo establece el Art.311 inc. 2, del Código Procesal Penal, las demás carecerán de valor probatorio, en este sentido en el Código Procesal Comentado, establece que “los actos de investigación realizados durante las primeras diligencias como en la instrucción (excepto que sean prueba anticipada) no tienen valor como prueba.

Esta regla es correcta y se explica de la siguiente manera: desde una perspectiva lógica y jurídica, en el proceso penal se pueden distinguir una etapa de investigación o averiguación de los hechos delictivos y una de verificación o comprobación de los hechos. Durante la etapa de investigación se realizan todos aquellos actos tendentes a la búsqueda de las fuentes de prueba para identificar los elementos probatorios que han de practicarse, a través de los medios probatorios, ante el tribunal.”(Sandoval Rosales, 2018)

En concordancia con lo anterior, al respecto, la Sala de lo Constitucional de la Corte Suprema de Justicia, en la sentencia de las quince horas y treinta minutos del día 21/06/2013, Ref. 22010, romano III, al resolver sobre la inconstitucionalidad planteada del inciso tercero del Art. 6 de la Ley Contra el Crimen Organizado y Delitos de Realización

Compleja que se refería a que "el acta y el informe policial" serían incorporados mediante lectura a la vista pública, ha ejemplificado a las entrevistas de las víctimas como "actividades puras de investigación", y que no deben incorporarse al juicio o debate y, estableció:

"en resumen, los actos de investigación agotan su finalidad en el fundamento de la acusación, mientras que los actos de prueba en el convencimiento del juez acerca de la ocurrencia de la situación con relevancia delictiva. Por ende, dentro de un modelo de juicio de tendencia acusatoria, los únicos actos en los cuales puede fundamentarse una condena penal son los actos de prueba es decir los vertidos en el plenario mediante la contradicción y la inmediación y no los que reporta la investigación, a excepción que se trate de los denominados actos definitivos e irreproducibles"

En efecto, el estatuto procesal penal en vigor es claro en señalar en el inc. 2° del art. 311 C.Pr.Pn. que sólo "los medios de prueba reconocidos en este código tendrán valor para probar los hechos en el juicio, las demás actuaciones de la instrucción carecerán de todo valor".

Según la hermenéutica jurídica, se interpreta que las únicas excepciones que se admiten en el ámbito del juicio oral son aquellas relativas a la prueba testimonial anticipada, prueba preconstituida y actos urgentes de comprobación que sean incorporados conforme las prescripciones que el mismo Código Procesal Penal se encarga de estipular (art. 372 núm. 1° C.Pr.Pn.). De ello se desprende, que la generalidad de actas e informes que contiene el atestado policial conforme lo señala el inc. 2° del art. 276 C.Pr.Pn. carecen de relevancia probatoria a efectos de desvirtuar la garantía constitucional de la presunción de inocencia, y, por ende, no tiene sentido su incorporación en el debate."(Corte Suprema de Justicia, s/f-b)

2.4.15. Exclusión de medios de prueba obtenidos en las conversaciones entre el agente encubierto y el investigado.

La exclusión de la prueba obtenida por el agente encubierto será excluida, cuando recaiga en los siguientes tipos de prueba, según doctrina: Prueba Ilícita; por prueba ilícita debemos entender aquella en la que en su origen y/o desarrollo se ha vulnerado un derecho o libertad fundamental, es decir, en su génesis se han vulnerado derechos fundamentales o libertades públicas, o cuando se producen con la más absoluta inobservancia de las reglas de procedimiento, siempre que por esta causa se produzca indefensión. En este sentido como afirma ASECIO, del concepto de prueba prohibida o ilícita es posible extraer cuatro conceptos diferenciados: obtención, prueba, no surtirán efectos y directa o indirectamente. En cuanto al concepto de obtención, se refiere a que la infracción de la norma se ha producido en el momento de la búsqueda, recogida y adquisición de la fuente de prueba. Esto a lo que MIRANDA denomina ilicitud extraprocesal.

Prueba Ilegal. Debemos entender por prueba ilegal aquella que se obtiene sin vulneración de derechos fundamentales, pero sin respetar las normas de procedimiento legalmente establecidas en la ley siempre y cuando éstas causen indefensión. Esto supone aceptar que el acto realizado sin respetar las reglas del procedimiento será nulo y que siempre y cuando se cause indefensión no podrá ser tenido en cuenta como material probatorio apto para desvirtuar la presunción de inocencia. De este modo, cuando en un acto concurren estos dos aspectos (contravenir las reglas procedimentales y causan indefensión), el efecto es la nulidad de pleno derecho y, por tanto, nada de lo obtenido podrá ser utilizado en el proceso penal.

Prueba Irregular. La prueba irregular, será aquella realizada sin la observancia de los requisitos establecidos legalmente para el efecto, pero sin que con ello se cause indefensión. sí, cuando en el seno de la infiltración policial se llevan a cabo actuaciones tales como intervención de comunicaciones postales, telefónicas o electrónicas, captación de imágenes y sonidos en lugares cerrados, registros domiciliarios, por citar las más aplicadas, podemos encontrarnos con infracciones de las normas procesales que regulan estas diligencias. De este modo, en aquellos casos en que la legitimidad constitucional de la limitación del derecho fundamental queda asegurada.(Espinosa de los Monteros, 2009)

Según jurisprudencia en El Salvador, el agente encubierto tiene límites y más cuando se trata de violentar derechos fundamentales, en el ejercicio policial, en el momento que están investigando, se plantean límites, los cuales en principio, tales actividades de indagación pueden en algún momento entrar en colisión con algunos derechos y garantías fundamentales consagrados en la Constitución (entrada a domicilios privados, obtener conversaciones de contenido incriminatorio con los futuros procesados y grabarlas, etc.). Sin embargo, resulta posible conciliar la utilización de estos mecanismos de inteligencia policial, con los principios fundamentales que informan el proceso penal constitucionalmente configurado, por medio de la fijación de límites claros a su ejercicio y de un control judicial efectivo, así:

Deben utilizarse en el esclarecimiento de hechos delictivos relacionados con la criminalidad organizada. En consecuencia, no resulta posible su aplicación a la delincuencia de bagatela o de escasa complejidad.

Su uso ha de ser indispensable para superar las insalvables dificultades derivadas de la utilización de los medios convencionales de investigación y de prueba. En otras palabras, sólo podrá acudirse a esta técnica de investigación cuando la utilización de otras vías resulte inútil o cuando el esclarecimiento de los hechos resulte seriamente dificultado (principio de subsidiariedad).

Ha de existir autorización debidamente motivada por parte del fiscal general de la República, o de quien por delegación ostente la referida competencia de parte del funcionario arriba citado (en consonancia con lo establecido en la sentencia de 19-XII2003, pronunciada en el proceso de HC 236-2002). Entre otros requisitos, tal resolución debe indicar el plazo durante el cual se desarrollará la investigación.

La información obtenida por el agente encubierto debe ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación (información inmediata), y deberá ser aportada al proceso penal en su integridad. Conforme a ello, únicamente podrá ser utilizada con fines intraprocesales, con exclusión de otras causas criminales por otros hechos delictivos.

(v) La introducción al proceso penal de los datos obtenidos por el agente encubierto se encuentra condicionada al irrestricto respeto de las garantías constitucionales de defensa y contradicción (como elementos probatorios sujetos a valoración judicial dentro del juicio oral).

De acuerdo con lo anterior, tanto el imputado como la defensa han de tener: la posibilidad de una percepción visual del testigo; el conocimiento de los datos y circunstancias que él haya aportado a la causa, aunque únicamente ello se refiera a su identidad "infiltrada" y no real; por último, la posibilidad de interrogarle debidamente y formularle las preguntas pertinentes.

(vi) Por último, y no por ello menos esencial, la legitimidad constitucional de tales prácticas se condiciona a que las actuaciones policiales no provoquen o generen la idea criminal; sino, únicamente se limiten a constatar la realización delictiva e identificar plenamente a cada uno de sus intervinientes. (*Centro de Documentación Judicial, s/f*)

En este sentido, las conversaciones entre el agente encubierto digital encubierto y el investigado, es la última ratio, cuando concurren los siguientes requisitos: a) cuando la utilización de otras vías resulte inútiles, b) cuando el esclarecimiento de los hechos resulte seriamente dificultado en una investigación, es decir se deben agotar otras fuentes de prueba antes, de violentar derechos fundamentales, la sala en sus consideraciones ha manifestado, así mismo toda investigación autorizada por la fiscalía ha de ser fundamentada, es decir, que no es automático el grabar u obtener prueba incriminatoria, porque lo fundamental en el juicio son los actos de prueba, los que son sometidos a contradicción, inmediación y que están presentes las partes procesales.

En cuanto al agente encubierto realizadas por la Policía Nacional Civil en el Art. 175, que regula la legalidad de la prueba autoriza el uso de engaño para la obtención de prueba en relación a ciertos delitos los cuales son: crimen organizado, delitos de realización compleja, delitos de defraudación al fisco y delitos contenidos en la Ley Especial contra Actos de Terrorismo, la Ley contra el Lavado de Dinero y de Activos, la Ley Reguladora de las Actividades relativas a las Drogas y la Ley Especial para Sancionar Infracciones

Aduaneras, solo en estos casos se permite el menoscabo de derechos fundamentales en el curso de una investigación y no pueden ser excluidas como prueba por el juzgador.

2.4.16. La prueba digital y los derechos fundamentales

En la prueba digital por diversos autores, han existido diferentes posturas en cuanto su obtención, en este sentido, siempre ha sido sometido a debate los derechos fundamentales en el juego de la función funcional de la policía, el Estado protege al ser humano con todos los mecanismos que son las diversas leyes, pero sobre todo en la ley primaria que es la Constitución, es por ello la necesidad de justificar la limitación de los Derechos Fundamentales en un proceso Investigativo. Los derechos fundamentales que pueden ser sometidos a dicha delimitación son el derecho a la intimidad, Derecho a la no incriminación, lo cual, a través de la jurisprudencia y doctrina, se pueden establecer los parámetros, sobre todo en los delitos complejos, que son de complicada investigación y esclarecer la veracidad de un hecho.

La jurisprudencia en El Salvador establece que debe "distinguirse de su mera regulación. La regulación o configuración es la dotación de contenido material a los derechos fundamentales, es decir, la determinación de sus manifestaciones y alcances, las condiciones para su ejercicio, la organización y procedimientos que sean necesarios para hacerlos efectivos y la estructuración de sus garantías. Por otra parte, la limitación o restricción (también llamada intervención, injerencia o afectación) a un derecho, es un tipo de regulación que implica la modificación del objeto o sujetos del derecho, de forma que impide o dificulta el ejercicio de las acciones, posibilidades o situaciones habilitadas por él. Una limitación a los derechos fundamentales es válida o constitucionalmente aceptable cuando cumple los requisitos fijados por la ley suprema para efectuar dicha restricción: reserva de ley, justificación constitucional del fin perseguido, proporcionalidad de la medida (su idoneidad, necesidad y ponderación) y, finalmente, el respeto al contenido esencial del derecho". (Sentencias de 13-X-2010, Inc. 17-2006; y de 21-IX-2012, Inc. 60-2005).

Por lo anterior, la afectación de un derecho fundamental debe ser fundamentado y justificado, lo cual para el agente encubierto digital en el ejercicio de su dirección funcional en la investigación, debe tener en cuenta que para que una prueba se encuentre dentro

del parámetro de legalidad, debe tener un fin, es decir, una vez agotados todos los recursos para la obtención de prueba, proceder con los medio engaños, que es lo que protegen los derechos fundamentales, porque todo derecho puede ser limitado, siempre que se tenga la necesidad, para no recaer en una prueba ilegal o ilícita, pero en todo caso debe justificada y probada por el agente.

2.4.17. Tratamiento de la técnica de investigación del agente encubierto digital en el derecho comparado.

Esta es la primera legislación que reguló la figura, por medio de la reforma a la ley de enjuiciamiento penal, de fecha 06 de octubre de 2015, por medio del cual se reformó añadieron 2 nuevos apartados a dicha ley de la manera siguiente:

«6. El juez de instrucción podrá autorizar a funcionarios de la policía judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.

6. El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.

7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio.»(BOE.Es - BOE-A-2015-10725 Ley Orgánica 13/2015, 2015)

2.4.18. Derecho de defensa del imputado en la investigación de los delitos informáticos

El autor Jaime Robleto, considera que el Titular del Derecho de defensa es el imputado, quien debe ejercer por el mismo y otorgar un defensor particular o público (Robleto Gutierrez, 2013), los cuales según El instrumento Principios Básicos sobre la Función de los Abogados, **los abogados, al proteger los derechos de sus clientes y defender la causa de la justicia, procurarán apoyar los derechos humanos y las libertades fundamentales reconocidos por el derecho nacional e internacional, y en todo momento actuarán con libertad y diligencia, de conformidad con la ley y las reglas y normas éticas reconocidas que rigen su profesión.**(Principios Básicos Sobre la Función de los Abogados, 1990, pág. 3)

La defensa además de ser un derecho puede visualizarse como un poder dirigido lógicamente al mejoramiento de la situación procesal del imputado y obviamente se traduce en una actividad que parte desde el primer momento o de la atribuidad de un ilícito, hasta la eventual objeción de la pena. (Robleto Gutiérrez, 2013, pág. 47)

Es evidente que el abogado defensor posee autonomía de actuar, libremente en la defensa, es decir, que jurídicamente, su actividad en cuanto al imputado no puede conducir a causar un daño que sea deliberado a su defendido, su actividad debe lograr el mayor beneficio posible para él, sea logrando un resultado absolutorio, o bien una responsabilidad atenuada o una pena menos gravosa.

La resolución de la Sala de lo Constitucional manifiesta sus implicaciones en la investigación que establece “el derecho fundamental de defensa en términos generales implica una garantía esencial del proceso, en cuanto que toda persona objeto de imputación ante una autoridad judicial o administrativa se presume inocente y debe asegurarse que el proceso se instruya con todas las garantías necesarias para ejercer su defensa. El referido derecho se concretiza a través de actuaciones específicas del propio imputado: defensa material, y por medio de actuaciones a cargo de un técnico del derecho: defensa técnica. La primera, consiste en la intervención directa y personal del imputado en el proceso, realizando actividades encaminadas a preservar su libertad: impedir la condena u obtener la mínima sanción penal posible. La segunda, es la confiada a un profesional del

derecho, que interviene en el proceso penal para asistir y representar al imputado, rebatiendo los argumentos contrarios, interviniendo en las pruebas, o bien formulando conclusiones” (sentencia 172-04R, 2005), pág. 2

Según sentencia de la Sala de lo Constitucional 172-04R de las doce horas y tres minutos del día dieciséis de junio de dos mil cinco. “El derecho de defensa se encuentra establecido en el artículo 12 de la Constitución, el cual prescribe que: "...toda persona a quien se impute un delito se presumirá inocente mientras no se pruebe su culpabilidad conforme a la ley y en juicio público, en el que se le aseguren todas las garantías necesarias para su defensa."

Por lo que el artículo 9 del Código Procesal Penal lo desarrolla bajo el ese parámetro que dispone que "el imputado tendrá derecho a intervenir en todos los actos del procedimiento que incorporen elementos de prueba y a formular todas las peticiones y observaciones que considere oportunas...". (sentencia 172-04R, 2005, pág. 2)

En la jurisprudencia antes citada, el derecho de defensa del imputado es una esfera compuesta en primer lugar en el acceso a las diligencias de prueba que fundamentan la acusación fiscal, y garantizar su legalidad, en segundo lugar, que es inocente mientras se demuestre su culpabilidad y en tercer lugar su defensa técnica.

La figura del agente encubierto digital permite tener acceso a medios informáticos del imputado invadiendo su intimidad personal, es decir, verificar sus redes sociales, páginas web, entre otros, que sin tener conocimiento el sujeto investigado de la carpeta investigativa en su contra, lo que permite no tener control de ello en el procedimiento de las probatorio y verse afectado el Derecho de defensa.

2.4.18. Agente encubierto digital en El Salvador y la investigación.

2.4.18.1. Fundamentos

Con la avanzada evolución de las tecnologías y por ende el uso estas, el legislador en el marco nacional e internacional ha tenido que hacer grandes esfuerzos a través de la

creación de mecanismos para combatir y contrarrestar los delitos cometidos a través del internet; si bien es cierto no existe una terminología o concepto universal para este tipo de delitos, pero si son reconocidos por los juristas y la legislación como delitos computacionales, cibercrimen, delitos informáticos, etc., los cuales recaen en las acciones realizadas contrarias al uso determinado o específico por las personas por medio del internet, por decirlo así, el uso de estas sin la autorización del titular de una cuenta o con el mero uso premeditado para lograr un beneficio contrario a la ley; con relación a ello la Organización para la Cooperación y el Desarrollo Económico (OCDE) considera los delitos relacionados con sistemas de cómputo como *“cualquier comportamiento ilícito, no ético y no autorizado que involucra el procesamiento automatizado y la transmisión de datos”* (C. Velasco San Martín, 2012, p. 53)

En la doctrina española, para el Dr. Davara Rodríguez considera que los delitos informáticos se cometen por medio de la utilización de bienes o servicios informáticos; definiéndolos como:

“la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea lleva a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (C. Velasco San Martín, 2012, p. 52)

Y, como corolario de lo anterior se establece la regulación normativa de los delitos informáticos, a efectos de dar una seguridad “ciberseguridad” a las personas en el uso del internet, los cuales al igual que los delitos tradicionales requieren para su penalidad, de un proceso investigativo.

En todo proceso penal, debido a su naturaleza se requiere de la práctica de una investigación, esta con el propósito de reunir elementos que sustenten las teorías propuestas por las partes procesales al juez para la comprobación de la verdad y con ello razonar y justificar el grado de probabilidad de las resoluciones emitidas; por tanto, que este está integrado por actos de investigación y actos de prueba. En ese sentido es preciso señalar respecto que la investigación penal o investigación del delito: *“es el conjunto de diligencias orientadas al descubrimiento del delito, ejecutadas principalmente por los órganos de investigación penal”* (Piva Torres, 2021, p. 30)

Así la Sala de lo Penal de la Corte Suprema de Justicia, establece como finalidad de las diligencias de investigación el obtener, identificar o asegurar las fuentes de información que aporten resultados o respuestas lógicas o coherentes sobre la realización de un hecho ilícito y su presunto autor, citado en Libro de Reglas Prueba en el Proceso Penal Salvadoreño (Miriam Geraldine Aldana Revelo, 2014)

2.4.19. Investigación criminal y tecnología.

La Universidad Europea, con base a la criminología y respecto a las técnicas de investigación criminal, expresa, que la investigación criminal tiene como objetivo principal recolectar y obtener pruebas relacionadas con la comisión de un delito con el fin de descubrir con la mayor certeza los hechos acontecidos y el autor responsable de ellos. Con el transcurso del tiempo y el desarrollo de la sociedad, la tecnología se ha convertido en una herramienta esencial para investigar y resolver todo tipo de crímenes, así la tecnología ayuda a resolver los delitos en cuanto a:

1. Analiza la investigación. Permitiendo acelerar el tiempo de la investigación judicial para resolución de los casos, en comparación de décadas pasadas; esto a través de, por ejemplo: la implementación del sistema automatizado de huellas dactilares, los sistemas de reconocimiento facial; contribuyendo de esta manera a descongestionar el trabajo en los órganos judiciales.
2. Recopilar indicios y pruebas. En la investigación criminal, la tecnología puede ser aplicada para delitos tradicionales, (por ejemplo, un homicidio), así como también en delitos informáticos (hurto de identidad), puesto que las técnicas de investigación criminal existentes actualmente permiten, por ejemplo: rastrear e identificar huellas digitales de una persona, intervenir comunicaciones o darles seguimiento a su actuar para recabar información certera y fidedigna para la resolución de los hechos investigados. Facilitando así la recolección y el registro de indicios forense.
3. Mayor fiabilidad. Dentro de las investigaciones de delitos, la tecnología es una excelente aliada, puesto que proporciona información más confiable que permite

resolver casos complejos, por medio de procedimientos de investigación convencionales. Ejemplo: la identificación por ADN.

2.5. Bases legales.

2.5.1. Legislación.

El proceso evolutivo de la sociedad obliga a que las normas que la rigen se transformen al mismo tiempo, obedeciendo a factores socioeconómicos, tecnológicos, políticos, entre otros; un claro ejemplo al respecto es la evolución de la sociedad relacionada a las Tecnologías de la Información y la Comunicación (TIC), siendo notorio en las redes sociales y en su uso para realizar lo que popularmente se conoce como ciberbullyng o acoso, lo que extremadamente ha llegado en muchos casos a ocasionar el suicidio de jóvenes y adolescentes (Arteaga, 2015)

Como consecuencia de lo anterior, resulta la necesidad de un constante cambio en los ordenamientos jurídicos, a efectos de realizar una investigación eficaz de manera integral (marco legislativo – técnicas de investigación).

Con la creación de la figura del agente encubierto digital como una nueva técnica de operación encubierta para la investigación de los delitos informáticos y conexos, cometidos en el uso de las tecnologías de la información y comunicación en El Salvador, originándose esta para combatir el cometimiento de las conductas delictivas a través del internet; y, habiendo entrado en vigencia por Decreto Legislativo número 280, de fecha uno de febrero del año dos mil veintidós, y publicado en el Diario Oficial Tomo 434 de fecha cuatro de marzo del dos mil veintidós, por medio del cual se adicionó el artículo 259-D en el Código Procesal Penal, estableciendo:

“Art. 259-D. Agente Encubierto Digital y otras Técnicas de Investigación Informática. Durante la investigación de los delitos cometidos en la Ley Especial contra los Delitos Informáticos y Conexos u otros contenidos en leyes penales especiales y de conformidad a lo establecido en el artículo 175 inciso cuarto de este Código, podrá ordenarse la relación de operaciones encubiertas digitales que resulten necesarias, las cuales estarán a cargo de la Policía, previa autorización de la Fiscalía General de la

República . La fiscalía también podrá realizar la búsqueda a través de las Tecnologías de Información y Comunicación de carácter abierto y público, incluyendo las páginas de internet, de evidencia digital que constituya el hecho punible informático o pueda servir de prueba para el mismo, por medio de programas informáticos que le permitan identificar los valores únicos identificativos de tal evidencia digital, o mediante la búsqueda o indagación libre de tales espacios informáticos virtuales. La policía o la fiscalía podrán celebrar acuerdos con entes públicos o privados con sedes en otros países, que le permitan recibir y documentar noticias criminales de cometimiento de hechos delictivos de forma directa, inclusive mediante el uso de las tecnologías de información y comunicación; la información así recibida podrá ser incorporada al proceso como evidencia digital, conforme a las regulaciones de este capítulo

2.5.2. Configuración normativa del uso de la técnica de agente encubierto digital.

Con esta nueva técnica de investigación encubierta, el legislador autoriza a la policía para que con la autorización del ministerio público fiscal realice indagaciones por medio de programas informáticos en las tecnologías de la información y comunicación, de carácter abierto o público, con el propósito de potenciar la seguridad de aquellos derechos intangibles que las personas han adquirido y continúan adquiriendo con la utilización e interacción en el internet, debido a que los sistemas informáticos y de telecomunicación se han vuelto fundamental ya no solo en el ámbito social sino también en muchas otras áreas tales como: laboral, empresarial, financiera, operacional, etc. en el país y en el mundo. El avance y desarrollo de las tecnologías, ha generado vulnerabilidad para los sistemas de comunicación e información, convirtiéndose en objetos para el cometimiento de ilícitos, entre algunos: hurtos de identidad, estafa informática, acoso a través de tecnologías de la información de carácter personal y otros. Esta técnica será implementada en la investigación de los delitos establecidos en la Ley Especial de Delitos Informáticos y Conexos; dicha ley fue aprobada en El Salvador a través del Decreto Legislativo número 260, publicado en el Diario Oficial número 410 de esa misma fecha, en la que se recopilan los tipos penales vinculados con la ciberdelincuencia.

“El proceso de investigación en los delitos informáticos permite la aplicación de todas las diligencias reguladas en el Código Procesal Penal, así como los diversos actos urgentes de comprobación” (Fiscalía General de la República de El Salvador, 2018, p. 10)

En el artículo 201 del Código Procesal Penal, versa sobre el procesamiento de la información electrónica, específicamente sobre la obtención y resguardo de la misma, la cual según el tenor se accederá de manera electrónica en los casos que existan motivos debidamente fundados para inferir que un sujeto posee información almacenada en equipos tecnológicos de su propiedad o posesión y que la misma es constitutiva de delito o de utilidad en la investigación que se desarrolla. Haciéndose una relación comparativa de este artículo, con el artículo 259-D del mismo código, resulta la diferencia en cuanto a que, para los casos de investigación de la técnica encubierta digital no mediará autorización judicial para intervenir la información y comunicación tecnológica objeto de investigación, puesto que esta será realizada por la policía previa autorización únicamente de la Fiscalía. No obstante, dicha situación no generará ilicitud en la prueba obtenida, puesto que su legalidad recae en el artículo 175 inciso cuarto del Código Procesal Penal, en el que se establece:

“ No obstante tratándose de operaciones encubiertas practicadas por la policía, se permitirá el uso de medios engañosos con el exclusivo objeto de investigar y probar conductas delincuenciales del Crimen Organizado, delitos de realización compleja, delitos de defraudación al fisco, y delitos contenidos en la Ley Especial contra Actos de Terrorismo, la Ley contra el Lavado de Dinero y de Activos, la Ley Reguladora de las Actividades Relativas a las Drogas y la Ley Especial para Sancionar Infracciones Aduaneras, previa autorización por escrito del fiscal superior”

La carga de prueba le corresponde al ente acusador, es decir a la fiscalía, tomando en cuenta el derecho a la presunción de inocencia que asiste al imputado, pero si bien, tal y como lo establece la norma “ en los casos que existan motivos debidamente fundados para inferir que un sujeto posee información almacenada en equipos tecnológicos de su propiedad o posesión y que la misma es constitutiva de delito o de utilidad en la investigación que se desarrolla” , debe de tomarse en cuenta que para el caso de los delitos informáticos, no basta únicamente una duda razonable o sospecha, pues en caso de duda

para el legislador se considera lo más favorable al imputado, artículo 7 del Código Procesal Penal .

Es de hacer notar que, en el proceso de investigación, respecto a la obtención, resguardo y/ o almacenamiento de la información, se debe de tener en cuenta la legalidad de la prueba, desde su recolección como evidencia digital para estos casos, debiendo someterla a la cadena de custodia en el caso requerido art. 250- 252 Código Procesal Penal ; advirtiendo la aclaración que la cadena de custodia que se aplica es la “cadena de custodia tradicional” ósea la establecida en el Código Procesal Penal para los delitos “tradicionales”, por no tener regulada en el ordenamiento jurídico penal una cadena de custodia para específicamente en la investigación de los delitos informáticos y directamente para las evidencias recabadas por el agente encubierto digital.

2.5.3. Análisis comparado de la figura del agente encubierto digital.

2.5.4. Agente encubierto en El Salvador

El ordenamiento jurídico de El Salvador, en el Código Procesal Penal regula la evidencia digital estableciendo:

“ Art. 259A. – Para los efectos penales, se considera evidencia digital lo siguiente: los documentos digitales, mensajes electrónicos, imágenes, videos, datos y cualquier tipo de información que sea almacenada, recibida o transmitida a través de las Tecnologías de la Información y Comunicación o por medio de cualquier dispositivo electrónico, serán admisibles como prueba y valoradas conforme a las reglas de la sana critica establecidas en este código y en el código penal.”(Diario Oficial, 2022)

Con esta evidencia resulta necesario se practique un análisis especial, por peritos especialistas en el área, según corresponda a través de un proceso especial, puesto que, esta se convierte en prueba ventilada en el juicio, la cual ilustra al juzgador para este dictar una sentencia, por lo que se somete a un “análisis forense digital” , consistiendo este en la implementación de procedimientos y técnicas, científicas y analíticas especiales, que

permitan identificar, preservar, analizar y presentar resultados certeros y con validez dentro del proceso. Vinculándose lo anterior ampliamente con la “cadena de custodia”, regulada por cada ordenamiento jurídico, teniendo implícita esta la adecuada obtención de la prueba, su preservación e individualización, así como el transporte adecuado y su entrega controlada, para su incorporación en el proceso; ello a través de la cadena de custodia para la evidencia electrónica.

En el Salvador, la evidencia digital tiene carácter de prueba y será incorporada de acuerdo con lo establecido en el Código Procesal Penal, por lo que, para que esta sea admitida en el proceso debe de cumplir los requisitos de obtención, resguardo y almacenamiento, *requeridos en el art. 201 del Cód. Pr. Pn., en el cual se establece:*

“Cuando se tengan razones fundadas para inferir que una persona posee información constitutiva de delito útil para la investigación, almacenadas en equipos o instrumentos tecnológicos de su propiedad o posesión, el fiscal solicitará la autorización judicial para adoptar las medidas que garanticen la obtención, resguardo o almacenamiento de la información; sin perjuicio que se ordene el secuestro respectivo.

“Durante dispositivo de entrega bajo cobertura policial, operaciones policiales encubiertas, allanamientos, requisas penitenciarias o de cualquier lugar de detención y en los casos de flagrancia previa dirección funcional de la Fiscalía General de la República, la policía podrá adoptar las medidas que garanticen la obtención, resguardo o almacenamiento de la información almacenada en equipos o instrumentos tecnológicos y como secuencia de lo anterior, el Código Procesal Penal en el art. 259-C. establece las condiciones para la incorporación y producción de la evidencia digital, estableciéndose:

1. *“Acreditación de su autenticidad, lo cual puede ser realizado por cualquiera de los medios siguientes:*
2.
 - a) *Prueba testimonial de la persona que intervino directamente en la elaboración, generación, transmisión o recepción de la evidencia digital por medio de las Tecnología de la Información y Comunicación.*
 - b)

- c) *Acreditación de los mecanismos técnicos informáticos idóneos utilizados para su generación, que aseguren esa autenticidad, como puede ocurrir en el caso de la firma electrónica u otros mecanismos semejantes.*
- d)
- e) *Perito informático que haya intervenido en la obtención, resguardo o almacenamiento de la información o en el análisis de la evidencia digital, designado conforme a las reglas de este código.*
- f)

Las reglas de acreditación de autenticidad de la evidencia digital establecidas anteriormente, pueden ser aplicadas de forma independiente entre sí, por lo que cada una será suficiente para tenerla por acreditada; sin embargo, en el caso de las contenidas en los literales a) y b), si alguna de las partes impugna de manera fundada el mecanismo de acreditación dentro de la fase de instrucción formal, la parte interesada en la admisión de evidencia deberá demostrar su integridad por medio de la intervención de un perito informático, designado conforme a las reglas de este código.

- 3. *El acceso al contenido de la evidencia digital, en virtud del derecho a la intimidad que se puede ver afectado, tal como lo regula el art. 202 del Cód. Pr. Pn. requerirá orden judicial, la cual podrá ser solicitada por la fiscalía durante los actos urgentes de comprobación o diligencias iniciales de investigación al juez de paz competente, o durante la fase de instrucción formal al juez de instrucción que conozca de la imputación. Lo anterior no será necesario cuando se obtenga el consentimiento informado del titular del derecho a la intimidad que podría verse afectado; así como sus consecuencias legales si las hay, lo cual deberá registrarse por escrito; en el caso del imputado, además de su defensor, deberá acreditar que ha informado las consecuencias de la realización de la diligencia.*
- 4. *En caso de que sea necesaria la realización de la prueba pericial de la evidencia, se deberá cumplir con los requisitos establecidos para este medio probatorio por este Código; sin embargo, si el perito informático es de carácter permanente, los puntos de pericia podrán ser establecidos por el fiscal del caso, o solicitados al juez competente por requerimiento de las partes. Sin perjuicio de lo anterior las partes podrán acordar estipulaciones de la evidencia digital, en los términos establecidos en este Código.*

5. *El secretario del tribunal o quien disponga administrativamente la Corte Suprema de Justicia notificará de inmediato a las partes, citará a los testigos o peritos y solicitará los objetos y documentos y dispondrá cualquier otra medida necesaria para la organización y desarrollo de la vista pública. La producción de la evidencia digital podrá ser realizada en el proceso penal mediante el uso de cualquier método o recurso tecnológico, que sea idóneo para realizar la correcta presentación de la misma, inclusive con el apoyo de perito informático designado conforme a las reglas de este código.”*

2.5.5. Tratamiento de la evidencia digital en el proceso penal salvadoreño.

De acuerdo con lo prescrito en el art. 259- B del Código Procesal Penal, para los casos de evidencia digital, la policía, fiscalía y demás instituciones que intervengan en la incautación, procesamiento, análisis, ofrecimiento o producción de la misma dentro del proceso penal, deberán cumplir con lo dispuesto en los artículos del cuerpo legal antes citado, independientemente si la evidencia es obtenida de oficio o haya sido proporcionada por la víctima, un testigo o por el mismo el imputado. Resultando del aludido precepto legal, que a la evidencia digital, se regirá por la cadena de custodia establecida en los arts.250 – 252 del Código Procesal Penal ; aplicándose las reglas establecidas en el art. 251del mismo cuerpo legal, que expresa: “ las personas que hayan tenido contacto con los objetos y documentos incautados registrará toda la información necesaria para facilitar la constatación de autenticidad de los mismos en las diferentes etapas de su manejo o utilización, tales como recolección, embalaje, transporte, análisis y custodia. “

2.5.6. Ámbito internacional.

En razón del manejo y control adecuado que resulta para la evidencia digital, se hace alusión a un instrumento internacional de gran relevancia en el tema, como lo es la norma ISO/IEC 27037:2012, publicada por la Organización de Estándares Internacionales (ISO) en octubre del año 2012, conteniendo esta los fundamentos para la identificación,

obtención, adquisición y preservación de evidencia digital, siendo esta una guía para la realización de actividades relacionadas con el manejo de evidencia digital, tomando en cuenta los principios del modelo genérico Rodney Mckemmisk incluyendo cuatro etapas del manejo de evidencias electrónicas: i) Identificación; ii) recolección; iii) conservación; y, iv) preservación; sin incluir dicha norma la etapa del análisis de la evidencia. (C. V. A. Velasco San Martín, 2021)

Estas normas ISO, contiene directrices que sirven de lineamientos en cuestiones relacionadas al manejo o tratamiento de las evidencias digitales en una investigación, con el fin de apoyar a las organizaciones en los procedimientos realizados; siendo estos estándares internacionales, con aceptación por parte de la comunidad técnica y científica que tienen a su cargo la realización de funciones relacionadas con el manejo y análisis de evidencias digitales.

No obstante, estas directrices, no tienen carácter obligatorio o vinculatorio o más bien no son normas de obligatorio cumplimiento para las legislaciones de los países, quedando estas sujetas su aplicación por lo especialistas y responsables de los laboratorios forenses digitales.

2.5.7. Análisis comparativo del Art 24 Cn. y la regulación de la técnica del agente encubierto digital.

La figura del agente encubierto digital sin duda alguna puede menoscabar derechos a la intimidad personal y la inviolabilidad de la correspondencia, la cual como garantía constitucional tienen todos los habitantes de la República.

En El Salvador la honorable Sala de lo Constitucional ha establecido la siguiente acepción de esta garantía constitucional:

1.1) El artículo 24 de la Constitución establece: "la correspondencia de toda clase es inviolable, interceptada no hará fe ni podrá figurar en ninguna actuación, salvo los casos de concurso y quiebra", y el término "correspondencia", alude a la comunicación postal, es decir, a la transmisión explícita de mensajes entre personas que no se encuentran en el mismo sitio, y cuya comunicación se

propicia mediante un soporte físico que es confiado a un tercero; por tanto, la protección constitucional en comento se dispensa a objetos mediante los cuales se transmiten mensajes a través de signos lingüísticos. (Sala de lo Constitucional de la Corte Suprema de Justicia, 2008, p. 6)

Par
ecería que la protección se circunscribe únicamente a la correspondencia física, pero en la misma sentencia establece lo siguiente:

Debe indicarse asimismo, que el alcance del término correspondencia no se reduce a la escrita, sino también a la formulada a través de cualquier medio que exprese palabras u otro tipo de lenguaje; amplitud que se fundamenta en el tenor literal de la citada disposición constitucional, la cual no contempla una concreción del medio utilizado para la correspondencia garantizada, ni señala el contenido de esta, sino que se refiere a "todo tipo de correspondencia" (Sala de lo Constitucional de la Corte Suprema de Justicia, 2008, p. 6 y 7)

Por
ello desde esa fecha podemos asumir que las comunicaciones por cualquier vía están protegidas por dicha garantía.

De
sde la promulgación de la Constitución la protección era total, no se había regulado la ley secundaria que permitiera la utilización de interceptación de mensajes o llamadas telefónicas en juicio.

	Artículo 24 Cn.	Art. 259 – D.
Protección/limitación	Correspondencia física	Comunicaciones digitales
	Correspondencia digital Se mantiene el secreto de lo privado, de la información recolectada que no guarde relación con el proceso.	No se regula el secreto de lo privado, de la información recolectada que no guarde relación con el proceso.

limitación	Orden judicial.	No es necesaria autorización judicial. lo hace la PNC o FGR (a pesar de ello, es importante que se configure un control judicial para efectos de graduar la dosimetría de la aplicación de esta técnica; así también para garantizar que el hallazgo de la evidencia sea íntegro, para evitar el uso imparcial de dichos hallazgos)
	Ley secundaria. Ley especial para la intervención de las telecomunicaciones Art. 8	Es una técnica de operación encubierta para la investigación de delitos informáticos y conexos

El problema acá es de carácter grave por las razones siguientes: Art. 259 – D, del Código Procesal penal que contiene la figura del agente encubierto digital no establece los niveles en los cuales los agentes encubiertos digitales establecerán su acción, su investigación.

La gravedad de lo anterior es que debido a la intrusión que hay en la correspondencia electrónica de los investigados se hace necesario la autorización judicial tal y como lo exige la ley de intervenciones

2.5.8. Análisis jurisprudencial

Por parte de la sala de lo constitucional de la corte suprema de justicia de el salvador, sobre y limitaciones y protección de garantías judiciales y derechos fundamentales, en El Salvador.

Los Estados dentro de sus ordenamientos jurídicos establecen los derechos fundamentales, así como también los mecanismos de protección para el estricto cumplimiento y respeto de estos; pero también se encuentran como mecanismos de protección natural la jurisprudencia supranacional, en el caso de El Salvador, se encuentran las sentencias emitidas por la Sala de lo Constitucional de la Corte Suprema de Justicia.

El Tribunal Supremo Constitucional posee un catálogo de sentencias en las que ha efectuado diversos pronunciamientos respecto a los derechos fundamentales, los cuales son inherentes a las personas, pero no únicamente versa sobre su regulación, sino, que además hace referencia en cuanto a la limitación de estos y a su protección frente a posibles vulneraciones.

Para ello tenemos **la sentencia de inconstitucionalidad 109-2018, del veintinueve de junio del dos mil veintidós**; en ella, la Sala cataloga los derechos fundamentales como facultades o poderes de actuación, otorgados a las personas humanas, como efecto de las exigencias ético-jurídicas resultantes de su dignidad, libertad e igualdad que como persona poseen, y consecuentemente positivadas en el ordenamiento jurídico constitucional, y a la vez con un rango supremo de protección constitucional. A criterio de la Sala, el legislador ha permitido la posibilidad de intervenir en los derechos fundamentales de las personas, siempre que dicha intervención se efectúe dentro del marco de la Constitución [es decir, para que una norma suspenda, impida, elimine o dificulte a una persona para el ejercicio de cualquier derecho fundamental que le asiste, esta intervención debe de estar autorizada por la Constitución de la República; puesto que se trata de un derecho que goza de protección de jerarquía suprema por parte de la misma Carta Magna]; si con dicha intervención se da un resultado de “afectación negativa” (llamado así por la misma Sala), pone en desventaja el derecho fundamental intervenido; considerado la Sala que supone una desventaja si: “entre la norma legal y la afectación del

elemento fundamental del derecho medie un nexo de causalidad o de idoneidad negativa (jurídica o fáctica), es decir, la norma debe ser apta para suprimir o eliminar jurídicamente la posición o elemento esencial en el derecho afectado (afectación normativa), o bien que sea idónea para impedir o dificultar el ejercicio de las acciones que habilita el derecho o menoscabar el estatus de las propiedades o situaciones pertenecientes a él (afectación fáctica)". Por lo que si con la interferencia por parte de la norma o precepto legal, existe una vinculación con el derecho fundamental, que arroje un resultado o efecto negativo, entonces se está frente a una intervención de afectación negativa. No obstante, a criterio del legislador, una intervención de afectación negativa en un derecho fundamental no siempre supone un efecto de inconstitucionalidad de manera indeliberada o automática, sino que frente a ello debe hacerse efectivas las garantías y mecanismos de protección material de los derechos fundamentales.

De acuerdo con la Sala, la afectación de un derecho fundamental opera de cuatro formas: "en cuanto a la regulación, limitación, suspensión y pérdida"; lo que a consideración de la Sala supone: "*La regulación o configuración de un derecho fundamental es su dotación de contenido material, es decir, disposiciones que establezcan sus manifestaciones y alcances, condiciones para su ejercicio, organización y procedimientos que sean necesarios para hacerlos efectivos y la estructuración de sus garantía*"; "la limitación de los derechos fundamentales (art. 246 Cn.) supone la afectación de su objeto o sujetos de forma que se impida o dificulte el ejercicio de las acciones, propiedades o situaciones habilitadas por el derecho afectado".

En todas las circunstancias antes dichas, toda injerencia o intervención de un derecho fundamental, de afectación negativa, supone la aplicación del "Principio de Proporcionalidad", entre la norma de afectación y el derecho fundamental, a efectos de establecer el valor y razones de justificación, que respondan de manera suficiente y necesaria para tal intervención. (Sala de lo Constitucional, 2022)

Así también se encuentra fundamentación de los derechos fundamentales, enfocada a su limitación y protección, en la **sentencia 26-2016, del veinte de diciembre del año dos mil veintiuno**, en la que a criterio de la Sala, los derechos fundamentales no son absolutos o ilimitados, puesto que los considera objetos de regulación (configuración) y/o limitación (restricción) legislativa para el legislador; cabe hacer notar que en esta

sentencia se establece en cuanto a que la limitación o intervención, que esta *“implica un acto normativo que modifica alguno de sus elementos configuradores, ya sea en cuanto a los sujetos —titulares o destinatarios—, su ámbito de protección material —el objeto en función del supuesto de hecho, del bien jurídico regulado y el sector físico o ideal que se protege— y la justificación de los límites —si los hay—* observándose en dicha consideración, hace alusión a una justificación en caso de existir límites con la intervención, [dando lugar con ello, a que debe de existir una justificación certera y de gran valor para limitar un derecho fundamental, puesto que con ello se está afectando un precepto de rango constitucional, que cuenta no solamente con la protección por parte de la normativa jurídica nacional sino también con la protección de las garantías reguladas por el ordenamiento jurídico internacional].

En ese orden de ideas, la Sala manifiesta, que las limitaciones a derechos fundamentales deben de efectuarse a través de una ley formal, y que además deben de concurrir tres requisitos:”.

1. Atender a un criterio constitucional que autorice limitar derechos fundamentales; en cuanto a este primer requisito, está claro que la Constitución de la República, no regula de forma expresa los criterios o parámetros a tomar para los casos de limitar un derecho fundamental; no obstante la Sala afirma: *“que las restricciones a los derechos fundamentales formuladas por el legislador solo pueden imponerse para asegurar la convivencia social, en relación con los valores fundamentales del ordenamiento, como la justicia, la seguridad jurídica y el bien común”*.
2. Respetar la proporcionalidad; ello supone, que toda limitación o restricción a derechos fundamentales, debe de estar al margen de arbitrariedades, y de contener una justificación para la misma restricción, efectuando un juicio de valoración de los mismos derechos y el carácter de vinculante de su contenido. Para ello la misma Sala afirma que: *“ la proporcionalidad conlleva las exigencias de la idoneidad de las medidas restrictivas, en relación con el logro del fin legítimo propuesto; la necesidad de dicha restricción, en el sentido de que entre varias medidas adecuadas para conseguir la misma finalidad, el legislador haya seleccionado la menos gravosa para el derecho correspondiente; y la proporcionalidad en sentido estricto, entre la interferencia al derecho fundamental*

limitado y el favorecimiento del bien jurídico o valor que se pretende salvaguardar mediante tal limitación o restricción”

3. No alterar su contenido esencial; ello con base a lo establecido en el art. 246 inc. 1° de la Constitución de la República, en él que se regula la prohibición de manera expresa, (enfocados para a los alcances, aplicaciones, reformas y derogatorias, en cuanto a no alterar, anular o destruir la esencia o el núcleo de los derechos fundamentales,) que, los principios, derechos y obligaciones establecidos en ese cuerpo legal, no pueden ser alterados por las leyes que regulen su ejercicio [por ejemplo para el caso de la normativa secundaria, la cual no puede y no debe contrariar lo prescrito en la Constitución.] Respecto a este punto, la Sala manifiesta: “el contenido esencial de un derecho consiste en el conjunto de facultades que permiten identificarlo en abstracto bajo esa denominación, en un determinado momento histórico; que no puede ser desplazado permanentemente por el legislador ordinario; y que debe ser definido a partir de las convicciones generalmente admitidas entre los juristas, adecuándolas a las peculiaridades de nuestro sistema jurídico, y respetando el pluralismo ético, ideológico y político”. (Sala de lo Costitucional, 2021)

Así también están las garantías judiciales o también llamadas garantías procesales, creadas por el legislador, con el propósito de dar mecanismos o herramientas de protección a las personas sometidas a un proceso legal, ante una autoridad competente, ello a fin de otorgar un marco de seguridad jurídica y, además, mantener un balance entre la verdad material y los derechos del procesado. Estas no solo cuentan con reconocimiento legal en el ámbito nacional sino también internacional, debido a su gran importancia.

Al respecto, existe además pronunciamientos por parte de la Sala de lo Penal de la Corte Suprema de Justicia, efectuando diversas consideraciones sobre las mismas; así, mediante **sentencia 67C-2014 del treinta de enero del año dos mil quince**, hace referencia a las garantías procesales, primeramente, al Debido Proceso, siendo este considerado por el derecho internacional como la base fundamental para una correcta impartición de justicia, requiriéndose el estricto cumplimiento y respeto de las garantías procesales establecidas en el marco legal de ámbito nacional como internacional; retomando la Sala para su definición, lo expresado por el autor Hoyos, Arturo: “*como aquel*

conjunto de garantías en virtud del cual se asegura a las partes en todo proceso legalmente establecido y sin dilaciones injustificadas, la oportunidad razonable de ser oídas por un tribunal competente, predeterminado por la ley, independiente e imparcial, de pronunciarse respecto de las pretensiones y manifestaciones, de aportar pruebas lícitas relacionadas con el objeto del proceso y de contradecir las proporcionadas por la contraparte, de hacer uso de los medios de impugnación consagrados por la ley contra resoluciones judiciales motivadas y conforme a derecho, de tal manera que las personas puedan defender efectivamente sus derechos". Expresando, además, que dentro de este se encuentran también a) derecho a la presunción de inocencia; b) principio "Non Bis in ídem"; c) derecho de defensa; d) principio del Juez Natural; e) principio de Igualdad de armas, etc.; destacando como el principio más importante "**el principio de legalidad**", fundamentando que este es de prevalencia ante cualquier función o potestad en el ejercicio del poder del Estado, y su reconocimiento en la Declaración Universal de Derechos del Hombre, Convención Americana sobre Derechos Humanos, Declaración Universal de Derechos Humanos, y Pacto Internacional de Derechos Civiles y Políticos, todos ellos instrumentos internacionales de derechos humanos. Considerando al principio de legalidad como el más amplio dentro del proceso penal, puesto que este además de integrar diversos principios [mencionados en el párrafo anterior] contiene un cuádruple significado para el legislador y para el juez penal, aludiendo: " *el juez no puede aplicar normas en forma retroactiva en principio del imputado (prohibición de retroactividad: lex praevia); el juez contará con una ley escrita para condenar o agravar penas (prohibición del derecho consuetudinario: ex scripta, principio de reserva de ley); el legislador formulará sus preceptos con tanta precisión, completitud y claridad (mandato de certeza: lex certa); el juzgador para imponer un castigo no puede basarse en la simple analogía o en criterios de arbitrariedad (lex stricta)*"; representado así este principio una garantía fundamental para las personas frente al "ius puniendi" del Estado.

En ese orden, la Sala establece consideraciones respecto al "derecho de defensa", siendo este una más de las garantías judiciales; [es de hacer notar que este se encuentra estrechamente relacionado con el debido proceso, puesto que si las garantías procesales no se cumplen indiscutiblemente se estaría en ausencia del debido proceso y frente al irrespeto del derecho de defensa], concibiendo este que toda persona a quien se le impute un delito, se presumirá inocente, mientras no sea vencido en juicio, así como lo establece el art. 12 de la Cn.; considerado que "el derecho de defensa ampara al imputado desde el

momento de la presunción de su participación en el evento supuestamente delictivo hasta la resolución jurídica del conflicto criminal”.

Pronunciándose en la misma, sobre el principio de contradicción, de este resulta una igualdad de actuación entre las partes (defensa-acusadora), en cuanto a los alegatos de sus teorías o hechos facticos planteados, pues estos deben ser revertidos en igualdad de derechos, principalmente en lo que respecta al ofrecimiento de prueba y a los interrogatorios de ambas partes. Estableciendo las Sala que: “este principio permite un control que se extiende aún hacia los argumentos de su contrario y puedan rebatirlos o aceptarlos, de manera que se propicie la formación de la convicción en el juzgador respecto de la verdad de los hechos”. (Sala de lo Penal, 2014)

En corolario de lo anterior y según la jurisprudencia, se infiere que en cuanto a la técnica de operación encubierta por parte del agente encubierto digital (miembro de la policía) en El Salvador, quien actuará en el proceso investigativo de delitos informáticos y conexos, de forma infiltrada, si mediar autorización judicial, sino únicamente con la autorización del ministerio público fiscal, para que realice indagaciones a través de programas informáticos en las tecnologías de la información y comunicación de carácter abierto o público; y es que dado a las actuaciones que el agente realizará dentro de la esfera de información del indagado, dentro de la cual podría encontrarse no únicamente información de carácter público sino también de carácter íntima o privada de la persona; existiendo además la posibilidad que dentro de esta misma información se encuentre información privada no relacionada con la investigación; considerando estos motivos suficientes para que el legislador prevea la necesidad de realizar un test o juicio de ponderación, basado en los criterios siguientes: a) si la técnica a utilizar resulta ser la menos gravosa (conforme al **principio de proporcionalidad**); b) tomando en cuenta la eficacia (con base al **sub principio de idoneidad**); c) si los resultados que se pretenden obtener atienden a ser indispensables (atendiendo al **principio de necesidad**); todo ello, a efectos que, para la implementación de la técnica de investigación del “agente encubierto digital”, se requiera la intervención judicial, como parte del cumplimiento a las garantías que otorgan la Constitución de la República, la normativa interna y tratados internacionales, a fin garantizarle a la persona investigada el respeto a las garantías judiciales que le asisten, dentro de ellas: **1) principio del debido proceso; 2) el derecho de defensa y 3) la presunción de inocencia**; así como también los demás principios que se encuentran

integrados a ellos; ya que si bien existe un gran interés y necesidad de sancionar los delitos cometidos a través del internet, la investigación de estos no debe realizarse a costa de cualquier medio o por decirlo así a costa de cualquier precio, ya que en estos casos, en los que se encuentran de por medio los derechos fundamentales de las personas, el Estado no puede valerse de cualquier medio para conseguir el fin de llegar a la verdad de los hechos investigados “ puesto que el fin no justifica los medios”.

El control Judicial, en la investigación del delito, tiene como finalidad controlar el ejercicio de poder punitivo, cuanto por medio de este se vayan a limitar derechos fundamentales, por lo que resulta que al analizar la técnica del agente encubierto digital, dicha técnica lesiona derechos fundamentales como las comunicaciones, la intimidad entre otras, por ello es que encontramos que ordenamientos especiales como la Ley de Intervenciones de las Telecomunicaciones, que determina que para su implementación de dicha técnica; es necesario que la autoridad judicial realice un juicio de ponderación para su ejecución, si bien nuestra investigación está dirigida a controlar la posible vulneración del derecho de defensa, por la utilización de la técnica de investigación, en la recolección y estudio de información, nos permite afirmar que per se, la falta de autorización judicial, en implementación de la técnica de investigación del agente digital encubierto, no vulnera el derecho de defensa; si hay otros derechos fundamentales que resultan comprometidos - como son las telecomunicaciones y la intimidad- , por parte del ente persecutor del delito, y tal como ya se indica, vulneración de derechos fundamentales, dentro de la investigación del delito en los casos don se limiten derechos fundamentales, significa una ausencia de garantías judiciales, la cual según Convención Americana ha dispuesto que el derecho de defensa como una garantía procesal se encuentra íntimamente ligado con la noción de debido proceso, por lo que como efecto reflejo pudiera de alguna forma resultar lesionado frente a la ausencia de la garantías judiciales, al momento de su aplicación.

~~al no así estableciéndose que dicho control judicial efectuado en la etapa previa a la judicialización del caso, es conforme a derecho a la intimidad de las telecomunicaciones, no así conforme al derecho de defensa que le asiste la persona investigada.~~

No obstante la jurisprudencia supranacional es el mecanismo de protección natural de los derechos fundamentales reconocidos por el ordenamiento jurídico interno de cada Estado, cabe advertir que si esta no surte su efecto o no cumple con los estándares de

protección, una vez agotados los recursos o vías legales internas se tendrá que recurrir a la jurisprudencia internacional, puesto que en materia de derechos fundamentales se encuentra vinculada con mecanismos o garantías de protección por los instrumentos internacionales de derechos humanos.

Para la Corte Interamericana de Derechos Humanos el “Debido Proceso”, es reconocido y llamado tal como lo denomina la Convención Americana de Derechos Humanos “garantías judiciales”, en su art. 8, expresando: “... *que se consagran los lineamientos del debido proceso legal, el cual está compuesto de un conjunto de requisitos que deben observarse en las instancias procesales, a efectos de que las personas estén en condiciones de defender adecuadamente sus derechos ante cualquier tipo de acto del Estado que pueda afectarlos.*”; así lo estableció en el **caso Barbani Duarte y otros Vs. Uruguay fondo reparaciones y costas. Sentencia de 13 de octubre de 2011. Serie C No. 234**

La Corte considera a los derechos fundamentales, como un límite al poder estatal, en relación con las actividades o funciones que los órganos o sus autoridades realicen, más aún cuando el derecho que se violenta se encuentra consagrado en la Convención Americana de Derechos Humanos; refiriendo además la importancia en cuanto a los casos en que el Estado de acuerdo a su facultad sancionatoria y a su ordenamiento interno es el ente que transgrede el derecho vulnerado; fundamentando en **caso del Tribunal Constitucional Vs. Perú. Fondo, Reparaciones y Costas. Sentencia de 31 de enero de 2001. Serie C No. 71**, que: “*cuando el Estado ejerce su poder sancionatorio, pues éste no sólo presupone la actuación de las autoridades con un total apego al orden jurídico, sino implica además la concesión de las garantías mínimas del debido proceso a todas las personas que se encuentran sujetas a su jurisdicción, bajo las exigencias establecidas en la Convención.*”

Este Tribunal Supremo internacional, reconoce como garantías judiciales, las establecidas en el art. 8 de la Convención Americana de Derechos Humanos; dentro de estas, las que se encuentran estrechamente relacionadas al derecho de defensa, están: 1) Juez competente, independiente e imparcial, [siendo considerado el derecho que le asiste a toda persona a ser juzgado por un tribunal ordinario de acorde a los procedimientos legalmente preestablecidos, constituido por un juez natural quien deriva su existencia y

competencia de la ley]; 2) Presunción de inocencia, ; 3) comunicación previa y detallada al inculpado de la acusación formulada, [debe realizarse una descripción material de la conducta imputada que contenga los datos fácticos recogidos en la acusación, que constituyen la referencia indispensable para el ejercicio de la defensa del imputado y la consecuente consideración del juzgador en la sentencia].; 4) oportunidad y medios adecuados para preparar la defensa (derecho a interrogar testigos y perito y hacer que comparezcan a estrados judiciales; 5) derecho a ejercer la defensa, sea personalmente o bien mediante defensor técnico; 6) derecho del imputado a no ser obligado a declarar contra sí mismo ni a declararse culpable(confesión), siendo esta valida únicamente si se realiza sin coacción; 7) “ne bis in idem” nadie puede ser castigado o sancionado dos veces por el mismo hecho punible; 8) publicidad del proceso penal; todas estas garantías se encuentran establecidas en la Convención americana de Derechos Humanos, en su art. 8.; así como también establece como garantías judiciales relacionadas con el proceso penal, además de las anteriormente citas: a) exigencias reforzadas en procesos vinculados con la pena de muerte; b) no declarar contra sí mismo; y, c) la prohibición de la coacción en la confesión; d) derecho a una resolución motivada. Si bien, en todo proceso legal se deben de garantizar el respeto de los derechos fundamentales, a través de las garantías judiciales, las cuales son reconocidas de forma expresa (como ya se expresó) por la Convención Americana de Derechos Humanos, haciendo énfasis la Corte Interamericana de Derechos Humanos en el aspecto de que las sentencias o decisiones que produzcan una posible afectación o limitación de derechos fundamentales, deben ser debida y legalmente fundamentadas, pues caso contrario se estaría frente a resoluciones arbitrarias.-

2.6. Agente encubierto informático en España.

2.6.1. Legislación.

En España, surge como respuesta del escenario criminológico manifestado en las “redes sociales” con el uso de las tecnologías de la Información y Comunicación; creándose la figura del agente encubierto informático en relación y consonancia con lo establecido en el Convenio de Budapest, el cual versa sobre la ciberdelincuencia por parte del Consejo de

Europa, teniendo como finalidad el sancionar conductas delictivas, cometidas con la utilización de herramientas o equipos informáticos o del internet. Así, se introdujo la figura del agente encubierto informático mediante una reforma efectuada a la Ley de Enjuiciamiento Criminal de 1882-ley 13/2015 ; dando con ello legalidad a la aplicación de técnicas de investigación a través del agente encubierto informático, con la agregación del artículo 282 bis. Siendo este un agente policial, cuya función es investigar y descubrir delitos realizados en el ciberespacio a través del uso de las tecnologías.

La Legislación Española determinó en la misma ley, los delitos en los cuales se permitirá el accionar de esta figura, siendo estos: delitos previstos en el art. 588 de la misma Ley de Enjuiciamiento Criminal, sean dolosos con una pena máxima al menos de tres años de prisión; delitos relacionados a organizaciones criminales y terroristas; delitos cometidos a través de instrumentos informativos o de otra tecnología de comunicación e información.

2.6.2. Funciones.

Para la intervención del agente encubierto informático (quien debe ser miembro de la Policía Judicial), se requiere de una autorización judicial, la cual debe ser requerida al juez instructor ya sea por el ministerio público o por la policía judicial, debiendo el juez al otorgar la autorización mediante resolución en la que deberá establecerse las actuaciones que el agente podrá realizar e indicarle su seudónimo con el que se identificará.

Las actividades o medidas que el agente encubierto informático podrá realizar, las regula el artículo 282 bis de la Ley de Enjuiciamiento Criminal:

“a) Intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido; b) analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos; c) obtener imágenes; grabar conversaciones que puedan mantenerse en los encuentros previstos por el agente y el investigado...” (Harbottle Quirós, 2021, p. 13)

2.6.3. Evidencia digital en delitos informáticos en la investigación.

El Consejo de Europa define la evidencia digital como: *“cualquier información de valor investigativo generada, almacenada o transmitida en forma digital que puede ser utilizada para probar o desaprobar un hecho disputado en un procedimiento legal”* (C. Velasco San Martín, 2012, p. 442)

2.6.4. Convenio de Budapest sobre la cibercriminalidad.

El Convenio de Budapest (también conocido como “Convenio de la Ciberdelincuencia”) es un acuerdo internacional, logrado a través de esfuerzos por parte de la comunidad internacional, con el propósito de establecer una legislación penal y procesal para sus Estados miembros, con el propósito de combatir el crimen organizado transnacional, específicamente los delitos cometidos a través de la informática, y así proteger a los usuarios de la web mediante la ciberseguridad.

“El Convenio de Budapest y su Informe Explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión el (08 de noviembre del año 2001) y el Convenio fue abierto a la firma en Budapest el 23 de noviembre del año 2001, con motivo de la celebración de la Conferencia Internacional sobre la delincuencia”. (Cardona Pérez, 2021, p. 137)

Teniendo además dicho Convenio como objetivo, el crear mecanismos y medios de cooperación transnacional, frente a la comisión de delitos informáticos.

El Convenio de Budapest, dentro de su propósito de combatir el crimen organizado transnacional en relación con los delitos informáticos, tiene además tres finalidades principales:

1. La primera es la de concertar los elementos de las conductas desviadas de acuerdo con el derecho penal sustantivo de cada nación y de igual forma buscar armonizar

los diferentes preceptos vinculados a la materia de delitos informáticos de cada país.

2. En segundo lugar, se encuentra, el instaurar de forma acorde al derecho penal procesal de cada estado, los poderes, atribuciones y demás facultades que resulten necesarias para la debida investigación y posterior procesamiento de tales delitos cibernéticos, también para las demás conductas delictivas que se cometan por medio del uso de un sistema informático y para las demás pruebas conexas que se encuentren en formato electrónico.
3. En tercer y último lugar, el convenio propende por implantar un régimen que sea tan rápido como eficaz para lograr una debida y correcta cooperación internacional que permita investigar y procesar los delitos cibernéticos de forma oportuna. (Molina Díaz, 2021, pp. 10, 11)

El Convenio de Budapest contiene 48 artículos, distribuidos en cuatro capítulos con sus respectivas secciones. El Capítulo I, art 1; contiene la “Terminología de definiciones” reguladas por el Convenio a) sistemas informáticos; b) datos informáticos; c) proveedor de servicios; y ,c) datos relativos al tráfico. El Capítulo II, arts. 2 al 11, desarrolla “Las Medidas que deberán adoptarse a nivel nacional” por los Estados parte, estableciendo que cada uno de ellos atendiendo a la necesidad criminalizará las conductas ilícitas que se realizan mediante el uso de aparatos o dispositivos tecnológicos, dentro de ellos el acceso ilícito a sistemas informáticos, interceptación ilícita de datos informáticos, delitos relacionados con pornografía infantil, etc. Estableciéndose además en el art. 15 “Condiciones y Salvaguardias” refiriéndose a que los Estados parte que implementes las actuaciones establecidas en el Convenio deberá hacerlo conforme a su normativa interna, garantizando la protección de los derechos humanos y libertades contenidos en los diferentes instrumentos jurídicos de protección de los derechos humanos, uno de ellos, el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas. Así mismo se establece una medida dentro del proceso de investigación de suma importancia como lo es “conversación rápida de datos informáticos almacenados (con el propósito de que sean eliminados antes o después que finalice la investigación). – El Capítulo III, arts. 12 al 35, trata sobre la cooperación

internacional, estableciendo la asistencia mutua relacionada a la extradición e información espontanea entre los Estados parte. Y como ultimo el Capitulo IV, arts. 36 al 48, conteniendo las disposiciones finales. (Consejo de Europa, 2001)

“El Convenio de Budapest se complementa con un Protocolo Adicional que penaliza la criminalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos (CETS 189). La negociación de un segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas comenzó en septiembre del año 2017.” (Consejo de Europa, 2021, p. 1)

Hasta en junio del 2021, 66 países formaban parte de Estados miembros del Convenio de Budapest, entre ellos países europeos, Australia, Canadá, República Dominicana, Estados Unidos, Filipinas, Argentina, Costa Rica, Chile, Colombia, Perú, Panamá, etc. Actualmente El Salvador no ha ratificado el Convenio de Budapest, por lo cual no es Estado parte de ella.

2.6.4.1. Análisis Comparativo: Ventajas y Desventajas.

2.6.4.1.1. Beneficio.

Si bien es cierto, el estar adherido al Convenio de Budapest como Estado parte, es de conveniencia para el combate de los delitos informáticos, puesto que los países en su mayoría no cuentan en su normativa interna con reglas referentes de manera específica al procesamiento y manejo de la evidencia digital, por lo que resulta necesario alcanzar acuerdos internacionales que faciliten en la cooperación de la investigación de estos delitos.

Dentro de los beneficios con que cuentan los Estados parte, se encuentran:

1. El Convenio proporciona un marco legal para la cooperación internacional en materia de ciberdelito y evidencia digital. El Capítulo III del tratado establece

disposiciones generales y específicas para la cooperación entre las Partes "en la mayor medida posible" no solo con respecto a los ciberdelitos (delitos en contra y a través de sistemas de cómputo) sino también con respecto a cualquier delito relacionado con evidencias electrónicas.

2. Los Estados Parte podrán ser miembros del Comité del Convenio sobre la Ciberdelincuencia (T-CY), que actualmente es el organismo intergubernamental más relevante que se ocupa del ciberdelito. Los Estados Parte comparten información y experiencias, evalúan la implementación del Convenio o lo interpretan a través de Notas de Orientación.
3. El T-CY también puede preparar Protocolos adicionales a este tratado. Por lo tanto, incluso si un Estado no participó en la negociación del tratado original, un nuevo Estado Parte podrá participar en la negociación de futuros instrumentos y la futura evolución del Convenio de Budapest.
4. Los Estados Parte del Convenio se comprometen entre sí para una cooperación confiable y eficiente. Los indicios indican que es más probable que las entidades del sector privado cooperen con las autoridades de justicia penal de los Estados Parte del Convenio, dado que los Estados Parte deben contar con un marco jurídico nacional vigente sobre ciberdelitos y evidencias electrónicas, incluidas las salvaguardas previstas en el Artículo 15. –
5. Los Estados Parte que soliciten la adhesión o que se hayan adherido pueden convertirse en países prioritarios para los programas de creación de capacidad. Dicha asistencia técnica es para facilitar la plena aplicación del Convenio y mejorar la capacidad de cooperación internacional. (Consejo de Europa, 2021, p. 2)

2.6.4.1.2. Desventaja.

Como es sabido la evidencia digital es intangible y volátil, pudiendo ser alterada o desaparecida en poco tiempo, por lo que resulta necesario que las investigaciones que se realicen para este tipo de prueba debe ser precisas y rápidas, requiriendo de un proceso ágil y eficaz, el cual resulta accesible a través del apoyo y cooperación internacional, siendo que dentro del Convenio la cooperación a través de la información es esencial, por la complejidad que generan estos delitos informáticos; como por ejemplo: supongamos que se comete un fraude a través de una página de pagos online, la víctima hizo una compra desde El Salvador, a través de un portal *hosteado* en Panamá, pero la persona que la engañó para hacer ese pago se encuentra en España. Además, tanto la víctima como el estafador mantuvieron varias conversaciones por un servicio de chat, el cual pertenece a una empresa norteamericana. La víctima realiza la denuncia por fraude en El Salvador por un delito que está tipificado, pero el delito en sí se cometió desde España y la evidencia está dividida entre Panamá y Estados Unidos. ¿Cómo se procesaría la evidencia digital como prueba en el proceso?, en el caso anterior resulta necesaria la cooperación de la información que estable el Convenio en el art. 35, RED 24/7, a través de un punto de información las 24 horas los siete días de la semana, para brindar información que estén en países extranjeros y sean necesarios para obtenerlos para ser incorporados como prueba en el proceso, asesoramiento técnico, conservación de datos, obtención de pruebas, suministro de información jurídica, localización del sospechoso.

CAPITULO III. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Método.

1. CUALITATIVO. Para los autores Bonilla y Rodríguez, esta se interesa por captar la realidad social a través de la percepción que tiene el sujeto de su propio contexto. (Arturo et al., 2011)

Con este método se analizaron sobre los alcances del agente digital encubierto en la investigación de delitos informáticos, con relación al derecho de defensa del imputado, y las garantías judiciales, en el proceso penal; tomando en cuenta el carácter subjetivo de los agentes entrevistados.

2. HERMENEUTICA JURÍDICA. Para el autor Dueñas José, esta consiste en asignar significado a expresiones de lenguaje jurídico; y en determinar el significado de una expresión jurídica dudosa. (Dueñas Ruíz, 2015).

En la investigación se realizó un análisis e interpretación de la normativa nacional e internacional, así como también de los instrumentos internacionales relacionados a la temática.

3.2. Tipo de estudio.

1. EXPLORATORIO: “Este tipo de investigación sirve para incrementar el conocimiento sobre una temática poco conocida o estudiada”

Por ser un tema novedoso y del que poco se ha discutido, se realizó la investigación con la información obtenida en las entrevistas, también con la información recabada del estudio y análisis de la normativa nacional e internacional, jurisprudencia y de los instrumentos internacionales.

2. EXPLICATIVO: Están dirigidos a responder a la causa de los eventos, su interés se centra en explicar por qué dos o más variables están vinculadas (Batthyány, 2013)

En la investigación se ha logrado determinar y explicar sobre la temática establecida, a fin de determinar sus condiciones y dar posible respuesta a la problemática existente.

3.3. Técnicas.

1. LA OBSERVACIÓN. Se consigue mediante la percepción; es decir se emplea uno de los sentidos (en este caso la vista) para obtener la observación. considerada como una forma más sintetizada y lógica para el registro visual y verificable de lo que se desea obtener. (Trejo Sánchez, 2021, pág. 48).

Esta se realizó mediante la observación de las actitudes y reacciones de la muestra de personas que se entrevistarán, basada en determinados parámetros los cuales se fijarán en la respectiva guía de observación.

2. ENTREVISTA. Es de naturaleza empírica, consistente en la comunicación interpersonal establecida entre el investigador y el sujeto de estudio con el fin de obtener respuestas verbales a las interrogantes planteadas sobre el problema propuesto. (Trejo Sánchez, 2021, pág. 52).

Las entrevistas se aplicaron a personas expertas en la materia, a fin de conocer su criterio y puntos de vista respecto a la temática, siendo estos operadores del sistema encargados del juzgamiento (jueces), operadores encargados de acción (fiscales) y, profesionales del derecho em el ejercicio libre de la profesión (defensores técnicos).

3. ANÁLISIS DE DOCUMENTOS. Permiten recabar datos contenidos en documentos de diversos tipos; presenta un carácter particular donde se considera que son interpretativas. (Trejo Sánchez, 2021, pág. 39).

Se enfocó en todos aquellos documentos que sean fuente de información legal y certera, dentro de ellos: doctrina legal, normativa nacional e internacional y jurisprudencia etc.; respecto a la temática de investigación, efectuándose una interpretación doctrinal, judicial, auténtica y popular.

3.4. Instrumentos.

1. GUÍA DE ENTREVISTA. Se realizarán entrevistas semiestructuradas a operadores del sistema encargados del juzgamiento (jueces, defensores y fiscales).

Esta presenta la peculiaridad de introducir preguntas adicionales para precisar conceptos u obtener más información sobre temas deseados. (Trejo Sánchez, 2021, pág. 53).

2. FICHAS BIBLIOGRÁFICAS. Estos son instrumentos de recolección de datos obtenidos de forma documental que nos permite identificar y clasificar una fuente escrita. (Trejo Sánchez, 2021, pág. 42).

Se recopilaron datos de información bibliográfica, a fin de consultar en las diversas fuentes para conocer, estudiar y analizar la información, tanto doctrinal de diferentes autores como la información legal.

4.

GUÍ

A DE OBSERVACIÓN. Se elaboró una guía de observación estableciendo los parámetros a observar en la muestra de personas entrevistadas, con el propósito de identificar sus actitudes y reacciones al momento de la entrevista.

4. CAPITULO IV. HALLAZGOS DE LA INVESTIGACIÓN.

Por tratarse de una investigación cualitativa y no cuantitativa consideramos que en los hallazgos de la investigación es relevante hacer un análisis a la luz de la hermenéutica Jurídica, la cual, consiste en asignar significado a expresiones de lenguaje jurídico, es decir, la percepción, del objeto de estudio que es el art. 259-D y así mismo, en el análisis a las entrevistas a fiscales y operadores judiciales.

4.1. Análisis hermenéutico Jurídico.

El análisis hermenéutico del art. 259 – D, del Código Procesal Penal es fundamental en el presente trabajo, debido a que este es el centro de operatividad de la figura del agente digital encubierto y que es uno de los métodos principales a utilizar en la presente investigación.

Por razones de interpretación, se transcribirá dicho artículo, con el objetivo de mayor entendimiento, en el cual encontramos literalmente establece:

Agente encubierto digital y otras técnicas de investigación informáticas.

Art. 259-D.- Durante la investigación de los delitos contenidos en la Ley Especial Contra los Delitos Informáticos y Conexos u otros contenidos en leyes penales especiales, y de conformidad con lo establecido en el Art. 175 inciso cuarto de este Código, podrá ordenarse la relación de operaciones encubiertas digitales que resulten necesarias, las cuales estarán a cargo de la policía, previa autorización por escrito del fiscal general de la República.

La policía también podrá realizar la búsqueda a través de las Tecnologías de Información y Comunicación de carácter abierto o público, incluyendo las páginas de internet, de evidencia digital que constituya el hecho punible informático o pueda servir de prueba para el mismo, por medio de programas informáticos que le permitan Identificar los valores únicos identificativos de tal evidencia digital, o mediante la búsqueda o indagación libre en tales espacios informáticos virtuales.

La policía y o la fiscalía podrán celebrar acuerdos con entes públicos o privados con sede en otros países, que le permitan recibir y documentar noticias criminales del cometimiento de hechos delictivos de forma directa, inclusive mediante el uso de las Tecnologías de la Información y Comunicación; la información así recibida podrá ser incorporada al proceso como evidencia digital, conforme a las regulaciones de este capítulo.

Dicha figura es creada en El Salvador, con el fin de esclarecer crímenes de carácter informático, debido al aumento de casos y que las tecnologías han ido en constante evolución, en un inicio como ya se relacionó supra, el agente encubierto digital es una figura que surgió en España con el objetivo de investigar la pornografía infantil en las redes P2P o “PEER TO PEER” o persona a persona, lo que es importante relacionarlo debido al avance que tiene dicha figura, por lo que se ira comprendiendo en cada punto de interpretación.

Con ello en mente, se analiza el contenido con base a la hermenéutica jurídica, de dicho Art. 259-D.- en la siguiente manera detallando cada punto:

4.1.1. Agente encubierto digital.

Como se abordó en el marco teórico, el agente encubierto digital es una derivación del agente encubierto, pero con un marco de acción específica: la investigación de los delitos informáticos, que si bien es cierto, debido al alto índice de criminalidad informática y no habiendo regulación sobre técnicas de investigación, se implementó dicha técnica de investigación, las cuales establecen literalmente que es autorizada por el fiscal y que estarán a cargo de la policía, por lo que se interpreta una ausencia de control judicial.

Esta técnica en otros países está probada su eficacia y pertinencia en el combate a la pornografía infantil, entre otros, pero la utilización de este es fuertemente vigilada por el juez competente y nunca otorgada por el ministerio fiscal.

Ese es el principal problema en nuestro país, la falta de control judicial de esta herramienta, porque a diferencia de la versión precedente, para acceder a los archivos del

sujeto investigado es necesario que se tenga acceso a la intimidad de este, lo cual estaríamos en presencia de una vulneración del derecho a la intimidad.

4.1.2. **Campo de aplicación.** Inciso. 1°

El inciso primero del mismo artículo establece el campo de uso de esta herramienta de investigación: investigación de delitos informáticos en primer lugar y en segundo otros contenidos en leyes especiales.

Así se establece una amplitud de aplicación, la cual no debe ser así, porque los agentes investigadores podrían llegar a vulnerar el derecho a la intimidad de los investigados en áreas que no son de la investigación que se está realizando.

No queda estipulado en qué canales de internet tendrá aplicación ésta figura, si en la internet superficial o en la internet profunda (Deep web). Esto es importante ya que si es para la internet superficial no es necesaria esta figura porque la internet superficial es pública, pero si es en la Deep web, es necesario que se establezca un control judicial ya que para tener interacción en estos canales privados de internet se necesita entrar en la zona protegida por la inviolabilidad de las telecomunicaciones, por lo cual se considera que está mal redactado.

Se comprende en cuanto al campo de aplicación que establece “en otras leyes especiales” y especificar en qué casos, debido a que es muy general, dando mala interpretación en el momento de investigar cualquier delito.

4.1.3. **Autoridad competente.**

La autoridad competente para autorizar es la Fiscalía General de la República.

Con relación al derecho comparado encontramos la legislación española la cual sostiene que la autorización de esta herramienta de investigación debe ser controlada por el juez competente. “Por un lado, su autorización es competencia exclusiva del juez instructor y por otro, su actuación se extiende no solo a los delitos del núm. 4 del art. 288 bis, sino también a los delitos típicos de las medidas de investigación tecnológica, como inmediatamente tendremos ocasión de ver.” (Sanchis Crespo & Velasco Núñez, 2019, p. 516) es

decir en España es obligatorio que su autorización sea dada por un juez competente y no por el ministerio público, por razones de control, independencia y garantías judiciales, las cuales quedan comprometidas si son otorgadas por el mismo ente investigador. Asimismo, el art. 24 de la Constitución exige que cualquier menoscabo a la privacidad de la correspondencia debe ser autorizada únicamente por el juez competente, por ello no compartimos esta configuración actual.

4.1.4. Órgano ejecutor.

Todas las investigaciones bajo la técnica del agente encubierto digital estarán a cargo de la policía. Una vez autorizado, el agente encubierto tiene libertad a la hora de ejecutar sus funciones. Estas facultades al ser totalmente discrecionales y que afectan la garantía de la privacidad de la correspondencia en el investigado deben ser controladas por el juez competente. Podemos advertir que esta función debería estar sujeta a control judicial para evitar el uso indebido de la información recolectada.

4.1.5. Campo de aplicación. Inciso 2°

El contenido de este inciso no da herramientas adecuadas a la investigación ya que limita la actuación a un sitio donde normalmente no se tiene mayor indicio de delitos: “los canales públicos” o como se le conoce como “internet superficial”. En España no es necesaria la figura del agente encubierto digital ya que el acceso a esta zona de la internet es libre, cualquiera puede hacerlo.

Por lo tanto, consideramos que la redacción de este inciso en lugar de aportar nuevas herramientas significativas restringe el campo de acción de los agentes, así mismo se observa de forma independiente al 1° inciso, al establecer que “la policía también podrá”, lo cual es facultativo, debido a que se comprendiera que puede hacerlo de oficio y no previa autorización fiscal.

4.1.6. Acuerdos de cooperación internacional. Inciso 3°

La intención es loable: utilizar las TIC a efectos de lograr una integración internacional de documentación de delitos informáticos. El presente inciso, ha sido

presidido a noticias criminales, en aras de investigaciones, las que literalmente dice “que puede agregarse al proceso como evidencia digital”, las cuales pueden ser recibidas y documentadas por la fiscalía o la policía.

Sin embargo, dicho objetivo se quedó corto porque podría haberse extendido a la cooperación internacional a agencias de investigación digital y celebrar investigaciones de carácter internacional con incidencia nacional, lo cual sería más atinado en el contexto de esta herramienta.

4.2. Análisis de entrevistas a fiscales.



UNIVERSIDAD GERARDO BARRIOS.

Alcances de la figura del agente encubierto digital y sus implicaciones en la investigación de los delitos informáticos frente al derecho de defensa del imputado.

ENTREVISTAS FISCALES

ENTREVISTA 1. Anónima.

1. ¿Cómo es el funcionamiento de la Técnica del agente encubierto digital, en el proceso penal salvadoreño?

Opera como un mecanismo o instrumento de investigación especial moderno, mediante el cual la Fiscalía General de la República se encuentra legalmente facultada para dejar a cargo de la Policía nacional Civil, realizar las operaciones encubierta digitales que resulten necesarias para investigar los delitos previamente señalados por la ley.

2. ¿En cuanto a la legalidad, que ha mencionado cuales son las razones o fundamento en aplicación en ese mecanismo?

3.

Las razones que fundamenta en la aplicación de la técnica del agente encubierto digital en casos penales obedecen a políticas de persecución penal que tienen su base en el evidente auge delincencial, por medio de la Comisión de una

serie de delitos haciendo uso de las tecnologías de la información y la comunicación, haciendo en consecuencia, como una respuesta a la mutación criminal que va surgiendo por medio del desarrollo tecnológico.

4. ¿En cuanto al desarrollo tecnológico, cuales con los criterios bajo los cuales debe aplicarse la técnica del agente encubierto digital?

Se regulan en el artículo 259-D del código procesal penal, 175 inciso cuarto del mismo cuerpo legal, respondiendo siempre a la gravedad del hecho denunciado en cada caso y dentro del marco de los delitos que se señalan en las disposiciones legales antes mencionadas.

5. ¿Cuáles son los criterios para asignar al agente encubierto digital?

El procedimiento para la asignación y acreditación de la gente encubierto digital, deberá estar a cargo de la policía nacional civil en razón que, de conformidad al artículo 259-D del código procesal penal la referida técnica deberá ser ejecutada por dicha institución con previa autorización por escrito fiscal de la Fiscalía General de la República siendo evidente que dicha asignación siempre deberá responder a los criterios de idoneidad en la función a desempeñar.

Los requisitos legales para ser agente encubierto digital deben ser definidos por la normativa interna que rige a la policía nacional civil, en los que pueden incluirse, entre otros, estudios psicológicos, preparación y entrenamiento, experiencia idoneidad, con relación a la función que ejercerá la persona seleccionada.

6. ¿Cuáles son las funciones que realiza el agente encubierto digital, en una investigación?

Las funciones operativas que el agente encubierto digital debe realizar dependerán de cada caso en particular, debiendo siempre ser autorizadas y coordinadas en la función en la Fiscalía General de la República y debido a ello las mismas tienen límite.

Las funciones para realizar por el agente encubierto digital deben responder a la dirección funcional dirigida por la Fiscalía General de la República y ser esta última la institución que posee la facultad constitucional de dirigir la investigación no puede existir de libertad absoluta del agente encubierto digital.

7. ¿Cuál es el proceso de la información obtenida por el agente encubierto digital, para la incorporación al proceso judicial?

De la incorporación de la evidencia digital al proceso nos habla del artículo 259 del Código Procesal Penal, y el mismo nos dice que los requisitos son los que menciona el artículo 201 del Código Procesal Penal, por lo que una vez incautado un equipo un instrumento tecnológico en el que se tenga razones fundadas para interferir, que en el mismo puede existir información útil relacionada a la comisión de un hecho delictivo, fiscal deberá solicitar autorización judicial para garantizar la obtención y resguardo de esa información.

8. ¿Cuáles son las responsabilidades en las que podría incurrir el agente digital en cubierto, en una investigación?

La responsabilidad penal puede existir en relación con las actuaciones de cualquier agente, durante cualquier tipo de investigación, por lo que eventualmente, también podría existir para el agente encubierto digital, qué tal suerte que los elementos objetivos y subjetivos presentes en el delito de fraude procesal regulado en el artículo 306 del Código Penal pueden también llegar a ponerse de manifiesto en una operación encubierto digital.

9. ¿Como garantizan el derecho de defensa del acusado, durante la investigación y al judicializar los casos?

Las diligencias iniciales en cierta medida son reservadas, cuando se judicializa es ahí donde se ponen en conocimiento las diligencias y puede el

imputado y defensor técnico ejercen el derecho de defensa y es ahí donde alegarían si el procedimiento se hizo conforme a las leyes, el defensor puede cuestionar si hubo una vulneración con el caso judicializado

Por ejemplo, en las intervenciones telefónicas, el juez solo autoriza, ellos van garantizando que todos los derechos y garantías, no obstante, se entregan informes de seguimiento al juez de los hallazgos, e incluso derechos humanos le da un seguimiento.

Es ilógico que el acusado al tener conocimiento no dejara de hacerlo o lo cometería de una forma diferente ejemplo en las compras controladas en los delitos de droga, donde agentes encubierto, compran en la investigación, el imputado no lo sabe y lo descubre, al momento que se detiene o hasta que se judicializa, debido a que si supiera que es un agente el que hace la compra siguieran cometiendo el ilícito de una forma diferente o ya no lo harían.

4.3 Análisis de entrevista 1.

La figura del agente encubierto digital es utilizada en el Art. 259-D del Código Procesal Penal, donde es la fiscalía quien tiene la facultad según el caso en concreto, donde bajo un estudio del caso se requiera su utilización, en este sentido, se auxilia con los agentes policiales entrenados, cuyas reglas se rigen por parámetros ya establecidos internamente en la policial, donde adquieren entrenamiento, pruebas psicológicas, conocimientos informáticos, que permitan un mejor resultado en la investigación de estos delitos, en este orden de ideas, la fiscalía es quien autoriza, pero la ejecución la tiene la Policía, quien se ve limitado debido a que las acciones que va a realizar son discutidas, para llegar a resultados favorables en cada caso.

En este sentido, en cuanto a la evidencia digital recolectada por el agente encubierto, se puede comprender que al incautar un objeto que contenga información tecnológica, que resulte útil en la investigación de un caso, si necesita autorización judicial, no así de otras formas de investigación en medios tecnológicos, es decir como al grabar conversaciones, la importancia de tener un control judicial, se debe al derecho de defensa del imputado, que se ve perjudicado en sus derechos fundamentales, en vista que en el

juicio se le debe dar certeza al juez, pero debido a la regulación del art.259- D, es poco el control que posee esta técnica, por lo que genera inseguridad, y una vulneración a un juicio justo.

Así mismo, ya lo establece el fiscal y este es un hallazgo importante en la investigación, en las intervenciones telefónicas, es una figura que vulnera derechos fundamentales, por lo que se aplica el control judicial, dando informes de hallazgos, relevantes de la investigación, donde está presente un delegado de derechos humanos dándole seguimiento, dando así seguridad en la investigación y garantizando un debido proceso haciendo menos el riesgo de vulneración de derecho de defensa del imputado.



UNIVERSIDAD GERARDO BARRIOS.

Alcances de la figura del agente encubierto digital y sus implicaciones en la investigación de los delitos informáticos frente al derecho de defensa del imputado.

ENTREVISTAS FISCALES

ENTREVISTA 2. Anónima

1. ¿Cómo funciona la técnica de agente encubierto digital?

La técnica del agente encubierto digital en el proceso penal salvadoreño se utiliza como una herramienta para determinar si una o más personas se encuentran vinculadas al cometimiento de un hecho delictivo de gravedad. Esta técnica tiene su sustento legal en el artículo 282 lit. D del código procesal penal.

2. ¿Cuál es la diferencia entre el agente encubierto digital y el agente tradicional?

La técnica del agente encubierto digital a diferencia de la técnica del agente encubierto que comúnmente conocemos, Esta en que la técnica digital conlleva en que la gente digital encubierto actúa con una identidad supuesta, permitiéndole la identidad ficticia grabar conversaciones y obtener imágenes de encuentros entre el agente y el investigado, asimismo acceder archivos ilícitos en el curso de una investigación.

3. ¿Cómo se fundamenta la aplicación del agente encubierto digital?

Se fundamenta su aplicación para tener contacto con la persona u organizaciones dedicados a realizar hechos delictivos, con el fin de ponerlas a descubiertas y someterla al proceso penal, procurando dos cosas básicas: por un lado, obtener la prueba necesaria para acreditar el comportamiento ilícito de esas personas y por otro lado tomar las precauciones necesarias para evitar que dichos sujetos alcancen el resultado que se proponían en el caso concreto.

4. ¿Cuáles son los requisitos esenciales para autorizar un agente encubierto digital?

Se deben tener en cuenta algunos requisitos esenciales como: uno contar con una orden o autorización por el fiscal, así también atender a principios de subsidiariedad, proporcionalidad y necesidad. El principio de subsidiariedad hace referencia a que la técnica especial de investigación debe ser utilizada como última medida para procurar pruebas dentro del proceso. El principio de proporcionalidad éste se debe a que su empleo se reserva a la investigación de delitos considerados graves y el principio de necesidad a qué se utiliza este método siempre y cuando no se disponga de otras técnicas de investigación que permitan lograr los mismos resultados.

5. ¿Cuál es el procedimiento para que un agente policial sea asignado como agente encubierto digital?

El procedimiento para asignar al agente encubierto digital debe ser determinado inicialmente por el departamento de investigaciones de la policía nacional civil quien proporcionará bien un listado de agentes que tienen la capacidad de información necesaria para desempeñar el trabajo de un agente encubierto, asimismo podrá designar de una vez quién será el agente para tal caso cabe aclarar que es necesario que las capacidades y formación de los agentes debe ser demostrada.

6. ¿Cuáles son los requisitos legales para la asignación?

Los requisitos legales son, ser miembro de la corporación policial, independientemente de su rango institucional, que haya sido nombrado como tal por el director general de la policía o por quien tuviere la potestad de hacerlo, que dicho nombramiento fuere autorizado por la Fiscalía General de la República . Además, debe poseer aspectos técnicos Tales como: manejo de pruebas, evidencias y cadena de custodia, manejo de equipo tecnológico, control emocional, ética y valores, actuación habilidades de engaño y conducción.

7. ¿Cuáles son las funciones operativas del agente encubierto digital?

Durante la investigación puede utilizar diversas funciones operativas entre ellas utilizar una falsa identidad, participar en los actos de preparación y ejecución de actividades, pero no en un rol de liderazgo, ingresar y participar en reuniones, realizar vigilancia y seguimiento utilizando los elementos técnicos apropiados. Todo lo anterior se puede realizar, no obstante, también existen límites a las funciones, las cuales deben determinarse por el fiscal, por ejemplo, no provocar o inducir a cometer una conducta punible.

8. ¿Cómo vigila las funciones del agente encubierto digital la fiscalía?

Si, deben acordarse cuáles serán las funciones a realizar, para ello también existe una vigilancia en el cumplimiento de deberes de la gente, transmitir la información que este reporte. En caso de ser necesario se podrán hacer coordinaciones para asignar nuevas funciones cuando el caso lo amerite.

9. ¿Cómo recopilan la prueba presentada por el agente, para ser incorporada a las diligencias investigas?

La información recopilada por el agente encubierto digital debe ser analizada y ver si esta reúne los indicios necesarios para considerarse que sea una prueba útil y pertinente en un determinado caso y que se respeten los preceptos legales establecidos en el código procesal penal, tales como los de los artículos 175, 176,

y 177, una vez cumplan con estos requisitos serán incorporadas al proceso según la etapa en que éste se encuentra, es decir, si esa en la fase de instrucción se presentarán al finalizar el plazo de este mediante un dictamen.

10. ¿Cuál es la responsabilidad en la que recae el agente encubierto digital, en las actuaciones que realiza durante las investigaciones?

La responsabilidad penal dependerá en la medida de cómo se ha llegado vulnerar un derecho, no obstante, la utilidad de esta técnica comprende previamente haber realizado una valoración del caso en el que se utilizará esta prueba o técnica, es decir, pese a que se puedan violentar derechos, pero en esta técnica fue utilizada como última medida para procurar pruebas dentro del proceso en hechos considerado como grave que esta función técnica se utiliza por no existir alguna otra técnica que no cause agravio a los derechos de los investigados o que cause menos agravio que la técnica del agente encubierto digital aplicando los criterios, considero que no se podría imponer responsabilidad penal alguna salvo que incurrieron en algunas prohibiciones.

11. ¿Como garantizan el derecho de defensa del acusado, durante la investigación y al judicializar los casos?

En las diligencias iniciales de investigación en este tipo de casos es de importancia que el imputado no tenga conocimiento debido a que la persona investigada ya está cometiendo un delito de carácter informático, por lo que a través de esta técnica se llega a la verdad de los hechos y es en la judicialización donde se ejerce el derecho de defensa.

4.4 Análisis de entrevista 2.

En el cometimiento de un hecho delictivo de carácter informático o en cualquier delito de gravedad la técnica del agente encubierto es incorporado bajo los parámetros que establece el reglamento interno de la policía es decir que son agentes entrenados de forma rigurosa bajo las instrucciones fiscales que por ser una técnica de actualidad, implica otras funciones a las que hace el agente tradicional como grabar conversaciones, acceder a

Archivos ilícitos, imágenes de encuentros, en este orden de ideas, todo lo anterior, debe ser autorizado por la fiscalía por lo que la gente encubierto digital, durante el desarrollo de la investigación se encuentra limitado debido a que la fiscalía mantiene una vigilancia de deberes durante la investigación en aras de garantizar un buen resultado, y como consecuencia pueden darse nuevas coordinaciones, según como se va desarrollando la investigación. La prueba que recopila el agente encubierto digital es analizada debido a que debe cumplir con los requisitos de ley ya que deben ser útiles y pertinentes.

Pero también esta técnica es utilizada como última medida, ya que no es una técnica que implementan en todos los casos, no es aleatoria, si no en cada caso concreto, dónde al realizar una exhaustiva revisión y bajo los principios de subsidiariedad, proporcionalidad y necesidad, por lo que en este análisis de entrevista se considera que existe la necesidad de un control judicial en la medida que debe tenerse claro que existe una vulneración de derechos fundamentales y que la técnica no es automática, sino que son casos concretos donde una gente con conocimiento en las tecnologías, y una preparación, ingresa bajo la dirección funcional de la fiscalía a realizar una investigación, remitiendo informes de seguimiento, pero esto no quiere decir que el control judicial no sea necesario debido a que toda persona tiene derecho a un juicio justo y el juez es garante desde el debido proceso, y el juez valora en una sentencia, lo que ha sido debatido por ambas partes en audiencia es decir que le da una mayor fiabilidad a la investigación.



UNIVERSIDAD GERARDO BARRIOS.

Alcances de la figura del agente encubierto digital y sus implicaciones en la investigación de los delitos informáticos frente al derecho de defensa del imputado.

ENTREVISTAS FISCALES

ENTREVISTA 3. Anónima

1. ¿Cómo opera la técnica del agente encubierto digital en nuestro país?

Encubierto digital nace en busca de legitimar las prácticas de Con el fin de incorporar evidencia de naturaleza digital en los procesos penales artículo 282 del código procesal penal, según el caso que lo amerite.

2. ¿Cuáles son los parámetros para la aplicación de la técnica del agente encubierto digital?

El parámetro de aplicación es para aquellos delitos cometidos mediante temas informáticos a fin de incorporar evidencia digital en el juicio penal.

3. esta técnica es para los delitos informáticos que se requieran y así se recolecte evidencia digital en la investigación ¿cuáles serían los criterios para implementarla?

A criterios siempre como última opción ya que siempre se debe respetar los derechos humanos del ciudadano, pero se verán efectuados de alguna forma por el agente encubierto ya que este busca, vigila y extrae, cualquier tipo de información y ya sea en dispositivos o transferencia o mediante las tecnologías.

4. ¿Cómo es el proceso para el nombramiento de un agente encubierto digital, según el caso concreto?

Debe asignarse un agente encubierto digital por el departamento de investigaciones de la PNC, siempre autorizado por la Fiscalía General de la República, dentro de los requisitos legales, el agente debe ser miembro de la PNC y ser capacitado en el manejo de evidencia digital.

5. ¿Cuáles son las acciones que pueden ser autorizadas en una determinada investigación en delitos informáticos?

El agente está facultado para vigilar, buscar, y extraer cualquier información mediante las tecnologías y es considerado como evidencia digital, deberá tener límites, pero, así como está planteada la reforma del 259-D no existe control y se estarán haciendo acciones que pongan en peligro la libertad de expresión, intimidad y seguridad.

6. ¿Todas las funciones que realiza el agente encubierto digital son autorizadas por la fiscalía?

Deberán estar establecidas las funciones en la autorización de la fiscalía, previo un estudio completo del caso, pero se dejan algunas a su discrecionalidad, por ser muy amplias sus funciones.

7. ¿cómo procesan, la prueba digital recopilada por el agente encubierto digital?

Es estudiada como evidencia digital, esa prueba y es admitida dentro de los requisitos de ley, así como valorada bajo la sana crítica.

8. ¿En qué responsabilidad podría recaer, el agente digital encubierto, en el cumplimiento de sus funciones?

Que podría incurrir en responsabilidad penal, y el agente encubierto sobre pasas tus funciones, revela información, y la extravía entre otras acciones.

9. ¿Como garantizan el derecho de defensa del acusado, durante la investigación y al judicializar los casos?

En la investigación de los delitos, esta técnica es necesaria en circunstancias que al existir sospechas fundadas y no encontrar otro método para llegar a la verdad se utiliza esta figura, respetando las garantías de la constitución y otras leyes, el derecho de defensa se ejerce cuando se presenta el requerimiento.

4.5 Análisis de entrevista 3.

El agente encubierto digital es una técnica utilizada exclusivamente en delitos de naturaleza digital, es decir, aquellos donde se amerite para encontrar la verdad en determinado hecho, por lo que no es utilizada en todos los casos, debido a que están en juego derechos fundamentales de las personas, por lo que es de ultima ratio, en ese sentido, el fiscal debe valorar si no existe otra forma de investigar determinado hecho.

Debido como ya lo establece el fiscal, si acuerdan las funciones, pero al momento de la ejecución quedan algunas a discrecionalidad del agente encubierto, por lo que los alcances de dicho agente pueden verse de una forma libre, por lo que necesita un control judicial, lo cual, permitiría garantizar el debido proceso, se debe tener en cuenta que dicha discrecionalidad, puede recaer en una violación a derechos de una persona, toda investigación en el que se implemente la técnica del agente digital encubierto debe tener límites claros, por lo que en ese sentido, no están establecidos en la nueva reforma del artículo 259-D.

4.6 Análisis de entrevistas a operadores judiciales.



UNIVERSIDAD GERARDO BARRIOS.

Alcances de la figura del agente encubierto digital y sus implicaciones en la investigación de los delitos informáticos frente al derecho de defensa del imputado.

GUÍA No 1. DE ENTREVISTA A OPERADORES DEL SISTEMA JUDICIAL.

1. **¿Cuál es su opinión respecto al agente digital encubierto y que no es autorizado por un juez?**

Considero que se puede prestar a vulneraciones a derechos de las personas, a quienes persiguen en la investigación de los delitos informáticos, por lo que estaría más controlada si esta está bajo el estricto control de un juez, quien garantizaría el derecho de defensa.

2. **¿En la práctica, cual son las consideraciones para valorar la evidencia digital?**

A través de los peritos, quienes deben llenar los requisitos, que deben contener los informes realizados, así mismo su entrevista para que exista veracidad y así condenar a personas que delinquen por medios informáticos.

3. ¿Considera indicado el rol de la defensa en los casos donde se infiltra un agente encubierto digital?

La defensa podría proponer un nuevo perito para revalorar la prueba presentada, incluso ya que no existe un control judicial, puede ser una forma para refutar y se demuestre la veracidad de la información obtenida por dicho agente, que ya la fiscalía en base a sus funciones es quien faculta.

4. ¿Considera que existe violación al derecho de defensa?

El defensor desde que tiene noticia que una persona está siendo procesada, en este caso toda la investigación se hace sin la asistencia de un defensor por lo que podría violentar el derecho de defensa, desde que se tiene noticia debe estar informado, porque tiene derecho a que cada prueba a emitir necesita que un defensor que le asista.

5. ¿Considera que en la investigación de estos delitos se violenta derechos fundamentales?

Si violenta derechos en el momento de la investigación, la constitución ya establece el derecho a la intimidad, que es el que más vulnera y sobre todo que no es autorizado por un juez.

6. ¿Considera que el agente encubierto digital es un apoyo en la investigación de los delitos informáticos?

Ya existe otros mecanismos por los cuales se investiga delitos informáticos.

7. ¿Cuáles mecanismos? Escuchas telefónicas donde si se requiere autorización digital.

4.6.1 Análisis de guía 2

A criterio del operador judicial que dio respuesta a las preguntas realizadas durante la entrevista, cabe la posibilidad de recaer en vulneración de derechos fundamentales a causa de la ausencia de un estricto control por parte de un juez, específicamente al derecho a la intimidad; así mismo, que es una figura utilizada en última instancia en una investigación, considerando que existen otros mecanismos para la investigación de delitos tecnológicos, por ejemplo: las escuchas telefónicas, en la que sí media una autorización judicial.

Respecto al derecho de defensa, este considera que el defensor tiene un papel importante desde el momento que tiene conocimiento debido a que, para su representado, quien podría tener un amplio campo de procesamiento de la información recolectada por el agente, lo cual, debe identificar una legalidad íntegra en la investigación.

La información recabada por la fiscalía a través de la policía, considera el operador que puede tener otros mecanismos, el abogado defensor al momento de presentar las diligencias y tenga conocimiento podría solicitar un nuevo perito, que de fe de la veracidad de la información, lo cual, por ello es de importancia en esta entrevista recalcar, que al no tener control judicial, es deber del abogado defensor trabajar con diligencia, en cada caso concreto, por lo que no hay juez quien garantice dicho derecho durante la investigación.

Análisis estructurado a entrevistas a operadores judiciales.

¿Cuál es su opinión respecto al agente digital encubierto y que no es autorizado por un juez?

Aquí la opinión de los jueces está dividida: por un lado un juez considera que sí se vulnera la garantía de defensa, pero el juez número dos, establece que por ser competencia, es suficiente



UNIVERSIDAD GERARDO BARRIOS.

Alcances de la figura del agente encubierto digital y sus implicaciones en la investigación de los delitos informáticos frente al derecho de defensa del imputado.

GUÍA No 2. DE ENTREVISTA A OPERADORES DEL SISTEMA JUDICIAL.

1. ¿Cuál es su opinión respecto a la técnica de operación encubierta del agente digital encubierto y que no es autorizado por un juez?

En estricto sentido, conforme los parámetros legales que la Fiscalía tiene en la dirección de la investigación, esta cuenta con las facultades para investigar cualquier tipo de hecho delictivo con el auxilio de personal técnico, para el caso lo hace de la policía nacional civil; resultando esta técnica un gran aporte investigativo, que ayudará a la investigación de la multiplicidad de delitos que se cometen de manera electrónica.

2. En cuanto a la práctica de esta técnica en la investigación de delitos informáticos y conexos, en la que no existe un control judicial; cuál es su consideración.

No debe perderse de vista, que cuando la investigación implica invasión de la intimidad o vulneración a derechos fundamentales, esa investigación debe ser controlada por un juez, ya que el ente jurisdiccional, es el encargado de vigilar que se cumplan los

presupuestos de idoneidad, proporcionalidad y necesidad, en la afectación o invasión a bienes jurídicos fundamentales.

3. ¿Cuál es el parámetro de validación de la evidencia digital recolectada durante la investigación, por parte del agente encubierto digital?

Para determinar la validez de la evidencia digital al igual que cualquier prueba, debe haberse obtenido en legal forma e incorporado en legal forma al proceso.

4. Como operador judicial ¿Cuáles son los criterios para valorar la evidencia digital obtenida por el agente digital encubierto?

La acreditación de la autenticidad de la evidencia y la acreditación del especialista que la incorpora.

5. Considera usted que, en los procesos penales, en los que interviene el agente encubierto digital se cumple el principio de contradicción.

Tiene las mismas posibilidades, la defensa tiene todas las facultades de refutar la prueba o evidencia incorporada a un proceso iniciado, proponer incluso los técnicos especialistas que le permitan debatir la misma.

6. ¿Según su criterio, podría o no existir una violación al derecho de defensa debido al retraso del conocimiento de las diligencias investigativas por parte del investigado?

No puede considerarse que existe vulneración al derecho de defensa, pues como en toda investigación, lo que se percibe es la determinación de la existencia de un delito; la defensa tendrá la oportunidad de valorar dentro del proceso si la investigación fue legal, por lo tanto, no se vulnera el derecho de defensa; pues es hasta el momento en que se determina la existencia del delito y la judicialización del caso, es que se realizan señalamientos directos contra el imputado.

7. ¿En qué caso considera que esta técnica del agente encubierto digital podría violentar derechos fundamentales al justiciable por el cometimiento de un delito informático?

Pueden verse afectados derechos fundamentales, por el hecho de que las investigaciones carecen de un control judicial, por ello considero que lo primordial sería que para la práctica de esta nueva técnica mediara autorización judicial.

4.6.2 Análisis de guía 3.

Para el entrevistado la técnica de operación encubierta del agente encubierto digital, realizada conforme a los parámetros y direccionamiento de la Fiscalía General de la República, resulta de gran aporte investigativo para la investigación de la multiplicidad de delitos cometidos de manera electrónica; ello tomando en cuenta que son los entes encargados de aplicarla y que toda investigación que implique invasión a la intimidad o vulneración a derechos fundamentales, existe la probabilidad que los derechos fundamentales se vean afectados, por ello es necesario el control judicial a efectos que se cumplan los presupuestos de idoneidad, proporcionalidad y necesidad, por lo que es un punto a tomar en cuenta.

Considerando que no existe una vulneración al derecho de defensa, debido a que la persona investigada tiene su momento para manifestarse con relación a su defensa.

4.7 Entrevista a defensores



UNIVERSIDAD GERARDO BARRIOS.

Alcances de la figura del Agente Encubierto Digital y sus implicaciones en la investigación de los delitos informáticos frente al derecho de defensa del imputado.

anónima

GUÍA DE ENTREVISTA A DEFENSORES TÉCNICOS.

1. **¿Cuál es su opinión respecto a la técnica de operación encubierta del agente digital encubierto y que no es autorizado por un juez?**

La opinión es que si no lo autoriza un juez estaríamos en una ilegalidad al menos que el régimen de excepción sea de forma definitiva.

2. **En cuanto a la práctica de esta técnica en la investigación de delitos informáticos y conexos, en la que no existe un control judicial; cuál es su consideración.**

Mi consideración es que estaríamos ante un atropello porque podrán involucrar a cualquier persona en un delito y podrán espiarlo acosarlo solo porque se les antoja.

3. **Considera usted que, en los procesos penales, en los que interviene el agente encubierto digital se cumple el principio de contradicción**

No se cumple porque el imputado y el defensor no podrá preguntar como ha sido la investigación debido a la calidad que tiene de a gente digital.

4. ¿Según su criterio, podría o no existir una violación al derecho de defensa debido al retraso del conocimiento de las diligencias investigativas por parte del investigado?

Si le notifican al que lo están investigando no habrá violación al derecho de defensa porque podrá defenderse. Pero aquí siempre el investigado se da cuenta hasta que presentan un requerimiento o le giran una orden administrativa.

5. ¿En qué caso considera que esta técnica del agente encubierto digital podría violentar derechos fundamentales al justiciable por el cometimiento de un delito informático?

En todos los casos, debido a que todos los procedimientos en esta técnica son de los mismos métodos de investigación, por lo que vulneran derechos fundamentales.

Análisis de entrevista. Entrevista 1

El agente encubierto digital es una técnica en delitos meramente informáticos, donde es la fiscalía la encargada de implementarla según el caso concreto, situación que para los defensores públicos, es ilegal debido a los derechos fundamentales, debe estar sujeta al control judicial, pero que puede ser legal en el régimen de excepción donde hay pérdida de derechos fundamentales, esto si fuera de forma permanente, por lo que debe ser regulado un control judicial, en aras de garantizar el derecho de defensa, porque podría haber un aprovechamiento de parte de las instituciones, durante las audiencias no existe el principio de contradicción debido a la calidad del agente encubierto, no se tiene la posibilidad de indagar en la investigación, esto agrava el derecho de defensa, que si le notificaran al imputado y su defensor la investigación no habría violación, pero en este tipo de técnica, el imputado tiene conocimiento hasta que es detenido o hasta que se presenta el requerimiento al tribunal.



UNIVERSIDAD GERARDO BARRIOS.

Alcances de la figura del agente encubierto digital y sus implicaciones en la investigación de los delitos informáticos frente al derecho de defensa del imputado.

GUÍA N° 2. ENTREVISTA A DEFENSORES TÉCNICOS.

Lic. Pedro Antonio Cuellar Arévalo.

1. ¿Cuál es su opinión respecto a la técnica de operación encubierta del agente encubierto digital y que no es autorizado por un juez?

Se vulnera, la intermediación, ya que la norma exige que toda prueba debe ser sometida a conocimiento del juez y en algunos casos específicos para ser validos debe ser autorizada su práctica por el juez, los requisitos ya están establecidos y en los de este tipo es uno de ellos, por su propia naturaleza que se puede prestar a manipulación antojadiza de quien la presenta al juez, y este no le quedaría más que simplemente recibirla(error) o rechazarla (en el mejor sentido) pues no tuvo intermediación; *así lo reconoce la Sala de lo Constitucional de la Corte Suprema de Justicia en parte de su jurisprudencia.*

2. En cuanto a la práctica de esta técnica en la investigación de delitos informáticos y conexos, en la que no existe un control judicial; cuál es su consideración.

Se vulnera el derecho de defensa, el derecho a la intimidad y seguramente otros por analizar; en el caso del defensa porque para el defensor no hay oportunidad de controvertir o inmediar su obtención sino que solo el resultado final el cual muy probablemente haya sido manipulado, y pues no sería raro que lo manipule la FGR y la

PNC (áreas de informática encargadas) ya que estos no obstante la ley les ordena la obtención e incorporación tanto de la prueba de carga como de descarga, siendo realistas el ente encargado de la investigación FGR y sus subalternos PNC no cumplen y solo incorporan generalmente los de carga, y el motivo “*secreto a voces*” es simplemente que el fiscal de cada caso para mantener su cargo o trabajo, debe dar resultados condenatorios ante sus jefes y es ahí entonces que la honestidad se pierde y no conviene a sus intereses personales, y resulta evidentemente un menoscabo al derecho de defensa del imputado que a todas luces es una injusticia; en cuanto al derecho a la intimidad se pierde efectivamente pues es evidente que los encargados de la investigación digital tendrán que leer todas las conversaciones inclusive las que no conciernen al caso y sin duda cada persona tiene conversaciones íntimas con su pareja, negocios privados con sus clientes, acuerdos con sus socios, pláticas delicadas con su familia, y el agente encubierto un ser humano como todos con errores y defectos no será inmune a su sensibilidad personal y en más de una ocasión podrá aprovechar lo que no concierne a su función o investigación para provecho propio de un tercero, así es el ser humano en sin fin de situaciones.

3. Considera usted que, en los procesos penales, en los que interviene el agente encubierto digital se cumple el principio de contradicción.

Absolutamente no se respeta el principio de contradicción, pues la contradicción solo podrá ser posible al resultado, por tanto, el defensor y el juez estarían aislados al conocimiento en cuanto al método, la legalidad, y el medio de obtención del resultado.

4. ¿Según su criterio, podría o no existir una violación al derecho de defensa debido al retraso del conocimiento de las diligencias investigativas por parte del investigado?

Si hay violación legal a los derechos fundamentales definitivamente: aunque es evidente que el investigado por razones de obstaculización de la investigación podría interferir o adelantarse a la investigación, más en estos delitos que las claves de los perfiles de redes sociales estarían a su disposición y al saber este inmediata e inminentemente intentará borrar sus huellas; pero ahí hay una situación a valorar muy de coherencia en relación lógica a la situación, que consiste en que: quien pone denuncia, o el afectado víctima por este delito puede poner por escrito sus cuentas de redes sociales o de

comunicación digital a disposición del ente investigador y este así ya tendría permiso legal para entrar a la intimidad de la víctima y justifica parte de su actuar pues esto no inhibe que posteriormente se deba comprobar la situación con la intervención judicial y defensora; la diferencia con el investigado como ya dije ciertamente este puede interferir, pero es más pesado el derecho a la intimidad que le merece versus la investigación de un “probable hecho” donde el que demanda o denuncia es el encargado de aportar la prueba y debe sopesarse definitivamente sin lugar a dudas abstractas.

5. ¿En qué caso considera que esta técnica del agente encubierto digital podría violentar derechos fundamentales al justiciable por el cometimiento de un delito informático?

Absolutamente cualquier caso puede suceder: veamos pues *cada caso es muy particular* y hay que valorar en base a la sana crítica, los derechos fundamentales y el caso concreto pues cualquier caso se puede prestar según los hechos que se deban investigar y los alcances o límites que debe tener en cuenta el agente encubierto, deben delimitarse clara y específicamente.

Guía No 2.

Para el entrevistado el licenciado Cuellar Arévalo, la figura del agente encubierto digital, es una técnica que pone en desventaja el derecho de defensa, ello por no haber una intervención judicial, ya que la información obtenida durante la investigación por parte del agente encubierto, no cuenta con un control o supervisión por parte de un juez, quedando todo únicamente a decisión de la policía y de la fiscalía, pues considera que estos solo se enfocan en la prueba de cargo no así la de descargo, lo que además supone un grave riesgo que esta sea distorsionada; así también considera que si bien no es coherente que el investigado tenga conocimiento con anterioridad que está siendo investigado, pues este intentaría obstaculizar toda evidencia, ya dentro del proceso penal la defensa queda en desventaja pues es hasta que la prueba ya está incorporada al proceso (sin existir un control judicial) que el defensor puede refutarla, con lo cual no se cumple el principio de inmediación y tampoco el principio de contradicción. Considerando que se vulnera específicamente el derecho a la intimidad y de defensa de la persona imputada.



UNIVERSIDAD GERARDO BARRIOS.

Alcances de la figura del agente encubierto digital y sus implicaciones en la investigación de los delitos informáticos frente al derecho de defensa del imputado.

GUÍA N° 3. ENTREVISTA A DEFENSORES TÉCNICOS.

Lic. Cristóbal Amaya.

1. ¿Cuál es su punto de vista sobre la técnica de operación encubierta del agente encubierto digital?

Mi consideración es que, la técnica puede ser efectiva siempre y cuando se tengan las herramientas técnicas que lleven a una verdad real, es de hacer ver que está en juego el derecho fundamental de la privacidad, en varias vertientes, la mala utilización de la técnica conlleva una violación a derechos fundamentales. -

2. En la práctica cómo considera usted, esta técnica durante la investigación de delitos informáticos, en la que no existe un control jurisdiccional.

Si no existe un control judicial carece de legalidad, ya que no se puede considerar la técnica como eficaz por carecer de una legalidad esta sea procesal, material o incluso administrativa. –

3. Considera usted que se cumple el principio de contradicción, en los procesos en los que interviene el agente encubierto digital.

Difícilmente se puede llegar a contradecir esta técnica, ya que, en su mayoría de técnicas especializadas de investigación, el abogado defensor desconoce su forma de llevarse a cabo y no tiene el acceso a las herramientas que faciliten su contradicción. –

4. ¿Según su criterio, podría o no existir una violación al derecho de defensa debido al retraso del conocimiento de las diligencias investigativas por parte del investigado?

Si, puede existir violaciones a la tutela judicial efectiva, ya que se está llevando una investigación que no tiene todos los elementos útiles para una contradicción, sumado a ello el poder acezar a las evidencias y poder cotejar en algún momento con otra que aporté elementos de contradicción.

5. ¿En qué caso considera que esta técnica de operación encubierta podría suponer violación de derechos fundamentales al imputado por el cometimiento de un delito informático?

En los casos donde solo la parte acusadora tenga las herramientas y el acceso a las evidencias; así mismo el no poder tener acceso a la información que se sustrae por motivos de no violar derechos fundamentales o alterar la evidencia. –

Guía N° 3.

A criterio del licenciado Amaya, la implementación de esta técnica de operación encubierta, si no se practica haciendo el uso adecuado de las herramientas y los fines de la investigación, supone una vulneración a derechos fundamentales del imputado, puesto que estos están de por medio en todo proceso penal; además considera que no se cumple el principio de contradicción por ser estas técnicas especializadas, las cuales a los defensores les resulta difícil contradecir o refutar. Por todo ello, el profesional considera que si esta herramienta no se realiza con la intervención judicial, y las herramientas adecuadas, respetando el derecho a la intimidad, recae en una violación a derechos fundamentales al igual que al derecho de defensa.

HALLAZGOS DE LA INVESTIGACIÓN.			
Criterio.	Agentes fiscales.	Operadores judiciales.	Defensa técnica.
Funcionamiento.	Debe ser autorizado por el fiscal.	Debería ser autorizado por el juez.	Debe ser autorizado por el juez.
Necesidad de la técnica.	Atiende a la política fiscal.	Debería ser decisión del juez competente.	Debería ser decisión del juez competente.
Necesidad tecnológica.	Sí es necesaria por evolución de las tecnologías.	Sí es necesaria por evolución de las tecnologías.	Debería usarse sólo en casos específicos.
Derecho de defensa y su vulneración.	Consideran que no se vulnera.	Consideran que sí se vulnera.	Autorización administrativa es ilegal.
Contradicción de la evidencia.	La contradicción se dará hasta que se judicialice el caso.	La contradicción se hace en el proceso.	No existe una verdadera contradicción, por falta de acreditación de la identidad del investigador y no hay forma de controvertir la información.
Discrecionalidad de las funciones.	Es acorde por la naturaleza de la investigación.	Es necesario una regularización.	Es violatoria por no ser reglado conforme a ley.
Ausencia de control judicial.	Los agentes fiscales están completamente de acuerdo con ser ellos quienes autoricen el funcionamiento del agente digital encubierto, lo cual a consideración del grupo investigador no es lo más idóneo por efecto de la necesidad del control judicial.	La opinión es dividida uno consideró que sí se vulneró, otro que no.	Autorización administrativa es ilegal.
Efectividad de la técnica.	Es necesaria y efectiva.	Debe ser ponderada.	Sólo en los casos que la ley debería preveer.

Violación a derechos y garantías fundamentales.	No existe violación a los derechos fundamentales.	La ausencia de control judicial podría configurar violación de éstos.	La ausencia de control judicial sí vulnera los derechos y garantías fundamentales.

CAPÍTULO V. CONCLUSIONES.Y RECOMENDACIONES.

5.1 Conclusiones.

Habiéndose realizado el análisis por el equipo investigador, de los elementos doctrinales, jurídicos y los hallazgos obtenidos en las entrevistas, se concluye lo siguiente:

La técnica del agente encubierto digital fue configurada sin ningún control de conformidad a la ley, para los operadores de la investigación del delito. Reconocemos que la estructura de nuestro proceso penal, en la investigación del delito está en manos de la Fiscalía General de la República, ello como una salvaguarda de la imparcialidad del juzgador, pero hay razones de peso para afirmar que en materia de investigación del delito, el juez no es un mero espectador, pues en los actos de investigación en los cuales debe limitarse derechos fundamentales, es una labor de la cual el juez no ha sido excluido, pues solo de esa forma se garantiza que la limitación sea producto de un juicio de ponderación, sea temporal y necesaria, con la finalidad de hacer efectivo el derecho de defensa, la cual se dispone dentro del ordenamiento jurídico como inviolable, en tanto la configuración normativa que presenta nuestro ordenamiento jurídico, la técnica del agente encubierto digital, podría vulnerar el derecho de defensa, por colocar al imputado en desventaja, respecto de la información recolectada sin ningún control Judicial.

La regulación del agente encubierto digital, presenta una regulación exigua, pues habida cuenta se legisló en un solo artículo, en tanto, no hay términos o plazos de duración en su implementación, con ello, se garantizaría una seguridad jurídica para el investigado, así como también el término de red pública, es bastante abierto, por lo que queda a discrecionalidad de operador ingresar a donde el considera puede encontrar información, otra situación a considerar es que toda la información encontrada no presenta ninguna regulación de cómo será procesada y si la misma podría ser presentada de forma íntegra o editada al proceso, lo cual coloca en desventaja al acusado, y como no hay autoridad judicial que haya controlado la recolección del descubrimiento probatorio información, no existe posibilidad de contradecir dicha información, ello es violatorio al derecho de defensa.

El agente encubierto digital, al entrar a la privacidad de las comunicaciones del investigado, entra en colisión con la garantía de inviolabilidad de la correspondencia, la cual sólo puede vulnerarse a través de autorización judicial.

Después de estudiar y analizar la técnica de investigación de agente encubierto digital, descubrimos que la misma presenta similitudes a las intervenciones de las telecomunicaciones, en cuanto a que en su aplicación existe una vulneración de derechos fundamentales, que si bien, esta técnica se desarrolla en un entorno donde se encuentra en dirección de la Fiscalía General de la República , pero en su estructuración se procuró en armonía con el derecho de defensa, pues para el uso de la misma se dispone que será el juez quien controle su implementación, así como personal de derechos humanos según operadores de la acción, de forma temporal es decir, se establece un plazo la investigación y sobre ciertos dispositivos, la información recolectada de forma integral podrá ser consultadas por las partes una vez se ingresa al proceso, de tal forma que el acusado puede determinar y utilizar en que contexto fue encontrada la información,

Como investigadores, consideramos que la técnica de investigación del agente encubierto digital es una técnica de investigación útil y necesaria en la investigación de los delitos informáticos, debiendo respetarse requisitos que no están contemplados en la reforma, como limites, control judicial, plazos, pero la misma debe ser configurada guardando armonía con el derecho de defensa del acusado, lo cual podría alcanzarse con una configuración distinta, ya que a nuestro juicio la investigación del delito tiene como limite el respeto irrestricto a las garantías procesales, constitucionales y convencionales de los procesados.

5.2 Recomendaciones.

Reformar el artículo 259 – D del código Procesal Penal, en los siguientes aspectos:

Establecer el control judicial sobre los hallazgos de la investigación y la recolección de la información íntegra; ya sea de forma anticipada o posterior, y regular plazo para la recolección de la información.

Establecer el campo de aplicación en los canales cerrados de internet ya que es inofensivo dicha figura en los canales abiertos. Porque los canales abiertos están contenidos e indexados de manera pública y el acceso al contenido de estos es libre e ilimitado.

La aplicación de agente encubierto digital será en los canales cerrados de internet previa autorización judicial.

Establecer parámetros de control para garantizar la integridad de los indicios probatorios recolectados a efectos de garantizar una adecuada defensa en juicio; en virtud de la amplia discrecionalidad en la ejecución del direccionamiento fiscal del que goza con la configuración actual dicho investigador encubierto digital.

Establecer parámetros de control para garantizar la integridad de los indicios probatorios recolectados, a fin de evitar que la información aportada al proceso pueda ser fraccionada o descontextualizada; y así garantizar un hallazgo íntegro de la información y proteger el derecho de defensa.

Establecer en el art. 259 -D, la garantía del secreto de lo privado en la información del sujeto de investigación, que no esté relacionada con dicha investigación a efecto de inhibir un uso fraccionado o descontextualizado de la información que el agente recolecte.

Propuesta de Reforma del art. 259 – D.

Para garantizar el derecho de defensa y demás derechos fundamentales del imputado se propone la reforma siguiente al art. 259 – D del Código Procesal Penal:

Refórmase el art. 259 – D:

Art. 259-D.- Durante la investigación de los delitos contenidos en la Ley Especial Contra los Delitos Informáticos y Conexos u otros contenidos en leyes penales especiales, y de conformidad con lo establecido en el Art. 175 inciso cuarto de este Código, previa autorización judicial, debidamente fundada, y por escrito, a solicitud de la Fiscalía General de la República podrá ordenarse la realización de operaciones encubiertas digitales que resulten necesarias, las cuales estarán a cargo de la policía, en los canales cerrados de internet

Los jueces competentes para autorizar dicha técnica serán los jueces de instrucción de la ciudad de San Salvador cuya duración máxima será de 6 meses prorrogables por un máximo de 2 años, atendiendo a los fines de la investigación debiendo detallar las actuaciones que el agente encubierto digital deberá realizar

La resolución que autorice el agente encubierto digital deberá constar tanto el nombre real del agente como el alias a usar por el mismo, la cual será reservada.

Durante la investigación deberán conservarse todas las actuaciones realizadas por el agente encubierto digital y podrán ser consultadas por el defensor una vez que el caso se judicialice de conformidad con el art. 356 de este código.

Preservándose en todo caso el secreto de lo privado de la información que no guarde relación con el proceso.

La policía también podrá realizar la búsqueda a través de las Tecnologías de Información y Comunicación de carácter abierto o público, incluyendo las páginas de internet, de evidencia digital que constituya el hecho punible informático o pueda servir de prueba para el mismo, por medio de programas informáticos que le permitan Identificar los

valores únicos identificativos de tal evidencia digital, o mediante la búsqueda o indagación libre en tales espacios informáticos virtuales.

La policía y o la fiscalía podrán celebrar acuerdos con entes públicos o privados con sede en otros países, que le permitan recibir y documentar noticias criminales del cometimiento de hechos delictivos de forma directa, inclusive mediante el uso de las Tecnologías de la Información y Comunicación; la información así recibida podrá ser incorporada al proceso como evidencia digital, conforme a las regulaciones de este capítulo

GLOSARIO.

Agente encubierto digital. miembro de la Policía que realiza funciones de investigación de delitos y que, por lo mismo, la competencia para autorizar este tipo de agentes ha sido otorgada por ley al fiscal general de la República, en virtud que no se trata de una simple investigación, sino de una autorización a una persona para que delinca a efecto de comprobar la participación delincuencia de otra u otras personas integrantes de una organización delictiva.

Almacenamiento. Es el lugar establecido según el caso, para resguardar la información

Canales cerrados. son aquellas que se caracterizan por la expresa voluntad del comunicante de excluir a terceros del proceso de comunicación.

Ciberbullyn. Es un acoso a través de redes sociales.

Ciberdelincuencia: son todos los ilícitos cometidos a través del sistema informático.

Convenio de Budapest: versa sobre la ciberdelincuencia por parte del Consejo Europeo.

CPP, c. Pr. Pn: Código Procesal Penal.

Criminología. ciencia general de la criminalidad y de las penas.

Debido proceso. conjunto de requisitos que deben observarse en las instancias procesales a efectos de que las personas estén en condiciones de defender adecuadamente sus derechos ante cualquier acto del Estado, adoptado por cualquier autoridad, sea administrativa, legislativa o judicial, que pueda afectarlos.

Defensa material. ejercicio de la defensa que lleva a cabo personalmente el propio imputado y que se manifiesta en diferentes formas y oportunidades.

Defensa técnica. actividad que se ejercita durante todo el proceso con el fin de eliminar toda duda que el ejercicio de la acción penal ha producido con relación a una persona determinada.

Delito. acción antijurídica, típica, culpable y sancionada con una pena.

Delitos informáticos. comprenden todas las acciones típicamente antijurídicas para cuya consumación se utiliza o se afecta perjudicialmente una computadora o sus accesorios y se incluyen las acciones de uso indebido del software, apropiación o comunicación ilícita de datos, interferencias de bancos electrónicos ajenos de datos, y muchas otras conductas antijurídicas relacionadas con la informática.

Derecho a la intimidad: es aquel que está vinculado a aspectos privados, es decir, situaciones interpersonales, valores, sentimientos, entre otros aspectos vinculados a la propia existencia de su titular

Derecho a la no autoincriminación. Tiene la finalidad de erradicar aquel afán por lograr la confesión del imputado, también conocido como Derecho a no declararse culpable.

Derecho de defensa. derecho de toda persona a ser oída con las debidas garantías y dentro de un plazo razonable por un juez o tribunal competente, independiente e imparcial, establecido con anterioridad por la ley en la sustanciación de cualquier acusación penal en su contra o para la determinación de sus derechos de carácter civil, laboral, fiscal u otro cualquiera.

Derechos fundamentales. todos aquellos derechos que constituyen el asiento o fundamento de protección de la vida o actividades esenciales de las personas, permitiendo el desarrollo de estas y el ejercicio de libertades públicas.

Derechos Humanos. Son aquellos derechos que son inherentes a la persona humana.

Estado. forma y organización de la sociedad, de su gobierno y al establecimiento de normas de convivencia humana.

Evidencia digital: los documentos digitales, mensajes electrónicos, imágenes, videos, datos y cualquier tipo de información que sea almacenada, recibida o transmitida a través de las tecnologías de la información y comunicación o por medio de cualquier dispositivo electrónico.

Garantías constitucionales. cumulo de principios, derechos y libertades fundamentales reconocidas por la constitución y “lato sensu”, por los tratados internacionales que tienen por finalidad otorgar al imputado un marco de seguridad jurídica, y en última instancia, mantener un equilibrio entre la llamada búsqueda de la verdad material y los derechos fundamentales del imputado.

Garantías procesales. todos aquellos derechos que tienen como finalidad la protección de la persona que se encuentra sometida a un procedimiento legal ante una autoridad competente, que puede ser de orden civil, laboral, fiscal, o cualquier otro carácter.

Internet. es un sistema global de dispositivos interconectados que utiliza la familia de protocolos TCP/IP para dar servicio a varios miles de millones de usuarios en todo el mundo.

Investigación criminal. proceso tendiente a comprobar la existencia de un hecho o conducta delictiva, identificar o por lo menos individualizar a sus autores y partícipes, así como recolectar las evidencias que permitan definir la responsabilidad de los mismos.

LECrim. Ley de Enjuiciamiento Criminal.

Motor de búsqueda: aplicación para buscar dentro de las páginas web indexadas en el internet.

Normas ISO: guía para actividades relacionadas con el manejo de la evidencia digital.

Obtención. Es aquel procedimiento de quitar de la esfera jurídica del titular, determinado objeto que sea útil en la investigación

OCDE: Organización de Cooperación y el Desarrollo Económico.

OEI: Organización de Estándares Internacionales.

Presunción de inocencia. Es una garantía que permite considerar inocente al imputado mientras no se compruebe su culpabilidad.

Proceso penal. Es aquel sistema utilizado para realizar el ius puniendi del estado, a través del cual trata de averiguar la comisión de un hecho delictivo.

Programas tecnológicos. Son los diversos programas que existen en la red, para determinado uso.

Prueba ilegal: aquella que se obtiene, sin vulnerar derechos fundamentales, pero sin respetar las normas de procedimiento legalmente establecidas.

Prueba ilícita: aquella donde su origen ha vulnerado un derecho o libertad pública o se producen con absoluta inobservancia de las reglas de procedimiento.

Prueba irregular: aquella realizada sin la observancia de los requisitos legales, pero que sin ello causa indefensión.

Prueba testimonial. Es un medio de prueba que permite y garantiza a través de un testimonio la verdad de los hechos.

Red oscura. Es una parte de la red que solo es accesible mediante ciertos navegadores o configuraciones de red determinadas.

Red privada. es aquella en la que las conexiones dentro de una red específica se establecen restricciones para promover un entorno seguro.

Red pública. es aquella en la que cualquier persona, es decir, el público en general tiene acceso y, a través de ella, puede conectarse a otras redes o a Internet.

Resguardo. Son las diversas formas o técnicas que se establecen para almacenar la información útil en el proceso.

Técnicas de investigación del delito. herramientas con las que cuenta el estado para descubrir la verdad cuando se tiene indicios que se cometió un ilícito penal.

TIC. Tecnologías de la Información y de la Comunicación.

- Ascencio Mellado, J. M., & Fernández López, M. (2017). *Justicia Penal y Nuevas Formas de Delincuencia*. Tirant lo Blanch.
<https://latam.tirantonline.com/cloudLibrary/ebook/show/9788491198017>
- Batthyány, K. y C. (2013). *Metodología de la investigación en Ciencias Sociales*.
https://perio.unlp.edu.ar/catedras/mis/wp-content/uploads/sites/126/2020/04/p.2_batthianny_k._cabreram._cap_5__metodologia_de_la_investigacion....pdf
- Belcic, I., & Nelson, B. (2020, septiembre 4). *¿Qué es la web oscura y cómo se accede a ella?* | Avast. <https://www.avast.com/es-es/c-dark-web>
- Benavides Monterrosa, L. A. (2010). *El debido proceso en la jurisprudencia constitucional*.
<https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/4/2010-2019/2010/11/89BD8.PDF>
- Cabezas Esteban, P. (2010). *TESIS DOCTORAL “LA INVESTIGACION DEL CRIMEN A TRAVÉS DE LOS TIEMPOS”* [UNIVERSIDAD AUTONOMA DE BARCELONA].
<https://www.educacion.gob.es/teseo/imprimirFicheroTesis.do?idFichero=FIHxYNhGkts%3D>
- Cardona Pérez, J. D. (2021). *La Valoración de la Prueba o Evidencia Digital en loss Procesos Judiciales*. Grupo Editorial Ibañez.
<https://latam.tirantonline.com/cloudLibrary/ebook/show/9789587913330>
- Cardoso Pereira, F. (2012). *AGENTE ENCUBIERTO Y PROCESO PENAL GARANTISTA: LÍMITES Y DESAFÍOS* [UNIVERSIDAD DE SALAMANCA].
https://gedos.usal.es/bitstream/handle/10366/121134/DDAFP_CardosoFlavio_Tesis.pdf?sequence=1&isAllowed=y
- Caro Coria, D. C. (2007). *Las garantías constitucionales del proceso penal*.
<https://www.corteidh.or.cr/tablas/r08047-30.pdf>
- Centro de Documentación Judicial. (s/f). Recuperado el 8 de junio de 2022, a partir de <https://www.jurisprudencia.gob.sv/busqueda/showExtractos.php?bd=1¬a=592278&doc=567560&&singlePage=false>
- COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS. (2017). *Estándares para una Internet Libre, Abierta e Incluyente Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos Edison Lanza Relator Especial para la Libertad de Expresión*.
http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf
- BOE.es - BOE-A-1999-846 Ley Orgánica 5/1999, de 13 de enero, de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves., (1999) (testimony of Congreso Español).
<https://www.boe.es/eli/es/lo/1999/01/13/5>
- BOE.es - BOE-A-2015-10725 Ley Orgánica 13/2015, (2015) (testimony of Congreso Español). https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725
- Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia*.
https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- Consejo de Europa. (2021). *Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: Beneficios El Convenio de Budapest sobre la Ciberdelincuencia*.

- <https://rm.coe.int/cyber-buda-benefits-junio2021a-es/1680a2e4de#:~:text=En%20junio%202021%2C%2066%20Estados,Tonga%2C%20otros%20%20Page%202>
- Consejo Nacional de la Judicatura. (2018). *CÓDIGO PROCESAL PENAL COMENTADO*. <https://escuela.fgr.gob.sv/wp-content/uploads/leyes-nuevas/codigo-procesal-penal-comentado-CNJ-v1.pdf>
- CORNEJO A., J. S. (2020). *XV. EVOLUCIÓN HISTÓRICA DEL DERECHO PENAL – INDICIUM*. <https://indiciumnace.wordpress.com/2015/11/08/xv-evolucion-historica-del-derecho-penal/>
- Corte Interamericana de Derechos Humanos. (2015). *Caso Ruano Torres y otros vs. El Salvador*. https://www.corteidh.or.cr/docs/casos/articulos/seriec_303_esp.pdf
- Corte Interamericana de Derechos Humanos. (2018). *Cuadernillo de jurisprudencia de la Corte Interamericana de Derechos Humanos No. 18 casos contenciosos sobre El Salvador*. <https://www.corteidh.or.cr/sitios/libros/todos/docs/cuadernillo18.pdf>
- Corte Suprema de Justicia. (s/f-a). *Lineas y criterios jurisprudenciales*. Recuperado el 9 de junio de 2022, a partir de <https://www.jurisprudencia.gob.sv/busqueda/showExtractos.php?bd=1¬a=678155&doc=672793&&singlePage=false>
- Corte Suprema de Justicia. (s/f-b). *VALORACIÓN INTEGRAL DE LA PRUEBA*. Recuperado el 8 de junio de 2022, a partir de <https://www.jurisprudencia.gob.sv/DocumentosBoveda/E/1/2010-2019/2019/07/E86AB.HTML>
- Cortéz Domínguez, V., & Moreno Catena, V. (2019). *Derecho Procesal Penal 9ª Edición 2019*. Tirant lo Blanch. <https://latam.tirantonline.com/cloudLibrary/ebook/show/9788413362632?showPage=274&search=agente+encubierto+informático>
- de Silva Gutiérrez, G. (2021). *Derechos fundamentales y derechos humanos*. <https://latam.tirantonline.com/cloudLibrary/ebook/show/9788413784656>
- Decreto Legislativo 280*. (2022). <https://imprentanacional.gob.sv/servicios/archivo-digital-del-diario-oficial/>
- Diario Oficial*. (2022, marzo 4). Tomo N° 434.
- Dino Carlos, C. C. (2007). *Las garantías constitucionales del proceso penal*. <https://www.corteidh.or.cr/tablas/r08047-30.pdf>
- Esparza Leibar, I., Gómez Colomer, J. L., Barona Vilar, S., Montero Aroca, J., & Etxeberria Guridi, J. F. (2019). *Derecho Jurisdiccional III Proceso Penal 27ª Edición 2019*. Tirant lo Blanch. <https://latam.tirantonline.com/cloudLibrary/ebook/show/9788413139265?showPage=193&search=agente+encubierto+informático>
- Espinosa de los Monteros, R. Z. (2009). *Las Reglas de Exclusión Probatoria al Hilo del Desarrollo de la Infiltración Policial*. 80–83. https://www.google.com/search?q=exclusion+medios+de+prueba+del+agente+digital+encubierto&rlz=1C1PRUG_enSV974SV974&oq=exclusion+medios+de+prueba+del+agente+digital+encubierto&aqs=chrome..69i57.12001j0j7&sourceid=chrome&ie=UTF-8

- Ferrajoli, L. (2006). *Garantismo penal*.
<https://www.derechopenalened.com/libros/garantismo-penal-luigi-ferrajoli.pdf>
- Ferrajoli, L. (2013). *Democracia y garantismo/ Luigi Ferrajoli ; edición de Miguel Carbonell*. Trotta. <https://elibro.net/es/ereader/bibliotecaugb/61306>
- Fiscalía General de la República de El Salvador. (2018). *Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexos* Fiscalía General de la República de El Salvador Escuela de Capacitación Fiscal Oficina de las Naciones Unidas contra la Droga y el Delito para Centroamérica y el Caribe (UNODC ROPAN) Equipo del Programa Global de Ciberdelito. <https://escuela.fgr.gob.sv/wp-content/uploads/leyes-nuevas/analisis-juridico-de-la-ley-especial-contra-los-delitos-informaticos-y-conexos-COMPLETO-CAP-I-II-III-V.pdf>
- Flores Salgado, L. Ludmina. (2015). *Derecho informático*. 223.
<https://elibro.net/es/ereader/bibliotecaugb/39404?page=149>.
- Fundación de Estudios para la Aplicación del Derecho. (2003). *Seguimiento de la Reforma Procesal Penal en El Salvador*.
<https://biblioteca.cejamericas.org/bitstream/handle/2015/5329/ceja-seg-slv2.pdf?sequence=1&isAllowed=y>
- García Molina, P., Fuentes Soriano, O., Pérez Simón, M., & Picó I Junoy, J. (2017). *El Proceso Penal. Cuestiones Fundamentales*. Tirant lo Blanch.
<https://latam.tirantonline.com/cloudLibrary/ebook/show/9788491196297?showPage=355&search=agente+encubierto+informático>
- Harbottle Quirós, F. (2021). *EL AGENTE ENCUBIERTO INFORMÁTICO: REFLEXIONES A PARTIR DE LA EXPERIENCIA ESPAÑOLA*. 131, 123–140.
<https://pjenlinea3.poder-judicial.go.cr/biblioteca/uploads/Archivos/Articulo/EL%20AGENTE%20ENCUBIERTO%20INFORMATICO%20HARBOTTLE.pdf>
- La Investigación del Delito en el Derecho Penal Español - Piva Torres, Gianni Egidio, Ruiz Carrero, Wilmer de Jesús, Lattuf Rodríguez, Williams de Jesús - Google Libros*. (2021).
https://books.google.com.sv/books?id=83o6EAAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- Lafont Nicuesa, L. (2022). *El agente policial encubierto*. Tirant lo Blanch.
<https://latam.tirantonline.com/cloudLibrary/ebook/show/9788413788234>
- Lluch, X. Abel. (2012). *Derecho probatorio*. 1227.
- López - Muñoz, J. (2019). *Criminalidad organizada y terrorismo. Formas criminales paradigmáticas*. Dykinson.
<https://latam.tirantonline.com/cloudLibrary/ebook/show/9788413240718?showPage=171&search=agente+encubierto+informático>
- María de las Nieves Jiménez López, García Molina, P., González Castell, A. C., Pérez Martell, R., Sánchez Barrios, M. I., & Sáez González, J. (2017). *Cuestiones Actuales de Derecho Procesal*. Tirant lo Blanch.
<https://latam.tirantonline.com/cloudLibrary/ebook/show/9788491436928?showPage=590&search=agente+encubierto+informático>

- Robledo Gutiérrez, J. (2013). *EL DERECHO DE DEFENSA PENAL COMO DERECHO FUNDAMENTAL*. https://escuelajudicialpj.poder-judicial.go.cr/Archivos/bibliotecaVirtual/penal/6_El derecho de defensa como Derecho Fundamental_2013.pdf
- Romero, M. L. (2018). *UN PASEO POR LA DEEP WEB*. <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72626/7/mlaboromTFM0118 memoria.pdf>
- Sala de lo Constitucional. (2007). *Sentencia de Amparo 168-2006*. <https://www.jurisprudencia.gob.sv/busqueda/showFile.php?bd=1&data=Documentos Boveda%2FD%2F1%2F2000-2009%2F2007%2F03%2F2C2C.PDF&number=11308&fecha=16/03/2007&numero=168-2006&cesta=0&singlePage=false%27>
- Sala de lo Constitucional. (2009). *Sentencia de Amparo 425-2004*. <https://www.jurisprudencia.gob.sv/busqueda/showFile.php?bd=1&data=Documentos Boveda%2FD%2F1%2F2000-2009%2F2009%2F12%2F37A6.PDF&number=14246&fecha=14/12/2009&numero=425-2004&cesta=0&singlePage=false%27>
- Sala de lo Constitucional. (2010). *Sentencia Hábeas Corpus 85 - 2008*. <https://www.jurisprudencia.gob.sv/busqueda/showFile.php?bd=1&data=Documentos Boveda%2FD%2F1%2F2010-2019%2F2010%2F03%2F38E5.PDF&number=14565&fecha=04/03/2010&numero=85-2008&cesta=0&singlePage=false%27>
- Sala de lo Constitucional de la Corte Suprema de Justicia. (1999). *Inconstitucionalidad 4 - 99*. <https://latam.tirantonline.com/latam/login.do>
- Sala de lo Constitucional de la Corte Suprema de Justicia. (2001a). 8-97Ac. <https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2000-2009/2001/03/1319.PDF>
- Sala de lo Constitucional de la Corte Suprema de Justicia. (2001b). *Amparo 714 - 99*. <https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2000-2009/2001/11/1625.PDF>
- Sala de lo Constitucional de la Corte Suprema de Justicia. (2008). *Hábeas Corpus 135-2005/32-2007 acumulado*. <https://www.jurisprudencia.gob.sv/busqueda/showFile.php?bd=1&data=Documentos Boveda%2FD%2F1%2F2000-2009%2F2008%2F05%2F30F7.PDF&number=12535&fecha=16/05/2008&numero=135-2005AC&cesta=0&singlePage=false%27>
- Sentencia Casación Ref. 92-CAS-2006, (2006). <https://www.jurisprudencia.gob.sv/busqueda/showFile.php?bd=1&data=Documentos Boveda%2FD%2F1%2F2000-2009%2F2007%2F12%2F6C79.PDF&number=27769&fecha=17/12/2007&numero=92-CAS-2006&cesta=0&singlePage=false%27>
- Sala de lo Penal. (2015). *Sentencia Casación Penal Referencia 67C2014*. <https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2010-2019/2015/01/AF8A4.PDF>

- Sala de lo Penal. (2018). *Sentencia Casación 44 C 2017*.
<https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2010-2019/2018/02/CC705.PDF>
- 7CAS2018., (el 8 de mayo de 2019).
<https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2010-2019/2019/05/D9815.PDF>
- Sentencia Casación 9-CAS-2016*, (2016) (testimony of Sala de lo Penal El Salvador).
<https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2010-2019/2016/10/BE247.PDF>
- Sanchis Crespo, C., & Velasco Núñez, E. (2019). *Delincuencia Informática*. Tirant lo Blanch. <https://latam.tirantonline.com/cloudLibrary/ebook/show/9788413133577>
- Sandoval Rosales, R. I. (2018). *CODIGO PROCESAL PENA COMENTADO: Vol. volumen II* (primera edicion). <https://escuela.fgr.gob.sv/wp-content/uploads/leyes-nuevas/codigo-procesal-penal-comentado-v2.pdf>
- Saniz Balderrama, R. (2001). *Computación Cuántica*.
http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1683-07892001000200006
- techopedia. (2022a). *¿Qué es una red privada?* . <https://es.theastrologypage.com/private-network>
- techopedia. (2022b). *¿Qué es una red pública?* . <https://es.theastrologypage.com/public-network>
- Téllez Valdéz, J. (2009). *Derecho Informático*. McGraw-Hill. <http://up-rid2.up.ac.pa:8080/xmlui/bitstream/handle/123456789/1384/Derecho%20inform%c3%a1tico-Tellez.pdf?sequence=1&isAllowed=y>
- UNESCO. (2013). *Universalidad de Internet: un medio para crear sociedades del conocimiento y la agenda de desarrollo sostenible después de 2015*.
<http://tech.qq.com/a/20120426/000023.htm>
- Velarde Callirgos, R. (2017). *Manual de Evidencia Digital* (primera). Publimagen ABC sac.
https://www.mpfm.gob.pe/Docs/0/files/manual_evidencia_digital.pdf
- Velasco San Martín, C. (2012). *La Jurisdicción y Competencia Sobre Delitos Cometidos a Través de Sistemas de Cómputo e Internet*.
<https://latam.tirantonline.com/cloudLibrary/ebook/show/9788490330128>
- Velasco San Martín, C. V. A. (2021). *Aspectos Practicos de los cibercrimes y la Evidencia Digital* (TIRANT LO BLANCH, Ed.).
- Villavicencio Macías, J. C. (s/f). *Las Garantías Judiciales en Sistema Interamericano de Derechos Humanos*. Recuperado el 22 de julio de 2022, a partir de <http://appweb.cndh.org.mx/biblioteca/archivos/pdfs/fas-csidh-garantias-judiciales.pdf>

Anexos.

UNIVERSIDAD GERARDO BARRIOS.

Alcances de la Figura del Agente encubierto digital y sus implicaciones en la investigación de los delitos informáticos frente al derecho de defensa del imputado.

Datos del agente a observar.

Nombre y apellidos: _____

Institución: _____

Dependencia: _____

Cargo: _____

Objetivo: observar los gestos, actitudes y comportamiento de los agentes entrevistados.

ITEM	SI	NO	OBSERVACIONES
Se expresa con claridad.			
Presenta familiaridad con el tema.			
Sus respuestas tienen congruencia con la normativa legal.			
Presenta dominio del tema sobre el que se está entrevistando.			
Muestra seguridad al expresar sus respuestas durante la entrevista.			

GUIA DE ENTREVISTA A OPERADORES DEL SISTEMA JUDICIAL

- 1- ¿Cuáles es su Opinión de la figura del agente encubierto digital y que no es autorizado por un juez?
- 2- ¿Cuál es el parámetro de validación de la evidencia Digital en el proceso Penal?
- 3- ¿Cuáles es el criterio para valorar la evidencia Digital obtenida por el agente digital encubierto?
- 4- ¿Qué papel juega la defensa, una vez presentado el requerimiento fiscal en el proceso investigativo de los delitos informáticos, en los casos donde se autoriza un agente encubierto digital?
- 5- Considera usted, ¿que podría existir una violación al Derecho de defensa el retraso del conocimiento de las diligencias investigativas en los casos de delitos informáticos, donde se autoriza el agente encubierto digital?
- 6- ¿Considera usted que podría ocurrir una nulidad, en un proceso por el hecho que no es dirigido funcionalmente por un fiscal?
- 7- ¿considera que el agente encubierto digital, violenta derechos fundamentales al justiciable por un delito informático?
- 8- ¿Considera usted que el agente encubierto digital, es un gran apoyo para la investigación de los delitos informáticos?



UNIVERSIDAD GERARDO BARRIOS.

Alcances de la Figura del agente encubierto digital y sus implicaciones en la investigación de los delitos informáticos frente al derecho de defensa del imputado.

Guía de Entrevista.

1. ¿Cómo opera la técnica del agente encubierto digital, en el proceso penal en El Salvador?
2. ¿Cuáles son los parámetros o razones que fundamentan las aplicaciones de la técnica del agente encubierto digital, para los casos penales?
3. ¿Con base a qué criterios se aplica la técnica del agente encubierto digital, en la investigación de los delitos informáticos?
4. ¿Cuál es el procedimiento para la asignación y acreditación del agente encubierto digital en una investigación?
5. ¿Cuáles son los requisitos legales que debe de tener la persona, para poder ser acreditada como agente encubierto digital?
6. ¿Cuáles son las funciones operativas que el agente encubierto digital puede o debe realizar, durante la investigación? ¿Tiene límites o no?

7. ¿En cuanto a la información obtenida por el agente encubierto digital durante la investigación, cual es el procesamiento que se le da a esta para su incorporación al proceso judicial?

8. Existe o podría existir algún tipo de responsabilidad penal para el agente encubierto digital, debido a las actuaciones de este durante la investigación; ello frente a los derechos y garantías específicamente al derecho de defensa que le asiste a la persona imputada.