**UNIVERSIDAD DE EL SALVADOR**

**FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE**

**DEPARTAMENTO DE CIENCIAS JURÍDICAS**

**TRABAJO DE GRADO**

# LA NECESIDAD DEL ESTADO DE REGULAR ESPACIOS CIBERNÉTICOS FRENTE AL USO DE LAS REDES SOCIALES POR PARTE DE LOS NIÑOS, NIÑAS Y ADOLESCENTES PARA EVITAR LA DEPREDACIÓN SEXUAL

**PARA OPTAR AL GRADO DE**

**LICENCIADO (A) EN CIENCIAS JURÍDICAS**


**PRESENTADO POR**

**MARVIN EDUARDO MARTÍNEZ LINARES**

**MYNOR LEONEL MARTÍNEZ PINEDA**

**NESTOR GEOVANY RAMÍREZ ZEPEDA**

**KARLA MARIA ALFARO RAMIREZ**

**DOCENTE ASESOR**

**LICENCIADO CARLOS ROBERTO TOMASINO MORÁN**


**ABRIL, 2020**

**SANTA ANA, EL SALVADOR, CENTROAMERICA**

**UNIVERSIDAD DE EL SALVADOR**

**AUTORIDADES**

**M. Sc. ROGER ARMANDO ARIAS ALVARADO**
**RECTOR**

**DR. RAÚL ERNESTO AZCÚNAGA LÓPEZ**
**VICERRECTOR ACADÉMICO**

**ING. JUAN ROSA QUINTANILLA QUINTANILLA**
**VICERRECTOR ADMINISTRATIVO**

**ING. FRANCISCO ANTONIO ALARCÓN SANDOVAL**
**SECRETARIO GENERAL**

**LICDO. LUIS ANTONIO MEJÍA LIPE**
**DEFENSOR DE LOS DERECHOS UNIVERSITARIOS**

**LICDO. RAFAÉL HUMBERTO PEÑA MARÍN**
**FISCAL GENERAL**

**FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE**

**AUTORIDADES**

**M.E.d. ROBERTO CARLOS SIGÜENZA CAMPOS**

**DECANO**

**M.E.d. RINA CLARIBEL BOLAÑOS DE ZOMETA**

**VICEDECANA**

**LICDO. JAIME ERNESTO SERMEÑO DE LA PEÑA**

**SECRETARIO**

**M.E.d. MIRNA ELIZABETH CHIGÜILA DE MACALL ZOMETA**

**JEFA INTERINA DE DEPARTAMENTO DE CIENCIAS JURÍDICAS**

## AGRADECIMIENTOS

### A DIOS TODOPODEROSO

Infinitas gracias por su fidelidad y misericordia; por darnos la oportunidad de llegar hasta esta fase llenarnos de sus bendiciones y poner a las personas correctas en nuestras vidas para culminar de forma satisfactoria nuestros proyectos.

### A MI MADRE:

Por ser una madre ejemplar, por enseñarme valores, por guiarme por el buen camino a lo largo de mi vida, por brindarme amor, comprensión, apoyo incondicional en el transcurso de todos mis estudios y estar presente en todo momento, por darme todo lo que he necesitado y educarme de la mejor manera que ha podido, por ser madre y padre a la vez, por hacer tantos sacrificios día tras día para ayudarme a ser quien soy, porque a pesar de los errores cometidos a lo largo del camino siempre ha brindado su mano y a enseñarme a ser un hombre íntegro.

### A MI PADRE:

Porque a pesar de la distancia nunca me ha dejado solo a lo largo del camino, por brindarme su apoyo a pesar de cada obstáculo, ayudarme a superarme y por brindarme amor, comprensión, apoyo incondicional en el transcurso de todos mis estudios y estar presente en todo momento, por darme todo lo que he necesitado y educarme de la mejor manera que ha podido

### A MI PADRASTRO:

Por ser un gran apoyo para mí y mi familia, por estar siempre cuando lo necesitamos, por brindarnos apoyo moral y económico, por demostrarnos cariño, admiración y respeto, por impulsarme a ser cada día una mejor persona, por ser mejor que un padre de sangre, por hacer feliz a mi madre y por lo tanto a mi hermana y a mí, le doy las gracias inmensamente.

**A MIS COMPAÑEROS DE TESIS**

A mis compañeros de tesis por su desempeño a lo largo de la realización de la investigación, por dedicación y empeño en las actividades que se llevaron a cabo en nuestro proyecto de graduación.

**A MI DOCENTE ASESOR**

Licenciado Carlos Roberto Tomasino Morán, por su tiempo y dedicación en su orientación de una manera profesional y ética por el cual se caracteriza y por sus valiosos aportes para nuestra investigación y para nuestras vidas laborales.

**A LA UNIVERSIDAD DE EL SALVADOR:**

Al alma mater por parir tantos profesionales de alta calidad, por todos los conocimientos compartidos por cada uno de los docentes que responsables de nuestra formación académica, en especial, al licenciado Miguel Ángel Dubón, por cada uno de sus consejos y brindarnos a cada uno de nosotros su amistad, cariño y respeto.

MARVIN EDUARDO MARTINEZ LINARES

## AGRADECIMIENTOS

### A DIOS TODOPODEROSO

Por su infinito amor que ha tenido hacia este servidor, porque me dio todas las oportunidades para superar los retos que vinieron y han de venir en la aventura de vivir en este mundo.

### A MI MADRE:

Porque estuvo siempre en todos los momentos importantes en mi vida, por su apoyo incondicional en los momentos de mayores dificultades, por su estricta enseñanza, que he de decir, ha dado frutos por haber llegado a esta etapa de mis estudios, y que aun en todo lo que me resta por vivir me seguirá guiando.

### A MI PADRASTRO:

Por ser un gran apoyo para mí y mi familia, por brindarnos apoyo moral y económico, y que desde que tengo memoria, ha contribuido en mi formación como persona.

### A MI FAMILIA:

En especial a mi abuela Victoria, quien a través de su dulzura añeja ha brindado su apoyo moral para poder superarme; asimismo agradezco a mi novia Alejandra, por ser alguien importante en mi vida, por ayudarme a ser mejor persona todos los días, por su apoyo incondicional y su inmensa ternura.

### A MIS COMPAÑEROS DE TESIS

Que a pesar de todas las dificultades que vivimos durante el transcurso de este trabajo y que a su vez las pudimos solventar, fue un gusto haber trabajado junto con ellos, deseándoles un futuro profesional exitoso.

### A MI DOCENTE ASESOR

Licenciado Carlos Roberto Tomasino Morán, que más que un asesor del montón, fue amigo e instructor de nuestra formación profesional durante algunos años de la carrera, por su

dedicación a la enseñanza y su esmero en que nosotros nos realizáramos como buenos profesionales del Derecho.

**A LA UNIVERSIDAD DE EL SALVADOR:**

Al alma mater, quien contribuye a la formación de excelentes profesionales que contribuyen al mejoramiento de la sociedad salvadoreña.

MYNOR LEONEL MARTINEZ PINEDA

## AGRADECIMIENTOS

### A DIOS TODOPODEROSO

Por darme la oportunidad de vivir, asimismo compartir la existencia de personas fantásticas que me ayudan a ser mejor persona y ciudadano.

### A MIS PADRES Y FAMILIARES

Mi eterno agradecimiento de tener la oportunidad de convivir con las personas más importantes en mi vida, de estar cada día orgulloso de ser su hijo por el enorme esfuerzo que hicieron para sacar adelante a mi familia proporcionándonos estudio, guía y experiencias de vida, porque vivir con ellos es poder afirmar que mi casa es un hogar feliz.

### A MIS COMPAÑEROS DE EQUIPO Y SUS FAMILIAS

Gracias a mis compañeros por dejarme formar parte de un equipo excepcional, con cualidades propias, diferentes, responsables, oportunas, eficientes y eficaces, personas con capacidades fantásticas; a sus familias por darnos la oportunidad de reunirnos en el seno de su hogar hasta altas horas de la noche y apoyarnos en todo momento para trabajar en este proyecto.

### AL ASESOR DE TESIS CARLOS ROBERTO TOMASINO MORAN

Por aceptar guiar a este equipo y aventurarse a asesorarnos sin aceptar nada a cambio, gracias por ser una persona diligente, puntual y responsable en todo aspecto, desde guiar la investigación, conceptos y herramientas necesarias y pertinentes.

### A LA UNIVERSIDAD DE EL SALVADOR

Por ser la mejor universidad del País, por ser mi alma máter, mi eterno agradecimiento por darme la oportunidad de recibir la formación académica necesaria para lograr mis objetivos, esperando algún día poder retribuirle tanto o más de lo que recibí.

NESTOR GEOVANY RAMIREZ ZEPEDA

## AGRADECIMIENTOS

### A DIOS TODOPODEROSO

Infinitas gracias por su fidelidad y misericordia; por brindarme la oportunidad más grande en mi vida de permitirme ser una profesional y por proveerme de todos los insumos necesarios y sabiduría para llegar hasta este punto y superar todos los obstáculos.

### A MI MAMI:

María Arely Ramírez Lima, por ser una madre ejemplar, por enseñarme valores, por guiarme por el buen camino a lo largo de mi vida, por brindarme amor, comprensión, apoyo incondicional en el transcurso de todos mis estudios y estar presente en todo momento, por darme todo lo que he necesitado y educarme de la mejor manera que ha podido, por ser madre y padre a la vez, por hacer tantos sacrificios día tras día para ayudarme a ser quien soy, por entenderme siempre a pesar de no ser una hija ideal, por ser la mejor mamá que pude tener, no la cambiaría por nada ni nadie.

### A MI PADRASTRO:

Mauricio Solís por ser un gran apoyo para mí y mi familia, por estar siempre cuando lo necesitamos, por brindarnos apoyo moral y económico, por demostrarnos cariño, admiración y respeto, por impulsarme a ser cada día una mejor persona, por ser mejor que un padre de sangre, por hacer feliz a mi mami y por lo tanto a mi hermano a mí, le doy las gracias inmensamente.

### A MI HERMANO:

A mi hermano y a la vez mejor amigo José Armando, por ser parte importante en mi vida, por brindarme su apoyo en todo momento, por compartir diferentes experiencias y momentos en familia, por ser compañero de aventuras y secretos, por escucharme, aconsejarme y no juzgarme y por quererme tanto.

### A MIS AMIGOS:

A mis amigas y amigos: Yenifer, Johana, Yasmín, Enyi, Héctor, Dominick, Emerson, Roxana, Efraín, por darme ánimos en este proceso, por estar en los buenos y malos momentos, por compartir juntos experiencias para distraerme del estrés acumulado, infinitas gracias por su atención, comprensión, lealtad y amistad.

**A MIS COMPAÑEROS DE TESIS**

A mis compañeros de tesis por emprender este desafío con mi persona y con visión de llegar a la meta deseada, por hacernos ver los unos con los otros cuando algo está mal, aceptar nuestros errores y corregirlos, por entendernos y llevarnos bien, por culminar este trayecto que, aunque no ha sido fácil; hemos aprendido y nos hemos divertido y seguimos siendo amigos.

**A MI DOCENTE ASESOR**

Licenciado Carlos Roberto Tomasino Morán, por su tiempo y dedicación en su orientación de una manera profesional y ética por el cual se caracteriza y por sus valiosos aportes para nuestra investigación y para nuestras vidas laborales.

**AL LICENCIADO MIGUEL ÁNGEL DUBÓN (Q.D.D.G.):**

Por haber sido en vida un gran amigo, aparte de ser el mejor docente que pude tener, por compartir con nosotros tantas experiencias en el área laboral; la cual era su rama, por contarnos anécdotas y chistes que hacía que las clases fueran más entretenidas, por habernos brindado tanto conocimiento y demostrarnos su cariño, siempre lo llevaré en mi memoria, infinitas gracias hasta el cielo.

**A MI PROFESOR DE SOCIALES EN BACHILLERATO:**

Roberto Aníbal Díaz (Profe Tito) por siempre haber confiado en mí y ver mi potencial, por darme palabras que me impulsaban a seguir siempre hacia adelante y desde entonces ver en mí una profesional.

KARLA MARIA ALFARO RAMIREZ

# INDICE

# INTRODUCCIÓN

Presentamos el trabajo de graduación de la investigación denominada "La necesidad del Estado salvadoreño de regular espacios cibernéticos frente al uso de las redes sociales por parte de los niños, niñas y adolescentes para evitar la depredación sexual", en el cual se aplicó el Método cualitativo tal como lo establece el Departamento de Ciencias Jurídicas de la Universidad de El Salvador, Facultad Multidisciplinaria de Occidente.

En la cual planteamos la problemática existente de que el Estado debe de crear, fortalecer, actualizar o adoptar las herramientas Jurídicas necesarias para la investigación, prevención y/o reprensión de los Delitos Informáticos que afectan a los Niños, Niñas y Adolescentes, todo esto sin afectar los Derechos Constitucionales o en dado caso los Derechos Fundamentales reconocidos por las Legislaciones Internacionales a las cuales el Estado salvadoreño está adscrito.

Asimismo se han abordado una serie de temáticas desarrolladas en el Marco Teórico el cual creemos que el lector debe de conocer para una compresión más precisa de los elementos que interrelacionan en la sociedad cuya relevante importancia modifica el actuar de las entidades privadas así como la soberanía de los Estados; se recopilan los más importantes conceptos jurídicos, doctrinarios y tecnológicos los primeros dentro de su respectivo Marco y los segundos dentro de las temáticas antes enunciadas.

En los cuales se estudió y analizó el ordenamiento jurídico del Estado salvadoreño, en específico la Constitución de la República en artículos específicos y las Leyes secundarias que están relacionadas con la Protección de los Niños, Niñas y Adolescentes, la represión e investigación de los Delitos Informáticos y las Leyes de orden administrativo que regulan el ciberespacio.

Seguidamente se aborda el Marco Metodológico, en el cual se delimita como se procedió a desarrollar la investigación desde el tipo y diseño de investigación, hasta el vaciado de información obtenida en las entrevistas a importantes representantes de Instituciones encargadas de la investigación de delitos informáticos, la imposición o

absolución de penas a incoados y destacados académicos cuyo, valioso aporte representó la culminación satisfactoria a la presente investigación.

Y habiendo realizado todo lo anterior llegamos a interesantes conclusiones relacionadas a la realidad del Estado salvadoreño afectada por la problemática enunciada al inicio de esta introducción, asimismo, nuestro aporte fue el enumerar distintas recomendaciones, que, como grupo consideramos que pueden apalear los déficits provocados por la problemática referida.

# CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

## 1.1 PLANTEAMIENTO DEL PROBLEMA

En las sociedades actuales se viven los efectos del desarrollo tecnológico que durante años ha evolucionado la forma de vida del elemento humano, bajo esa perspectiva se tiene que la revolución tecnológica beneficia a los sectores como la banca, el transporte, la educación, el tráfico aéreo y terrestre; pero así mismo ha incidido al ámbito jurídico, social y cultural.

La revolución informática ha originado que no exista área que no se encuentre influido por el fenómeno cibernético de la era digital, ante dicha situación, varios países han tomado las previsiones jurídicas que impone el caso; En virtud de ello se ha desarrollado lo que en la actualidad se conoce como derecho informático.

Evidentemente las Tecnologías de Información y de Comunicación son el sector más influyente en la vida cotidiana de las personas, es decir; la mayoría de usuarios tienen acceso a una gama indescriptible de material multimedia y audiovisual al alcance de un "clic".

En tal contexto, las Tecnologías de Información y de Comunicación se definen como: "Un término que contempla toda forma de tecnología usada para crear, almacenar, intercambiar información en su forma tales como datos, conversaciones de voz, imágenes fijas y video entre otros".

En particular las Tecnologías de Información y Comunicación están íntimamente relacionadas con los medios informáticos y los telemáticos, ya que los medios de comunicación a distancia nacen de la evolución de la telecomunicación y la informática para cubrir un espacio geográfico, científico y tecnológico beneficiando así el ámbito económico de una manera global, debido a una forma eficiente de prestación de servicios y basándose en tres características fundamentales:

a) La inmediatez de las comunicaciones a distancia;
b) La posibilidad de la realización de acciones masivas automatizadas; y,

c) La posibilidad de realizar acciones con un determinado nivel de anonimato.

En virtud de lo anterior se pueden considerar como las Tecnologías de Información y Comunicación tanto el uso de Internet, los aparatos electrónicos de intercambio de información como tecnologías de telefonía celular y digital, transmisiones de datos por medio de ondas radiales y los aparatos electrónicos necesarios para la transmisión de la información, entre otros.

Según los datos de la página web "marketingfourecomerce" en 2,019 se cuenta con promedio global de usuarios de 4,388 millones, lo cual significa un aumento del 9.1% de usuarios respecto del año 2,018 y en razón de ello, los estados implementan políticas educativas encaminadas al correcto uso de las Tecnologías de la Información y la Comunicación enfocadas en su mayoría en los niños, niñas y adolescentes, quienes a su vez poseen un fácil acceso a estas tecnologías y consecuentemente al ciberespacio.

El ciberespacio posee una variedad de contenido educativo, informático y de entretenimiento, así mismo existe la posibilidad al acceso a contenido explicito que puede resultar nocivo y perturbador a la psiquis de los niños, niñas y adolescentes, debido a que no poseen una madurez emocional para afrontar este tipo de información, ante lo cual es necesario que para regular el acceso ciberespacio exista un instrumento legal que obligue al proveedor a censurar el acceso al contenido explicito por parte de los niños, niñas y adolescentes.

Debe entenderse que la censura comprende a los diversos procedimientos implementados por los Estados u otros grupos no estatales con la finalidad de controlar o suprimir determinados contenidos en internet. En relación a lo anterior es necesario determinar los límites y el alcance que la censura implica en el ciberespacio.

Con relación a los alcances de la censura dentro de internet, nace una problemática, debido a que lo anterior puede significar una privación de derechos humanos, tal como lo establece la Organización de las Naciones Unidas (En adelante ONU) en la resolución A/HRC/32/L.20, en la que declara que el Derecho al Acceso a Internet es un Derecho

Humano básico y, aunque dicha resolución no posee un carácter vinculante en países como Rusia, China y Arabia Saudí; manda un fuerte mensaje a los Estados parte para regular el acceso al internet dentro de cada una de sus jurisdicciones.

La censura en los Estados obedece generalmente al desarrollo de la agenda política del gobierno en turno, lo cual puede resultar en una afectación a los derechos de los ciudadanos, lo cual es contrario al Estado de Derecho. Las consecuencias de las prácticas implementadas a partir de la censura estatal es la vulneración al Derecho la Libertad De Prensa, Libertad De Expresión Y La Libre Asociación En Línea en nombre del interés público, de la seguridad nacional, creación de políticas dirigidas al combate del cibercrimen o en defensa de intereses políticos, comerciales o de otra índole.

En El Salvador se han aprobado diversas normativas, tal es el caso de la "Ley Especial Contra Los Delitos Informáticos y Conexos"; no obstante, dicha normativa posee deficiencias, ante lo cual precisa la creación de instrumentos legales que obligue a los proveedores de los servicios de telecomunicación a establecer parámetros efectivos para el acceso a determinados contenidos dentro del ciberespacio, con la finalidad de limitar el acceso a material de contenido explícito a los niños, niñas y adolescentes

## 1.2 ENUNCIADO DEL PROBLEMA

**¿Cuáles son las principales deficiencias, obstáculos y debilidades que enfrenta el Estado salvadoreño para hacer efectiva la regulación de los espacios cibernéticos en cuanto a la adopción de medidas que limiten el acceso de los niños, niñas y adolescentes a material explicito dentro del ciberespacio, por parte de los proveedores de servicios de telecomunicaciones en lo relativo al uso de herramientas de acceso al internet o medios de comunicación conexos?**

## 1.3 JUSTIFICACION

En la actualidad, el acceso a las Tecnologías de la comunicación y de la información está al alcance de la mayor parte de la población en El Salvador, para el año dos mil dieciséis, se estima que en El Salvador existían 9.6 millones de celulares; esto representa que cada habitante indistintamente de su edad portaba un teléfono celular, y en

algunos casos portan hasta dos; por lo que es innegable decir que las nuevas tecnologías de la información y de la comunicación han incidido tanto en la vida del salvadoreño promedio a diferencia de años anteriores.

Uno de los efectos de la era digital por la que atraviesa El Salvador, es la facilidad con la que la información que circula dentro del ciberespacio, se esparce masivamente entre los usuarios de las diferentes webs; cabe destacar que no todos los datos almacenados virtualmente poseen un carácter para todo público, muchos de ellos guardan contenido explícito que puede ser nocivo para la salud mental para un sector de la población, en específico el de los niños, niñas y adolescentes.

Además, es fácil advertir el acceso que tienen los niños, niñas y adolescentes a las Tecnologías de la Información y de la Comunicación, convirtiéndolos en potenciales víctimas de depredadores sexuales, los cuales se aprovechan de sus condiciones de superioridad de desarrollo psíquico y físico respecto de los menores de edad, los cuales como se menciona en el párrafo que antecede la evolución de la comunicación y el acceso a las tecnologías de la Información ha aumentado notoriamente, en paralelo a ello aumenta y generan nuevas formas de cometer delitos, tal como el ciber acoso, o como ha sido denominado en el ámbito sociológico como “Grooming”.

Es necesario que exista control de la información que circula en los portales web, con el fin de que dicho contenido no sea utilizado para vulnerar o perturbar la psiquis de aquellos individuos que no cuentan con una madurez emocional completamente desarrollada; y una de las formas de ejercer el control en los medios de información y de comunicación, a través de las políticas de censura implementadas por el Estado salvadoreño.

Surge la necesidad de los Estados de crear normativas, tanto internas como externas, con la finalidad de prevenir y reprimir los delitos informáticos, en virtud de que son los Estados los encargados de la tutela de los Bienes Jurídicos de la población en general con un énfasis especial respecto de los Niños, Niñas y Adolescentes; así como también de los incapaces por ser éstos un sector vulnerable de convertirse en víctimas de los depredadores sexuales, en su mayoría a través de redes sociales.

La relevancia de esta investigación se manifiesta a partir de la controversia generada por el control del contenido multimedia dentro de internet; por un lado, el acceso por parte de los individuos que no son aptos para el consumo de material de contenido explicito dentro del ciberespacio; por otro lado, que las medidas aplicadas no afecten el goce del derecho al Libre Acceso a Internet por parte de los ciudadanos en pleno goce y ejercicio de sus derechos y libertades.

Por otro lado, en el ciberespacio como un acceso público libre no está exento de ser utilizado como medio o finalidad de la comisión de delito; tal es el caso de la Depredación Sexual en menores de edad, la conducta de las personas que los cometen se basan en la supremacía de condiciones en el orden cognitivo y cognoscitivo de la psiquis ya que los depredadores sexuales identifican e individualizan a las potenciales víctimas creándoles una esfera de confianza, empatía y de seguridad pero al mismo tiempo le generan la oportunidad de que los niños, niñas y adolescentes cedan a los más bajos instintos de los depredadores sexuales.

Con base a todo lo anterior, durante el transcurso de la presente investigación, se pretende la recomendación de propuestas dirigidas a la creación de mecanismos, que se encarguen de la regulación del ciberespacio, respecto del acceso a determinados materiales dentro del ciberespacio de los niños, niñas y adolescentes con la finalidad de proteger la moralidad y buenas costumbres de los mismos.

## 1.4 OBJETIVOS

### OBJETIVO GENERAL

Estudiar la necesidad dentro del Estado Salvadoreño de controlar o regular el acceso a las Tecnologías de la Información y Comunicación por parte de los niños, niñas y adolescentes.

**OBJETIVOS ESPECÍFICOS**

a) Enlistar las medidas de control del Estado salvadoreño aplicables al acceso a material explícito por parte de los niños, niñas y adolescentes a través de las Tecnologías de Información y Comunicación.

b) Indagar, los riesgos a los que se exponen los niños, niñas y adolescentes al hacer uso de las Tecnologías de Información y Comunicación en El Salvador.

c) Establecer los límites legales de las medidas de control aplicables al acceso al internet por parte de los niños, niñas y adolescentes en el país.

## 1.5 PREGUNTAS DE INVESTIGACIÓN

a) ¿Cuáles son los instrumentos legales vigentes dentro del Ordenamiento Jurídico del Estado salvadoreño que contienen medidas de control para la censura o limitación al acceso al contenido explícito de los niños, niñas y adolescentes?

b) ¿Cuáles son los beneficios de la aplicación de las medidas de control al acceso de contenido explícito por medio del uso de las TIC?

c) ¿Cuáles son las instituciones del Estado Salvadoreño que aplican las medidas de control y protección de los niños, niñas y adolescentes?

d) ¿Son eficaces dichas instituciones en la aplicación de las medidas de control y protección de los niños, niñas y adolescentes?

e) ¿Cómo afecta en el desarrollo psicológico de los niños, niñas y adolescentes el consumo de material explícito a través de medios tecnológicos?

f) ¿Vulnera los Derechos fundamentales de los adultos la censura del ciberespacio con la aplicación de los medios de control de protección de los niños, niñas y adolescentes?

## 1.6 CONSIDERACIONES ETICAS PARA ESTA INVESTIGACION.

Según el diccionario Filosófico Rossental: ética es una ciencia de la moral que de divide en ética normativa y teoría de la moral, la primera investiga el problema del bien y del mal, señala que aspiraciones son dignas y que conductas son buenas y cuál es el sentido de la vida; la teoría de la moral investiga la esencia de esta es buscar el origen, desarrollo y las leyes a que obedece su norma, su carácter histórico, por lo tanto las consideraciones éticas son aquellos principios que norman los pensamientos, acciones, conductas de los investigadores y de proceder ante tal investigación de manera profesional.

Por lo anterior, la presente investigación científica es de suma importancia hacer uso de la ética profesional como una herramienta del investigador, en donde exista el compromiso y respeto de lo que se investiga, como grupo investigador se tiene como objetivo el respeto a la dignidad de las personas, que formaran parte del presente trabajo.

En vista de lo anterior la información que será recopilada será tratada bajo el principio de confidencialidad, y se les dará crédito a todas aquellas aportaciones de cada uno de los partícipes de esta investigación, evadiendo situaciones en las cuales se pueda ocasionar prejuicios, desvalorizaciones y críticas, empleando los principios de probidad, imparcialidad, transparencia, confidencialidad y responsabilidad.

La investigación que se desarrollara será únicamente para uso de este trabajo, por ello existe el compromiso del grupo de investigación a actuar de manera responsable, respetando principios éticos que implica la búsqueda de la verdad por todos los medios lícitos, y dando el valor que corresponde a todos aquellos que serán parte fundamental para que este proceso de investigación sea veraz.

# CAPITULO II: MARCO TEORICO

# MARCO HISTORICO

## 1. SURGIMIENTO DEL CIBERESPACIO Y SU CONSECUENTE POPULARIZACION

En las últimas décadas, se han realizado una cantidad innumerable de estudios sociales y económicos e incluso jurídicos que se han enfocado en el análisis del desarrollo y aplicación de las llamadas "nuevas tecnologías de la información y la comunicación", de sus tendencias para el futuro y del cómo la interacción de la comunidad global con esta nueva área del conocimiento ha cambiado radicalmente la forma de hacer y pensar los negocios en todo el mundo.

Indudablemente, estas recientes modificaciones a las formas culturales en la comunicación e información no fueran posibles sin la existencia del ciberespacio y que éste simplemente no se limita únicamente al ámbito del mercado global; con cierta regularidad, se engloba dentro del sector de las telecomunicaciones y el fenómeno de las nuevas tecnologías, al ciberespacio, considerándolo una herramienta más dentro de las técnicas usadas en el tratamiento y la transmisión de las informaciones.

No obstante, al ciberespacio como tal, no se le puede equiparar con el impacto que causan la telefonía, el radio, el cine y la televisión ya que, a pesar de estar vinculados; el panorama que abre el ciberespacio es abismalmente amplio frente a aquellos ya que nos encontramos ante un verdadero "metaespacio", es decir, una realidad virtual muy extensa y que, aun siendo intangible, se puede comprobar su existencia.

Pero antes de explicar de lo que trata esta realidad virtual, en cuanto a sus componentes y características, es necesario realizar un bosquejo histórico que refleje las etapas por las cuales las interrelaciones personales y el avance tecnológico han evolucionada hasta el punto de crear ese fenómeno universal conocido como ciberespacio.

### 1.1 ETAPAS DE LA INTERCOMUNICACION EN LAS SOCIEDADES HUMANAS EN LA ANTIGÜEDAD

Primeramente, se debe tomar en cuenta que las relaciones interpersonales en la antigüedad se dieron en función de las necesidades humanas; cabe señalar que estas últimas

desempeñaron un rol esencial tanto en el origen como en el desarrollo mismo de todas las relaciones humanas. Todo lo que el ser humano hace se debe a alguna motivación, es decir, a aquel trasfondo psíquico, impulsor, que sostiene la fuerza de la acción y señala su dirección.

A su vez, las motivaciones nacen a partir de las necesidades o carencias del individuo, y estas van desde las básicas, las fisiológicas, hasta otras de tipo más complejas, como la pertenencia o la autorrealización e incluso a la supervivencia personal.

Varios historiadores concuerdan que la necesidad de las personas de relacionarse entre sí, se originan desde la prehistoria; momento en que la humanidad enfrentaba las inhóspitas condiciones de vida propias de la época, lo cual obligaba a estos individuos conformar comunidades (tribus), con el fin de conseguir el sustento y protección de sus semejantes.

Bajo ese modelo de convivencia, la humanidad vivió durante muchos años, no obstante, las relaciones interpersonales con el paso del tiempo sufrieron una evolución importante, lo anterior a consecuencia del nacimiento de la "escritura", lo que da paso al inicio de la Edad Antigua (4,000 a.C)

Entre los principales aportes a la evolución humana que dejo la Edad Antigua, se pueden mencionar los siguientes:

a) **La aparición de la escritura.** El nacimiento de la escritura marca el inicio de la Edad Antigua. Cada cultura desarrolla tipos de escritura particulares, como la egipcia, que representa objetos mediante símbolos, o la griega, que crea el primer alfabeto.

b) **La predominancia de las religiones politeístas.**

c) **Las clases sociales eran hereditarias.** La clase social no era flexible y se heredaba de padres a hijos. Generalmente, se hacía distinción entre monarquía, aristocracia, eruditos, artesanos y esclavos.

d) **Las primeras leyes.** Para facilitar la convivencia en las grandes poblaciones, se elaboraron leyes y, de esa forma, nacieron los primeros códigos que aplicaban penas a determinadas conductas; la exorbitante cantidad de individuos que llegaron a asentarse, ya en un lugar conocido como ciudad, generaba la necesidad de crear un mecanismo que regulara ciertas conductas dentro de la misma, con el fin de garantizar un orden y armonía entre los miembros de las polis

Se conoce que el fin de la Edad Antigua data del año 476 d.C, fecha en la que ocurrió la caída del Imperio Romano de Occidente, a manos de los bárbaros, encabezados por Odacro. Lo anterior da pie a un nuevo capítulo de la historia humana, conocido como la Edad Media; esta última finaliza con la caída del Imperio Romano de Oriente o Imperio Bizantino, cuando los Turcos Otomanos lograron apoderarse de Constantinopla, la capital del Imperio Bizantino o bien coincide con el descubrimiento de América en el año 1,492.

Entre los principales hechos aportados por la Edad Media, se pueden destacar los siguientes:

a) Desaparecieron los grandes imperios, para dar paso a otro tipo de organizaciones más pequeñas, denominados feudos.

b) Numerosas invasiones territoriales, guerras frecuentes y la amplia influencia de la Iglesia.

c) En el aspecto económico, se sustituye el modelo de producción esclavista al de producción feudal.

d) Desaparece la ciudadanía romana y la definición de los estamentos medievales.

e) En el ámbito político se produce la descomposición de las estructuras centralizadas romanas y dispersión del poder entre los pueblos bárbaros.

f) Evoluciona del pensamiento cultural lo que causa una sustitución de la cultura clásica por el teocentrismo cristiano o musulmán.

Por otra parte, la Edad Moderna empieza a desligarse del dominio de la iglesia y de los pensamientos teológicos predominantes de la Edad Media; asimismo se caracteriza por ser un periodo de grandes cambios en el terreno político, social, científico, literario, y

artístico. Respecto al pensamiento humano y la filosofía, predomina la corriente ideológica conocida como **humanismo, un pensamiento racionalista** que ya se había dado en los siglos posteriores, donde el hombre va a ser el centro de todas las cosas, exaltando por lo tanto el concepto del individualismo.

Sin embargo, han existido relevantes hechos precursores para el cambio sustancial que nuestra sociedad está viviendo. Es así que podríamos mencionar como un antecedente sumamente trascendental para nuestra época, a la invención de la imprenta, vista ésta como una nueva oportunidad de difusión de ideas a un número mayor de personas. En Occidente, sería en el año 1,440 cuando por fin se le atribuye la invención al Alemán **Johannes Gutenberg**, el llamado "Padre de la Imprenta" después de una gran controversia por disputarse la gloria de ese título entre alemanes, italianos, franceses y holandeses.

La imprenta fue en su momento, como ahora el ciberespacio una manera aún más revolucionaria, un mecanismo sin precedentes para el intercambio de ideas y reflexiones entre distintas regiones del entonces "mundo conocido", lo que indudablemente modificaba de manera sustancial la forma en la que el mundo debía de concebirse.

Otros acontecimientos importantes son las llamadas revoluciones, las cuales inician a finales de la Edad Moderna; una de la más importante marca el fin de la citada Edad, la cual es la Revolución Francesa, misma que estalla en el año 1789, dando inicio así a la Edad Contemporánea.

La Edad Contemporánea, es una fase caracterizada por el nacimiento de la industria, por los avances en las investigaciones científicas, por el perfeccionamiento de la tecnología y por la constante evolución de los medios de comunicación y de transportes.

Su inicio fue bastante marcado por la corriente filosófica iluminista o la ilustración como también es conocido este pensamiento que dio origen a la revolución francesa, que destacaba la importancia de la razón y está marcado de manera general.

Asimismo, se consolidó el régimen capitalista en el occidente, a consecuencia de las disputas de las grandes potencias europeas por territorios, materias primas y mercados los consumidores.

Entre las principales características de la precitada época, se pueden señalar las siguientes:

**a)** Consolidación del capitalismo como sistema económico;

**b)** Desarrollo industrial.

**c)** Ascensión política y económica de la burguesía industrial, principalmente en los países europeos.

**d)** Consolidación del régimen democrático tras mediados del siglo XIX.

**e)** Brigadas entre las grandes potencias europeas que luchaban por los mercados consumidores, fuentes de materias, y la conquista de territorios. La disputa dio origen a los movimientos conocidos como Imperialismo y Neocolonialismo;

**f)** Amplio desarrollo tecnológico, principalmente a partir de mediados del siglo XX.

**g)** A principios del siglo XX estuvo marcado por el avance de la Estados Unidos de América como la potencia mundial.

**h)** Globalización de la economía a partir de mediados del siglo XX.

**i)** El siglo XX también fue configurado por los importantes descubrimientos y avances tecnológicos.

En el campo científico, las innovaciones y transformaciones también fueron profundas. Las investigaciones en medicamentos y en prácticas médicas proporcionaron un aumento significativo de la expectativa y de la calidad de vida de las poblaciones. Los acontecimientos de esta época fueron marcados por transformaciones aceleradas en la economía, la sociedad y la tecnología que han merecido el nombre de Revolución industrial.

Como consecuencia directa de la Revolución Industrial, se encuentran las innovaciones a las relaciones interpersonales a partir del nacimiento de las

telecomunicaciones, cuyo origen data con la invención del **telégrafo** en 1,829, por parte de Joseph Henry. Sin embargo, la persona que le dio gran impulso fue el estadounidense Samuel Morse, quien inventó un código que lleva su nombre, el cual fue un gran paso a la hora de establecer comunicaciones entre personas a distancia. Mediante los telegramas, era el medio a través del cual las personas mantenían contacto los unos con los otros en la distancia.

El problema de los telegramas radicó en el hecho de la tardanza con la que la información llegaba a los demás individuos; evidentemente era necesario dar otro paso más allá para evolucionar el sistema de las telecomunicaciones. La creación del teléfono en 1,876 supuso un gran cambio. Pero fue en 1,920 cuando se estableció la primera llamada a larga distancia. Lo que supuso el inicio de una nueva era de las telecomunicaciones, permitiendo a las personas comunicarse al momento sin importar la distancia. Y que derivó en la automatización de las comunicaciones años después.

## 1.2 NACIMIENTO DEL CIBERESPACIO Y DEL INTERNET; PROBLEMÁTICAS DE SU REGULACION

El ciberespacio es el ámbito de información que se encuentra implementado dentro de los ordenadores y de las redes digitales de todo el mundo; es también un tema recurrente en la ciencia ficción, como tal, es virtual; inexistente desde el punto de vista físico donde las personas o sujetos, públicas o privadas, desarrollan comunicaciones a distancia, exponen sus competencias, generan interactividad para diversos propósitos.

El término ciberespacio tiene su origen en la palabra griega "cibernao"(pilotear una nave) fue popularizado por la novela “Neuromante” de William Gibson publicada en 1984, pero procede del relato del mismo autor Johnny “Mnemonic” (1981), incluido en el volumen Quemando Cromo (Burning Chrome, 1986).

La evolución de los procesadores digitales luego de pasar por el ámbito militar y los centros de investigación científica, hizo accesibles a los individuos de las empresas y los hogares las computadoras personales, dispositivos que al vincularse en red producen un

sistema interconectado a escala planetaria los cuales combinados generan el "nuevo mundo".

El ciberespacio, como inteligencia colectiva y virtual contiene todos los recursos de información y comunicación disponibles en la red, donde los sujetos interactúan entre sí, a través de las nuevas tecnologías; las barreras físicas desaparecen, tiempo y espacio toman una nueva dimensión, y un individuo puede comunicarse con otros individuos en diferentes lugares del planeta al mismo tiempo.

Cabe aclarar, que con cierta frecuencia se utilizan como sinónimos, el término de ciberespacio no debe confundirse con el Internet "real" (International Network of Computers), ya que el primero se refiere a menudo a los objetos e identidades que existen dentro de la misma red informática, así que podría decirse, metafóricamente, que una página web; se encuentra en el ciberespacio; pero no podríamos limitar al ciberespacio como un término equivalente, exclusivamente a Internet.

De tal forma que, en términos generales, cuando se menciona al ciberespacio, podríamos afirmar que se hace alusión al "ámbito artificial creado por medios informáticos" (definición proporcionada por la Real Academia Española). No obstante, una definición más acertada, es aquella acuñada al ilustre erudito alemán en política y medios de comunicación, Hans J. Kleinsteuber[1]:

"aquellas construcciones sociales que describen las condiciones para que puedan producirse intercambios entre las personas sin perjuicio de la distancia que las separa".

Es así que se asegura que "la red de redes" (Internet) es simplemente un medio de comunicación, a pesar de los múltiples aspectos que engloba en la vida cotidiana y la facilidad que le busca otorgar a ésta, pero sin que sea el único medio de información que puede realizarse bajo las nuevas tecnologías de la información. Cabe destacar que dicho proceso electrónico al que llamamos actualmente como ciberespacio, a diferencia de otros medios de comunicación masivos como la radio y la televisión, tiene principalmente como

[1] Kleinsteuber, H. El surgimiento del ciberespacio: la palabra y la realidaden Vidal, J. (2002). La ventana global. Madrid: Taurus

característica el cambio de las conductas clásicas de interacción entre comunicadores y público.

Dentro de este nuevo espacio, todos y cada uno de los individuos dentro de la sociedad, somos verdaderos comunicadores (editorialistas, líderes de opinión, corresponsales y un largo, entre otros); sin importar las particularidades económicas o culturales que podamos tener, basta con crear un perfil virtual dentro de cualquier red social dentro del ciberespacio.

Con la generalización del uso de los ordenadores y el uso de Internet se desarrollan sistemas de comunicación entre usuarios, como los e-mails y los chats.

Ante este panorama, es posible afirmar que, efectivamente, las sociedades afrontan un fenómeno conocido como "era digital". Es así que el colectivo social de los Estados evoluciona y empieza a crear un nuevo estilo de vida, desembocando en un nuevo tipo de sociedad: "Sociedad de la Información[2]", término que hace alusión a la comunidad que interactúa en nuestra época; y consecuentemente da pie a una integración mundial entre los diferentes Estados.

Y en razón del inmenso fenómeno informático, que con el paso de los años no hace más que seguir creciendo, surge la problemática, en cuanto a la necesidad de una posible regulación total o parcial del ciberespacio y, asimismo, determinar los límites de la misma. El mayor óbice para lo anterior radica en el hecho de la inmensidad de la zona virtual y la incapacidad de precisar al individuo o entidad que posea su propiedad.

Según Ronen Palan[3], sostiene de acuerdo a su obra "The Offshore World" que el problema de la regulación del ciberespacio radica en la siguiente premisa:

"*No es que intrínsecamente se opere en contra de la soberanía estatal, ni pretenda legitimarla o no. Estamos en realidad frente a un espacio que se concibe bajo sus propios*

[2] La primera persona en acuñar este termino fue Marc Porat, en su obra *Global Implications of the Information,* (1978). Global Implications of Information Society. Journal of Communication, 28(1): 70-80.

[3] Palan, R. (2006). The offshore world: sovereign markets, virtual places, and nomad millionaires. Estados Unidos de América: Cornell University Press

*términos, separado y por encima de la Nación-Estado...su existencia corresponde a cambios mucho más profundos"*.

Puesto que, al tomar medidas restrictivas en cuanto al uso del internet, puede consistir en una vulneración de Derechos Humanos, y a su vez causar una polarización de la realidad ocurrida en los Estados.

Como paradigma del postulado anterior se encuentra la situación que se vive en la República Popular de China; en donde ese Estado tiene total control de las redes informáticas, y en consecuencia condiciona a sus ciudadanos a contenidos web que estrictamente el Estado permite que vean.

# MARCO DOCTRINARIO

## 1. SURGIMIENTO DEL DERECHO INFORMATICO

La aparición de la informática en la sociedad ha generado múltiples relaciones entre ella y el Derecho. Los vertiginosos avances tecnológicos en esta materia, con el uso masivo de los computadores y la comunicación interactiva, presentan un nuevo y original desafío al derecho. La informática ha provocado la aparición de reglas de derecho que le son particulares, dispersas algunas, inadecuadas otras, algunas veces contradictorias, que han desafiado a las tradicionales instituciones del derecho.

Durante mucho tiempo el ser humano se ha interrelacionado de forma individual y de forma colectiva, ha buscado diferentes formas de organización en las cuales prevalezcan la satisfacción de sus intereses individuales y colectivos, bajo este punto de vista la historia ha demostrado que en la organización de ello, han prevalecido los más importantes: la economía, el comercio, la política, el poder y el derecho; siendo este último uno de los más imprescindibles, puesto que es casi imposible separarlo de los demás, bajo este punto de vista la evolución, el desarrollo de la tecnología y los intereses colectivos permitieron que las personas y sus gobernantes crearan leyes de acuerdo a las necesidades del Estado y sus habitantes.

Tomando como base todo lo anterior y en aras de definir el Derecho Informático es necesario estudiar su objeto de regulación, es decir, "La Informática".

## 1.1 LA INFORMÁTICA

La informática es una ciencia que se encarga del tratamiento de la información mediante el uso de dispositivos electrónicos o computacionales. Según Philippe Dreyfus[4], los sistemas informáticos deben cumplir con tres funciones respecto de la información: "entrada (captación de la información), procesamiento y salida (transmisión de la información)".

La informática reúne muchos de los elementos que el hombre ha utilizado para potenciar sus capacidades de pensamiento, facilitación de labores de realización compleja y comunicación. La aplicación de la informática incide en muchos sectores de la sociedad, en el ámbito financiero, transporte, medicina, e inclusive en el ámbito del derecho; siendo que los medios informáticos han sido utilizados por el hombre para establecer relaciones con otros individuos de la sociedad y bajo esa premisa, surge la necesidad de los Estados de regular las relaciones que se establecen a través del uso de elementos informáticos.

## 1.2 CARACTERÍSTICAS DE LA INFORMÁTICA

Una de las principales características de la informática, dada la naturaleza de los elementos informáticos, es en cuanto a la imposibilidad de aplicar instrumentos jurídicos tradicionales para su regulación en el sentido que la informática requiere la creación de nuevos elementos para que el estado implemente un control directo sobre las tecnologías de la información y de la comunicación:

**a)** Pertenece a una rama de la ciencia y como tal es un conjunto sistematizado de conocimientos para el tratamiento de la información mediante el uso de medios electrónicos y computacionales.

[4] La palabra francesa "informatique" fue creada por Philippe Dreyfus, director de la Bull Corporation's National Centre for Electronic Computing en la década de 1950, quien acuñó el término en 1962 cuando describía su compañía como una "Société d'Informatique Apliquée" *SIA* (en castellano: "Compañía de Tecnología de la Información Aplicada").

**b)** La informática es una ciencia multidisciplinaria ya que tiene aplicación en diferentes tareas dentro de la sociedad, tales como: las finanzas, transporte público, medicina, comunicaciones, entre otros.

**c)** Tienen como finalidad la captación, procesamientos y transmisión de la información.

**d)** Es dinámica en virtud del continuo desarrollo tecnológico que se da en la sociedad contemporánea.

La relación entre derecho e informática tiene dos líneas de investigación: los aspectos normativos del uso de la informática, desarrollados bajo el derecho de la informática, y la aplicación de la informática en el tratamiento de la información jurídica, conocida como informática jurídica.

## 1.3 DEFINICIÓN DE DERECHO INFORMÁTICO

El derecho informático se define como aquel conjunto de normas y principios que se derivan de la relación entre el derecho, la informática y la información. Guillemo Jimenez[5] nos define el derecho informático como: *"…el conjunto de normas y principios que derivan de los efectos jurídicos nacidos entre los sujetos en el ámbito de la informática y sus derivaciones, especialmente en el área denominada tecnología de la información…".*

Siguiendo a Julio Téllez[6] concibe el derecho informático en dos ámbitos; el primero hace alusión a la informática como instrumento del derecho (informática jurídica) y la informática como objeto de estudio del derecho.

La informática jurídica se refiere al uso de Tecnologías de la Información y Comunicación para facilitar la labor de los operadores de justicia y profesionales del derecho en el libre ejercicio de la profesión como una herramienta facilitadora para el tratamiento de la información con relevancia jurídica.

[5] Jiménez, W. G. & Meneses, O. (2017). Derecho e Internet: introducción a un campo emergente para la investigación y práctica jurídicas. Revista Prolegómenos Derechos y Valores, 20, 40, 43-61. DOI: http://dx.doi.org/10.18359/prole.3040. Pag. 49.

[6] Téllez, J. Derecho Informático. 4ta. Edición. México: McGraw-Hill. 2009.

De acuerdo con esa tónica, el grupo de investigación, define al derecho informático como *el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática*. Ahondando un poco sobre este concepto, resulta válido decir que es un conjunto de leyes en cuanto que, si bien escasos, existen diversos cuerpos jurídicos nacionales e internacionales con alusión específica al fenómeno informático.

Por otra parte, se refiere a hechos como resultado de un fenómeno aparejado a la informática imputable al hombre. Por último, se alude a actos como resultado de un fenómeno directamente vinculado con la informática y provocado por el hombre.

## 1.4 NATURALEZA DEL DERECHO INFORMÁTICO

El derecho informático debido a su amplitud en cuanto a su ámbito de acción en las diversas ramas del derecho resulta un trabajo difícil para determinar su naturaleza jurídica y ubicarla en un campo jurídico correspondiente.

Respecto a las fuentes y estructura temática del Derecho Informático, Antonio Pérez afirma que: *"…la revolución tecnológica incide sobre a las ramas del Derecho tradicionales…"* [7]; por ejemplo en el ámbito del Derecho Público en relación al Derecho Penal actual en que se regulan los delitos informáticos; el problema de la regulación del flujo internacional de datos informáticos, que interesa al Derecho Internacional Público; la libertad informática o defensa de las libertades frente a eventuales agresiones perpetradas por las tecnologías de la información y comunicación, objeto de especial atención por parte del Derecho Constitucional y Administrativo.

Mientras que inciden directamente en el Derecho Privado los siguientes fenómenos jurídicos: los contratos informáticos, que pueden afectar tanto al Hardware como al Software, dando lugar a una tipología comercial en la que pueden distinguirse contratos de compraventa, alquiler, leasing, copropiedad, multipropiedad, mantenimiento y servicios; así como distintos sistemas para la protección jurídica de los programas del ordenador (software), temas que innovan los objetos tradicionales de los Derechos Civil y Mercantil.

[7] PÉREZ LUÑO, Antonio Enrique. "Manual de informática y derecho", Editorial Ariel S.A., Barcelona, 1996.

Por tal razón, la naturaleza del derecho informático se considera multidisciplinaria, ya que resulta imposible situar al derecho informático en un solo orden tradicional del derecho en razón de las diferentes relaciones que pueden llegar a establecerse a través del uso de las Tecnologías de la información. El derecho informático abarca un objeto de estudio particularizado y consecuentemente su propia metodología, por lo que la clasificación tradicional en público o privado restringe esta disciplina.

Así surge el problema a la hora de catalogar al derecho informático como derecho público o privado, e incluso social, debido a que no se puede establecer límite o separación entre estas ramas jurídicas, es por ello que se habla del derecho informático como un derecho autónomo.

No obstante, al hablar de la autonomía del derecho de la informática, este no puede entenderse como un cuerpo normativo con naturaleza propia e independiente, según Juan José Ríos Estavillo, debido a que *"no se le da validez a la existencia a esta disciplina como autónoma o científica, sobre todo porque sus derivaciones pueden darse en el campo del derecho público, del derecho privado y hasta del derecho social y por tal, supuestamente no goza de autonomía propia"*[8]; es decir, no se circunscribe propiamente al derecho público, privado o en el social, como sí se da en otras disciplinas.

Pese a lo anterior, la autonomía no implica que se separe o desentienda de la ciencia a la cual pertenece y de la cual depende, sino que aborde los problemas con métodos propios e instrumentos legales integrados, principios normativos y ámbito de aplicación. Por lo que la naturaleza especial del Derecho Informático debe integrarse a las normativas establecidas por el ámbito público del derecho, sin perjuicio de las connotaciones privadas o sociales de los bienes jurídicos afectados en las de las relaciones que nazcan a partir de la regulación de dicho Derecho.

[8] Ríos Estavillo, Juan José autor Derecho e informática en México : informática jurídica y derecho de la informática / México : Universidad Nacional Autónoma de México, 1997; pag. 70.

## 1.5 CARACTERISTICAS DEL DERECHO INFORMATICO

Como toda rama del Derecho, el Derecho Informático posee características especiales que permiten individualizarlo, entre las cuales se pueden mencionar[9]:

**a)** Es un derecho moderno, en comparación con otras ramas tradicionales del Derecho, que tiene sus orígenes en los problemas generados por la Implementación de la computadora en la sociedad. Se recordará que el impulso y posterior desarrollo de las computadoras data de los años 50 del siglo XX.

**b)** Es un derecho íntimamente influenciado por las tecnologías en general, debido a que éstas han permitido un desarrollo sostenido de la computadora y su entorno, por ejemplo, en la actualidad se tienen una serie de problemas jurídicos generados por el uso de Internet en las diversas actividades de las personas.

**c)** Es un derecho que se encuentra ligado al proceso de globalización, por lo que el jurista se encuentra obligado a resolver el problema del juez competente, el mismo que debe conocer y dar solución a determinado caso concreto, debiendo, asimismo, analizar todo aquello que esté relacionado con la ley aplicable a cada situación en particular.

**d)** Es un derecho que necesariamente debe ser legislado en leyes especiales, debido a que su objeto de estudio, así como sus formas de regulación son muy dinámicas.

**e)** Es un derecho autónomo, con instituciones propias que se encarga de brindar soluciones legales a los problemas planteados por el avance científico en el ámbito de su competencia. Es importante indicar, que conforme transcurre el tiempo surgen nuevas dificultades legales no previstas por el jurista, el legislador o el juez, pero que el Derecho informático permite solucionar, hecho que refuerza y sustenta la característica en mención.

[9] https://www.ecured.cu/Derecho_inform%C3%A1tico#Caracter.C3.ADsticas

# 2. TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EN RELACIÓN AL DERECHO INFORMATICO Y SU REGULACIÓN

Las Tecnologías de la Información y de la Comunicación como parte del desarrollo de la tecnología forman parte esencial en la sociedad y como tal es necesaria la regulación del mismo, puesto que a partir de la interrelación del Derecho y de la Informática surgen efectos en el Bien Jurídico de los usuarios, uno de los primeros cuerpos normativos que contempla esto es la Declaración Universal de Derechos Humanos en su artículo 19.

Esto permitió a los países integrantes de la ONU, elaborar cuerpos jurídicos que les permitan la regulación de las TIC´S, debido a la inminente globalización tecnológica se toma como bien jurídico a la información; es ahí donde el Estado Salvadoreño participa con la imposición de Leyes secundarias que regulan a las Tecnologías de la Información y Comunicación, ejemplo de ello es la Ley de Telecomunicaciones de la Superintendencia General de Electricidad y Telecomunicaciones, la Ley Especial Contra los Delitos Informáticos y Conexos.

## 2.1 DEFINICIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

En cuanto a las Tecnologías de la Información y de la Comunicación (a partir de este párrafo llamadas TIC´S), tiene una aplicación práctica universal ya que son útiles en el fácil acceso a la Información, utilización de instrumentos para el procesamiento de todo tipo de datos tanto hardware como software, canales de información multimedia, almacenamiento de grandes cantidades de información en pequeños soportes de fácil transporte, facilitan tareas o actividades de realización compleja puesto que con la programación de dispositivos se hace más eficiente el desempeño de labores domésticas, académicas y empresariales, interactividad entre grandes cantidades de usuarios de las redes de comunicación digitales como redes sociales, blogs, páginas web, plataformas, entre otros.

Bajo esta perspectiva un concepto general de Tecnologías de Información y Comunicación es el siguiente: "*Son todos aquellos recursos herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos*

*soportes tecnológicos tales como: computadoras, teléfonos móviles, televisores, reproductores portátiles de audio y video o consolas de video juego. Ofrecen muchos servicios como correo electrónico, búsqueda de información, banca online, descarga de música y cine, comercio electrónico, entre otros*" [10].

## 2.2 CARACTERISTICAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Las características de las TIC más representativas, son su capacidad para mejorar habilidades intelectuales, compatibilidad con otros medios de enseñanza, se pueden usar desde cualquier lugar, se centran en los objetivos, espacio reducido de almacenamiento y otras que a continuación se explican.

a) La interconexión y la capacidad de que varias tecnologías puedan funcionar en conjunto para propiciar nuevas herramientas de comunicación.

b) La interactividad como el intercambio de información entre usuarios por medio de dispositivos tecnológicos. Esto es posible una vez se han adaptado ciertos sistemas a las necesidades de los usuarios. Por ejemplo, en la actualidad se realizan diversas actividades escolares por medio del uso de dispositivos móviles.

c) Funcionan a gran velocidad, en especial si se cuenta con una excelente conexión a internet, lo que permite ahorrar tiempo y acercar a las personas más allá de la distancia física.

d) Tienen un amplio alcance tanto individual como social, esto se debe a que están involucradas en las actividades económicas, educativas, culturales, científicas, en el sector industrial, entre otras áreas en las que se comparte y genera información de manera grupal.

e) Se encuentran en constante cambio e innovación debido a su desarrollo indetenible y la búsqueda de ofrecer mayor alcance comunicacional y de transmisión de la información.

[10] ¿Qué son las TICS? UNAM, disponible en: http://tutorial.cch.unam.mx/bloque4/lasTIC

# 3. EL CIBERESPACIO COMO UN ESPACIO PÚBLICO Y LA NECESIDAD EMERGENTE DE LA INTERVENCIÓN ESTATAL

Puede decirse que el ciberespacio es una realidad virtual. No se trata de un ámbito físico, que puede ser tocado, sino que es una construcción digital desarrollada con computadoras (ordenadores).

Es necesario agregar que el término "ciberespacio" deriva de "cibernética", el cual fue acuñado por Norbert Wiener en la década de 1940 para hacer referencia al estudio de las analogías entre los sistemas de comunicación y de control de las máquinas y los seres vivos.

En la actualidad, el concepto de ciberespacio suele asociarse a internet. Todo aquello que se desarrolla en internet, a través de sitios web, correos electrónicos, redes sociales, entre otros, no tiene lugar en un país específico, más allá de la ubicación concreta de los servidores y de los usuarios. El ciberespacio, de todos modos, es más amplio que Internet.

Si bien algunas personas utilizan los términos "ciberespacio" e "internet" como sinónimos, es más correcto entenderlos de forma jerárquica: podemos pensar que internet se encuentra en el ciberespacio, que el gran conjunto de páginas y aplicaciones a las que accedemos desde nuestros dispositivos se alojan en ese dominio infinito e intangible, donde también tendrán lugar experiencias futuras que no forman parte del concepto de internet.

## 3.1 CARACTERÍSTICAS DEL CIBERESPACIO

El ciberespacio se refiere a un entorno no físico creado por equipos de cómputo unidos para interoperar en una red. En el ciberespacio, los operadores del equipo pueden interactuar de manera similar al mundo real sin necesidad de tener interacción física.

El ciberespacio sobrepasa los límites de cómo y cuándo interactuar. Entre las características del ciberespacio están las siguientes:

a) Identidad, flexibilidad y anonimato: la falta de interacción física cara a cara causa un impacto en cómo la gente presenta su identidad. Pues se tiene la

oportunidad de expresar sólo algunas partes de tu identidad o quizá quedarse en el anonimato, incluso se da la posibilidad de tener una identidad imaginaria o falsa.

b) Trasciende los límites espaciales: Las distancias geográficas no limitan quién pueda comunicarse con quién. Es posible comunicarse con cualquier persona sin importar que esté en otro país.

c) Tiempo extendido y condensado: puede haber una comunicación con cualquiera vía internet, puede haber varias personas sentadas en su computadora al mismo tiempo. Este tipo de comunicación crea un espacio temporal donde el estar, como tiempo interactivo se extiende.

## 3.2 EL CIBERESPACIO COMO UN ESPACIO PÚBLICO

El ciberespacio no cuenta con una circunscripción geográfica sino que se establece a partir de la interrelación que se da virtualmente en la conexión entre usuarios, ejemplo de ello se da cuando una persona que se encuentra en El Salvador sostiene intercambio de mensajes con su esposa que se encuentra en España, entre los dos intercambian mensajes, conversan por medio de video llamadas; el punto de encuentro entre ellos es el ciberespacio ya que no existe un "encuentro" físico sino una forma de vinculación digital.

En razón de ello, la relación de interconexión entre millones de usuarios surge a partir de las relaciones de coincidencia de visitas y usos en dominios de páginas web del internet. Por lo tanto, estas relaciones de interconexión pueden ser comerciales, personales, didácticas, entre otras; sin embargo, también existe la posibilidad de que sean utilizadas para el cometimiento de ilícitos que transgredan, vulneren y violenten los bienes jurídicos de las personas naturales o jurídicas, sean estas de carácter personal o a terceros.

## 3.3 EL CIBERESPACIO FRENTE A LA SOBERANÍA DE LOS ESTADOS

A inicios del siglo XXI y como consecuencia del legado que el siglo pasado nos dejó, marca una tendencia en materia tecnológica frente a un eminente cambio de paradigma social, cultural y económico.

Internet, como la expresión tecnológica que revolucionó (y sigue revolucionando y evolucionando) las comunicaciones a escala global, plantea un nuevo espectro de problemáticas a debatir, donde se funden los límites y fronteras de los que conocimos hasta ahora como "Estados", para constituir una sola comunidad.

El derecho, como ciencia social que estudia los mecanismos y los contenidos de los enunciados a través de los cuales los hombres reglamentan su vida en comunidad, no puede estar ajeno a esta "red de redes" que conecta cada pequeña sub-comunidad y la congrega en una verdadera comunidad universal.

"En cuanto a su amplitud, la Internet ha afectado la efectividad y contenido de derechos fundamentales de raigambre constitucional, y ha alterado significativamente la operatividad de las fronteras nacionales"[11].

El sistema jurídico nacional vigente no contiene tal cual una codificación general de reglas aplicables a cuestiones del ciberespacio. Sin embargo, el derecho de Internet está evolucionando en nuestro país, inicialmente a través de la aplicación de reglas contenidas en el Código Civil y otras leyes generales, y luego de ello, a través de leyes específicas que regulan algunos aspectos del derecho de Internet, como es el caso de la firma digital[12].

Esta aparente precariedad en la normativa que regula Internet encuentra diversas razones que la justifican. La principal ha sido la velocidad con que el desarrollo de Internet se ha instalado en nuestra sociedad, lo que impide su regulación a través del complejo proceso legislativo tradicional.

En teoría, la estructura legal puede adaptarse fácilmente a cambios tecnológicos y corresponde a la jurisprudencia ir realizando los necesarios ajustes para hacer viable el sistema en el contexto de conflictos y transacciones específicas.[13]

El creciente uso de Internet es uno de los avances tecnológicos y políticos más interesantes de los últimos años del siglo XX. El potencial que tiene Internet para

[11] PERRITT, Henry H., "Internet: ¿Una amenaza para la soberanía?", Indiana Journal of Global Legal Studies, 1998, vol. 5, p. 423.

[12] DECRETO N° 133, D. O. N° 196 Tomo N° 409 Fecha: 26 de octubre de 2015, Ley de Firma electrónica.

[13] CABANELLAS DE LAS CUEVAS, Guillermo - MONTES DE OCA, Ángel, Derecho de Internet, cit

convertirse en el medio propicio para el desarrollo de un mercado global y en un foro de actividades políticas tradicionales y novedosas se está haciendo realidad a pasos agigantados.[14]

De esta forma, frente a los conflictos interpersonales que se originan a raíz de Internet, surge el problema de la ley aplicable, y con ello, el interrogante de quién gobierna y legisla en este "espacio virtual". Para dar respuesta a esta problemática primeramente se debe dar por establecido el concepto de la soberanía de los Estados.

## 3.4 EL CONCEPTO TRADICIONAL DE SOBERANÍA

La soberanía, se refiere al ejercicio de la autoridad en un cierto territorio. Esta autoridad recae en el pueblo, aunque la gente no realiza un ejercicio directo de la misma, sino que delega dicho poder en sus representantes.

La palabra soberanía, "souverainité o soveregnity" se usó desde el medioevo para referirse al poder del soberano, del que estaba sobre todos; o sea, el rey, el príncipe o emperador. Se la usó con ese significado en el francés medieval para referirse al rey o al señor feudal, pero llegó a generalizarse para calificar también a la autoridad del juez o del señor feudal.[15]

La soberanía a *groso modo* significa independencia, es decir, un poder con competencia total. Este principio señala que la Constitución es el fundamento o la base principal del ordenamiento jurídico, por lo que no puede existir norma que esté por encima de esta.

Frente a la realidad que nos presenta el ciberespacio, nacen unas cuantas interrogantes; en dónde o en quién recaería esta soberanía. ¿Es posible que recaiga sobre un Estado, sobre una comunidad de Estados, sobre cada individuo, sobre un ente abstracto supranacional?

---

[14] AOKI, Keith, "Soberanías múltiples y superpuestas. Liberalismo, doctrina libertaria, soberanía nacional, propiedad intelectual 'global' e Internet", Indiana Journal of Global Legal Studies, 1998, vol. 5, p. 443.

[15] PELLET LASTRA, Arturo, Teoría del Estado, LexisNexis, Buenos Aires, 2003.

Del concepto de soberanía se puede entender que da paso al concepto de co-soberanía. Ésta es la tendencia dominante para responder la pregunta que se formuló anteriormente. La red de redes genera un espacio en donde convergen individuos, independientemente de su ubicación geográfica, y estos individuos, como miembros de Estados, se despojan de sus nacionalidades para interactuar.

El conflicto surge cuando se intenta establecer bajo qué pautas actúan y dónde reside esa "soberanía" si nos posicionamos en un espacio sin fronteras. Esto no sólo sucede en el "ciberespacio". Es la tendencia mundial que las relaciones internacionales y la creación de organismos supranacionales tengan papel primordial en lo que se llamó "derecho de la integración". Un ejemplo es el de la Comunidad Europea: los Estados miembros están cediendo derechos que tradicionalmente se consideraban indelegables en los órganos comunitarios.

A consecuencia de lo anterior el concepto de soberanía se ve obligado a mutar. A adaptarse para no extinguirse. Y en esta reformulación conceptual nos vemos obligados a pensar en un lugar despojado de toda idea física de "lugar". De esta forma vemos una denominación especial de soberanía que puede llamarse: soberanía a-territorial, soberanía supranacional, soberanía de no-estados.

A su vez, las nuevas relaciones que nacen para estos ciudadanos que se congregan en la red de redes nos plantea el perfil de un individuo anónimo, incluso despojado de toda conciencia cívica. Es el reinado de los Estados de *no-ciudadanos*, pese a las corrientes que afirman que el ciberespacio funcionaría reafirmando la idea de soberanía y de democracia participativa, al mejor estilo liberal.

## 4. LA REVOLUCIÓN TECNOLÓGICA COMO POTENCIADORES DE DELITOS.

En 2,011, al menos 2.300 millones de personas, el equivalente a más de un tercio de la población total del mundo, tenía acceso a Internet. Más del 60% de todos los usuarios de Internet se encuentran en países en desarrollo, y el 45% de todos los usuarios de Internet tienen menos de 25 años de edad.

Para el año 2,017 se calcula que las suscripciones a banda ancha móvil llegarán al 70 por ciento de la población total del mundo. Para el año 2,020, el número de dispositivos interconectados por la red rebasará a las personas en una proporción de seis a uno, transformando las concepciones actuales de lo que es Internet. En el mundo hiperconectado del mañana, será difícil imaginarse un 'delito informático', y quizás cualquier otro delito que no involucre evidencia electrónica vinculada con la conectividad del Protocolo de Internet (IP)[16].

En muchos países, la explosión en conectividad global ha llegado en una época de transformaciones económicas y demográficas, con crecientes disparidades en los ingresos, ajustes en los gastos del sector privado y menor liquidez financiera.

Se calcula que más del 80% de los actos de delito cibernético se originan en algún tipo de actividad organizada, con mercados negros de delito cibernético establecidos en un ciclo de creación de programas informáticos maliciosos, infección de computadoras, administración de redes zombi o "botnet", recolección de datos personales y financieros, venta de datos, y 'cobro' a cambio de información financiera.

Los perpetradores de delitos cibernéticos ya no requieren aptitudes o técnicas complejas. En particular en el contexto de los países en desarrollo han surgido subculturas de jóvenes que participan en fraudes financieros informáticos, muchos de los cuales comenzaron a participar en el delito cibernético a finales de su adolescencia.

El uso creciente de las redes sociales y el contenido de Internet generado por usuarios ha dado pie a respuestas regulatorias de los gobiernos, incluida la aplicación del derecho penal, y a llamamientos en favor de los derechos a la libertad de expresión.

El elemento sociocultural de algunas limitaciones se refleja no solo en la legislación nacional, sino también en los instrumentos multilaterales; por ejemplo, algunos instrumentos internacionales[17] sobre delito cibernético contienen delitos amplios con

[16] Ziewitz, M. and Brown, I. 2013. A prehistory of Internet governance. En: Brown, I.Research Handbook on Governance of the Internet. Cheltenham: Edward Elgar.

[17] Uno o más de los siguientes instrumentos: El Convenio sobre Ciberdelincuencia del Consejo de Europa, la Convención para combatir Delitos con Tecnología de la Información de la Liga de los Estados Árabes, el Acuerdo de Cooperación para combatir Delitos.

respecto a la violación de la moral pública, el material pornográfico y los principios o valores religiosos o familiares.

La legislación internacional sobre derechos humanos actúa tanto de espada como de escudo al requerir la criminalización de (ciertas) formas extremas de expresión mientras que protege otras. Por lo tanto, a los Estados que son parte de los instrumentos internacionales sobre derechos humanos se le exigen algunas prohibiciones a la libertad de expresión, incluyendo la instigación al genocidio, la manifestación del odio que constituye instigación a la discriminación, hostilidad o violencia, la instigación al terrorismo, y la propaganda de guerra.

Para otros, el 'margen de apreciación' les permite cierto margen para que los países determinen las fronteras a la libertad de expresión de conformidad con sus propias culturas y tradiciones jurídicas. No obstante, la legislación internacional sobre derechos humanos intervendrá en cierto punto. Por ejemplo, las leyes penales sobre difamación, desacato a la autoridad e insulto que se aplican a las expresiones en línea tendrán un alto umbral para demostrar que las medidas son proporcionales, adecuadas y lo menos intrusivas posible.

Cuando el contenido sea ilegal en un país, pero legal producirlo y divulgarlo en otro, los Estados tendrán que enfocar las respuestas de la justicia penal en las personas que obtienen acceso al contenido dentro de la jurisdicción nacional, y no al contenido producido fuera de su país.

## 4.1 LOS DELITOS INFORMÁTICOS

Los cambios sociales provocados por las tecnologías de la información resultan decisivos en todos los ámbitos y por supuestos también tienen su repercusión en el campo del Derecho penal.[18]

Las inmensas posibilidades que abren las nuevas tecnologías, evitando al ser humano cierto tipo de tareas más mecánicas, suponen como señala Sieber[19] unos cambios

[18] Sobre los cambios de perspectivas en los planos cultural y jurídico con la irrupción de las nuevas tecnologías, en lo que se denomina la nueva etapa del "simio informatizado, puede verse la exposición de TÉLLEZ AGUILERA, A. Nuevas Tecnologías. Intimidad y protección de datos, Edisofern, 2001, pp. 21 y ss.

[19] SIEBER, U. Computerkriminalität und Strafrecht, München, 1977, p. 23.

más radicales que los que introdujo la revolución industrial del siglo XIX con la sustitución del trabajo físico de los hombres por el de las máquinas.

Los avances de la informática sitúan al Derecho penal ante problemas nuevos, o ante problemas que debe abordar con una nueva visión de los mismos.

Las enormes potencialidades que se abren para el tratamiento automatizado de datos, tienen un reverso que son los riesgos que se introducen para facilitar la realización de hechos que afecten a los intereses fundamentales de las personas.

Es decir, la informática, o en general, el tratamiento automatizado de datos se presenta como factor criminógeno, pues permite el acceso y el manejo de bases de datos, programas de cualquier género, en ocasiones de forma lesiva para los intereses básicos de las personas y de la sociedad, siendo más costosa la averiguación del autor y la prueba de los hechos debido a la naturaleza del procedimiento informático.

Tomando como base lo anterior, los delitos informáticos se definen como aquellos actos ilícitos cometidos por medio de tecnologías de la información y comunicación prevaleciéndose de las capacidades y características de estas tecnologías en cualquiera de sus dos modalidades: a) en cuanto a los actos en contra de sistemas informáticos tales como bases de datos, piratería, entre otros; b) en relación a delitos comunes cometidos por medio de tecnologías de la información y comunicación aprovechándose de las diversas ventajas que ofrecen estas tecnologías como lo son el anonimato y la capacidad de realizar transacciones de forma inmediata desde diferentes puntos geográficos.

## 4.2 NATURALEZA DE LOS DELITOS INFORMÁTICOS

La naturaleza jurídica se refiere al lugar que ocupan las instituciones del derecho dentro del universo jurídico de las cual dichas instituciones forman parte; es decir, es el lugar que las características propias de estas instituciones del derecho les asignan, haciéndolo parte de un sistema género-especie.

Para identificar la naturaleza jurídica de los delitos informáticos, es menester entonces, analizar los elementos de cada género y especie, los elementos diferenciadores y sus similitudes:

Dentro del derecho positivo partiendo del principio *"Nullum crimen, nullum poena sine praevia lege"* entenderemos entonces que se regulan aquellas conductas en las cuales los poderes públicos del Estado pretende hacer uso de su facultad punitiva en cuanto el individuo actúe al margen de la norma prestablecida[20].

En ese orden de ideas se ubica entonces a los delitos informáticos, dentro del género del Derecho Público, en la rama del derecho penal dado que la finalidad de los Estados en su regulación atiende a la protección de bienes jurídicos tutelados de importancia tal, que da la potestad al Estado de coartar la libertad de quienes atentan contra los bienes jurídicos tutelados, previendo en los ordenamientos jurídicos, penas de este tipo o penas de carácter pecuniario.

## 4.3 CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS

Según el Julio Tellez Valdes en su obra *"Derecho Informático"*[21] enlista las características principales de esta manera:

a) Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos;

b) Algunos de estos delitos requieren determinados conocimientos por parte del actor directo del delito informático razón por la cual se les consideró como "Delitos de Cuello Blanco"

c) Presentan dificultades en su comprobación debido al carácter técnico que poseen los delitos informáticos;

---

[20] NOTA: Si bien es cierto que la tendencia general es la de "privatizar el derecho penal", ofreciendo a las victimas la posibilidad de acordar con los victimarios una forma de resarcimiento convencional y dejar de lado la rigidez clásica las penas de carácter privativo de libertad como la sanción para la rehabilitación del individuo; no es menos cierto que se conserva un interés público relativo a la preservación de ciertos derechos y libertades, que ameritan una protección jurídica de "ultima ratio" dándole a estos la innegable carácter público.

[21] Derecho Informático por Dr. Julio Téllez Valdés

d) Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos;

e) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del derecho o por desconocimiento de las conductas típicas de la víctima.

## 4.4 CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

Como se mencionó, todos los delitos cibernéticos tienen el común que se suceden en internet y/o se emplean medios informáticos para ello. Por esta razón, el delito cibernético engloba en realidad cualquier hecho delictivo que, si bien antes sólo se realizaba en el mundo físico, ahora puede ser perpetrado a distancia, en internet, a través de herramientas y equipos informáticos.

Una de las compañías especializadas en seguridad informática más prestigiosas del mundo, Symantec[22], trata de poner orden en la inmensa variedad de tipos de delitos cibernéticos al clasificarlos en sólo dos tipos en base a la perspectiva de la víctima:

**a)** Delitos cibernéticos de tipo I. Son todos aquellos que tienen lugar una única vez respecto a la misma víctima. Con relativa frecuencia, aunque no siempre, algún tipo de programa malicioso para registrar la actividad de la víctima aprovechando los fallos de seguridad del navegador o del sistema operativo; forman parte de este tipo de delitos el *"phishing"* el cual consiste en el envío de un correo electrónico falso que trata de engañar al usuario para que éste revele sus datos personales, la instalación de un malware en un ordenador para espiar a la víctima, la usurpación de identidad, el fraude, la piratería, entre otros.

**b)** Delitos cibernéticos de tipo II. En este caso, la interacción con la víctima se produce en repetidas ocasiones, por ejemplo, en casos de chantaje, extorsión, acoso, espionaje industrial, planificación de actividades terroristas, etcétera.

[22] Symantec, "Norton Cybercrime Report", 2012. Disponible en http://us.norton.com/cybercrimereport.

# 5. MECANISMOS DE CONTROL SOBRE EL CIBERSPACIO

Siendo el internet una herramienta muy útil, versátil con gran influencia en los mercados internacionales y que ha cambiado la forma de vida de la población a nivel mundial este configura a través de los años la forma de su funcionamiento, desde la infraestructura física que sirve para la comunicación de servidores, los protocolos que utilizan las empresas que proveen el servicio y la información que es almacenada y que genera datos.

Es necesario entonces conocer estos cambios que han llevado a la administración actual de este servicio. En los años 90´s surgieron problemáticas acerca de la administración y al acceso de información puesto que Jon Postel era el encargado de administrar las extensiones o dominios y del sistema de nombres y dominios que existían en ese entonces en la ARPANET, que era una red de defensa del Departamento de Defensa de los Estados Unidos.

La importancia de ello es que a través del protocolo de internet (I.P.) se accede al número que identifica las direcciones IP, de los dispositivos conectados a la red. Por lo tanto el poder que conlleva es delicado, el gobierno de los Estados Unidos se da cuenta de ello e interviene despojando a Postel y a la comunidad tecnológica; se integra el gobierno, sector privado, sociedad civil y la comunidad tecnológica surge entonces el ICAAN, que dirigirían el uso del internet y su evolución.

El ICAAN (Internet Corporation for Asigned Names or Numbers) o “IANA” en español es la entidad encargada de administrar las asignaciones de protocolo, la administración de los recursos numéricos de internet y la gestión de la zona raíz, cada uno de estos elementos son modificados a conveniencia de lo que dicha administración considera positivo, ello conlleva la “Gobernanza del internet”.

Esto permitió que exista un tipo de regulación en la red, sin embargo los datos que se almacenan y su estructura sigue siendo dependiente de administración privada aunque por principio universal de soberanía los Estados lograron que los intermediarios regularan

el contenido que circula en internet, asimismo los datos de geo localización de los usuarios.[23]

## 5.1 DEFINICIÓN DE MECANISMOS DE CONTROL DEL CIBERESPACIO

En términos generales, los mecanismos de control son todos aquellos medios de los cuales hacen uso los Estados para ejercer un control tanto de las entidades estatales, concesionarios y gobernados a través de la creación de normativas, procedimientos, lineamientos, reglamentos, entre otros, para dar cumplimiento a los fines del Estado.

En cuanto a los mecanismos de control dentro el ciberespacio, hoy en día aún es muy difícil y delicada su reglamentación en virtud de las características propias del ciberespacio y la situación en la que este se encuentra incluido; siendo considerada como un tema de interés mundial. Esta problemática se introduce en la mayoría de gobiernos alrededor del mundo y a pesar de los grandes esfuerzos realizados por estos Estados, aun no es posible imponer una adecuada regulación; dejando a la merced el cometimiento de los delitos informáticos.

Además de ello, incrementa de forma exponencial y se perfeccionan de forma constante, siendo casi imposible de investigar estos flagelos y, consecuentemente, dirimirlos dentro de la esfera jurisdiccional. Con el simple hecho de la ausencia de Tribunales, juzgados y unidades fiscales especializados en el ámbito de los llamados "ciberdelitos" o delitos informáticos; brindándonos un procedimiento deficiente con procedimientos que aún no están armonizados con el momento actual lo cual afecta con demasía dicho proceso.

Uno de los intentos más palpables para regular el ciberespacio con la finalidad de regular el uso y la administración de lo que circula dentro de la World Wide Web es el Convenio de Ciber-Delincuencia o Convenio de Budapest en el cual El Salvador forma parte; siendo su principal objetivo la cooperación entre los países firmantes, para el intercambio y suministro de evidencia digital.

[23] Fuente: Historia del internet y ciberespacio

El ciberespacio debido a su constante expansión y evolución es algo que se encuentra en nuestro entorno y forma parte de nuestra cotidianeidad tanto en los ámbitos sociales, culturales, educativos, entre otros. En razón de ello, resulta menester desarrollar mecanismos de control concretos, efectivos y regulatorios atendiendo a los límites y capacidades del ciberespacio. Asimismo, es necesario dejar por sentado que el ciberespacio no es solo internet o un sitio dentro de este (páginas web, videojuegos en línea, redes sociales, entre otros); esto es, todo lo que hace posible la interacción entre dos o más personas en el ámbito virtual, así como también lo que hace posible la relación entre el sujeto y un objeto a través de internet.

Por ello, consideramos que la transición de la sociedad a la llamada "Era de la Revolución Digital" a un ámbito virtual como lo es el ciberespacio como un entorno de interacción entre los individuos, ya sea para realizar el comercio, ocio, entretenimiento, y, en el peor de los casos, para realizar actos contrarios al ordenamiento jurídico; hace imperativo que los estados establezcan mecanismos de control, a través de cuerpos legales, instituciones encargadas de la investigación, entre otros, aparejado con una adecuada capacitación de los operadores de justicia del órgano jurisdiccional.

## 5.2 TIPOS DE MECANISMOS DE CONTROL

### 5.2.1 LA CENSURA

La censura, según el Diccionario de la lengua española de la Real Academia Española, es la "i*ntervención que practica el censor en el contenido o en la forma de una obra, atendiendo a razones ideológicas, morales o políticas"*[24]. En un sentido amplio, se considera como supresión de material de comunicación que puede ser considerado ofensivo, dañino, inconveniente o innecesario para el gobierno o los medios de comunicación, según lo determinado por un censor.

Un censor puede referirse a una persona o institución, con cierto tipo de poder político, cultural, social, económico entre otros; es responsable de verificar que las publicaciones realizadas en medios de comunicación tales como noticieros, películas,

[24] "censura", "censura previa" en *Diccionario de la lengua española* (de la Real Academia Española), vigésima segunda edición enmendada.

espectáculos y otros más, cumplan con las normas o criterios establecidos, dentro de un marco legal o político de un estado.

Etimológicamente La palabra *censura* proviene de la palabra latina *censor*, es decir, el trabajo de dos romanos cuyo deber consistía en supervisar el comportamiento del público y la moral, por lo tanto, *censuraban* la forma de actuar.

Tradicionalmente la censura se clasifica en razón del tipo de información que se desea censurar frente a un conglomerado de individuos dentro de la sociedad, entre algunas clases de censura se pueden mencionar:

**a) Censura Moral**: íntimamente relacionado a lo políticamente correcto, trata que se tome como ley común el gusto o la predilección moral de un grupo social predominante de una época.

**b) Censura Política: e**n un sentido amplio se considera como el ejercicio, por parte directa del Estado o por delegación en alguna organización o grupo, para controlar la libertad de expresión, así como la libertad de opinión y pensamientos.

**c) Censura Religiosa:** es uno de los tipos de intervención que la religión hace sobre la libertad de expresión, controlándola o limitándola sobre la base de su autoridad.

**d) Censura Militar:** es el proceso de mantenimiento de la inteligencia militar y tácticas de carácter confidencial y lejos del enemigo. Esto se utiliza para contrarrestar el espionaje, que es el proceso de recopilar información militar.

## 5.3 LA NEUTRALIDAD DE LA RED

Todos los servidores que forman la red de internet están distribuidos en los países más desarrollados en el mundo, las empresas que proveen el servicio se conocen como intermediarios. El Principio Universal de Soberanía permitió a los gobiernos presionar a los intermediarios o proveedores de servicio para que protegieran los Derechos de autor, pero no se pronuncia ante la libertad de expresión

Al ser el ciberespacio un punto de encuentro de interconexión digital entre usuarios a nivel mundial no es ajeno a la regulación en cuanto a su funcionamiento y la operatividad

que necesita, sin embargo, no tiene regulación alguna en cuanto a su contenido. Pero existen diferentes formas de regulación que se han hecho populares y se han promulgado en los diferentes Estados que hacen uso del ciberespacio, a continuación, se enuncian las principales:

La heteroregulacion del ciberespacio por parte de los Estados que hacen uso del ciberespacio, significa que los Estados a través de sus Leyes y sus instituciones son las encargadas de regular la administración de la banda ancha y regulan la forma de asignación a las empresas distribuidoras y estas a su vez el contenido del ciberespacio, en algunos Estados se debe a la coyuntura sociopolítica y económica.

La autorregulación por parte de las empresas que regulan el servicio a través de sus códigos de ética, debido a la falta de regulación o al libre mercado, algunos Estados no regulan el contenido del ciberespacio, sino que este queda a discreción de la empresa que presta el servicio, la controversia entonces está en los códigos de ética que la empresa plantea, ya que en muchas de las ocasiones impera los intereses económicos por sobre los intereses de la sociedad.

En tal sentido, la intimidad y la privacidad de los usuarios del ciberespacio puede verse vulnerada ya que la información de estos es valiosa, puesto que con la venta de estos datos se pueden canalizar dicha información para la colocación de productos o servicios de forma focalizada; ya que en muchos de los casos los usuarios no se toman el tiempo de leer los términos y condiciones de los servicios proveídos por las plataformas digitales.

Los ciberciudadanos pueden regular el ciberespacio, esta forma de regulación plantea que los usuarios pueden regular el contenido que circula por el ciberespacio partiendo del conocimiento que son los que conocen como funciona este y que son letrados en ello.

## 6. LA NECESIDAD DE POLÍTICAS EN MATERIA DE CONTROL DE LAS TECNOLOGIAS DE COMUNICACIÓN E INFORMACIÓN.

Existe la controversia en cuanto a la regulación del contenido que se encuentra en la red, siendo su alcance global y tomando en cuenta que una de las características del mismo

es que siempre va un paso delante de la ley ya que estas se crean para regular conductas típicas antijurídicas a partir de uno o varios hechos delictivos detectados por las autoridades, la ley en principio no se anticipa a los hechos que suceden en internet.

En ese caso, surgen las iniciativas de ley para regular el contenido que circula por el ciberespacio, es entonces donde surge la controversia en cuanto lo que debe imperar la libre circulación del contenido, sin embargo, en el caso del Estado Salvadoreño existieron iniciativas de Ley que plantearon la vulneración de Derechos Constitucionales, debido a la ambigüedad o la falta de esclarecimiento en cuanto a los sujetos activos.

Dicho anteproyecto de Ley fue impulsado por un sector conservador de la política salvadoreña que no estaban de acuerdo con la crítica hacia las autoridades en el ciberespacio, por parte de los usuarios de las plataformas de redes sociales que no estaban de acuerdo con las decisiones de los funcionarios públicos, surgiendo el debate en que esto vulneraba flagrantemente la libertad de expresión.

## 7. POLITICAS PÚBLICAS DE REGULACION CIBERNETICA UTILIZADAS POR EL ESTADO SALVADOREÑO.

Como se dijo anteriormente, el ciberespacio como tal debe considerarse como un espacio intangible y gigante, en donde ningún país puede ejercer una soberanía como tal, y que a su vez puede traspasar las fronteras de los diferentes países por medio del flujo de información que nace a partir de los datos compartidos entre los usuarios del internet, lo cual inhibe a los Estados de ejercer sus derechos soberanos.

En materia bursátil podríamos mencionar el caso de la firma electrónica, misma que por su naturaleza y la contante globalización que afrontan todos los Estados en el mundo, era necesario que en El Salvador se legislase en pos de favorecer a las nuevas relaciones mercantiles originadas a partir del uso de las redes informáticas.

En materia pública podríamos mencionar el caso de la Ley de Acceso a la Información Pública[25], en la cual a razón que los habitantes tienen derecho a conocer la información que se derive de la gestión gubernamental y del manejo de los recursos

[25] Decreto nº 534, de 2 de diciembre de 2010. Ley de Acceso a la Información Pública. (Diario Oficial número 70, tomo nº 371, de 8 de abril de 2011)

públicos, fue necesario de servirse de los sistemas informáticos a fin de facilitar la información a la población en general, con el fin de fomentar la transparencia en las diferentes esferas de poder estatal.

En cuanto al ámbito del Derecho Penal, el ejemplo más palpable en este caso, es el de la Ley de Delitos Informáticos y Conexos, en la cual el espíritu que le quisieron impregnar los legisladores, es el de proteger bienes jurídicos (los cuales pueden ser de índole patrimonial, personal e incluso a la administración pública), que debido al avance tecnológico, generó nuevas formas de afectación a los mismos, por lo que era necesario crear un cuerpo legal actualizado que protegiese a la población en general, de las posibles vulneraciones a sus derechos frente a la era digital que atraviesa El Salvador.

La crítica realizable al régimen jurídico informático de El Salvador, es la precariedad existente respecto a la regulación de los contenidos vertidos por los usuarios cibernéticos en la red de redes, es decir, que no existe como tal una ley que explícitamente regule a aquellos sitios web con contenido altamente cuestionables, ni al flujo de información generado por los cibernautas.

Si bien es cierto que la Ley de Delitos Informáticos y Conexos, trate de dar cierta regulación a contenidos de carácter erótico o pornográfico (y en casos graves, implique a menores de edad), en si no da una solución para detener el consumo de este contenido, más allá de cumplir una función represiva, al tratarse de la tipificación de conductas delictivas y que muchas veces, ni si quiera cumple su función reparadora, debido al daño masivo que puede generar la interconectividad del ciberespacio.

En cuanto a las telecomunicaciones, en el Estado salvadoreño existe la Dirección General de Espectáculos Públicos de Radio y Televisión perteneciente al Ministerio de Gobernación, quienes son los encargados de analizar los contenidos que serán difundidos a través de estos medios, otorgándoles una clasificación, en relación al tipo de población a la cual está dirigida la programación o el mensaje enviado por los particulares e incluso por el mismo Estado.

Muchas veces el rol de control que debe cumplir el Estado, con respecto a los contenidos explícitos existentes en la web, queda relegado a los protocolos y directrices ya establecidos en los proveedores de internet, e incluso en las mismas páginas web.

## 7.1 MECANISMOS DE CONTROL CIBERNETICOS IMPLEMENTADOS POR LOS PROVEEDORES DE SERVICIOS DE INTERNET.

Los mecanismos de control de los proveedores de internet, nacen a partir de la compra de un dominio de internet (.com; .net; .onion; entre otros). El dominio es el nombre exclusivo que se asigna a un sitio web**.** Esta es la manera de identificar y traducir la dirección IP, facilitando la posibilidad de encontrarla en Internet. No obstante, para que la página web sea visible es necesario contar con otros elementos más allá del dominio. Estos son el alojamiento o hosting y el servidor.

Mientras que el **dominio** es el nombre de la web, el **alojamiento** es el lugar dónde se encuentra almacenada. Dominio y alojamiento son dos conceptos ligados estrechamente entre sí por lo que es importante saber diferenciarlos correctamente. Cuando se va a registrar un dominio en Internet se debe tener en cuenta que es necesario contratar un hosting para que el sitio web sea visible en el futuro. Sin hosting, no hay web, a pesar de que se tenga el mejor dominio del mundo.

Por otro lado, el **servidor** es la máquina (ya sea física o virtual) en la que se encuentra el espacio de alojamiento. El dominio está dirigido a un servidor DNS y se relacionan entre sí mediante direcciones IP. Al asignar al dominio una dirección IP se podrá visualizar la página web al escribir en el navegador el nombre elegido.

El **registro de dominios** es el proceso por el cual personas, empresas, organizaciones sin ánimo de lucro o educativas, organismos internacionales o gobiernos, solicita el registro de un nombre de dominio a cambio de pagar una cierta cantidad de dinero y cumplir determinado procedimiento administrativo ante un registrador.

Si es concedido, el solicitante contará con el control de dicho nombre y será responsable de su buen uso en la red internet. Estos registros tienen un período de validez

que puede ser renovado indefinidamente por el registrador. Si no es renovado, dicho registro queda liberado para que cualquier registrador inicie el proceso de registro.

Los registros realizados por gobiernos u organismos internacionales, están limitados a este tipo de instituciones y en algunos países también las organizaciones sin ánimo de lucro y educativas.

Dichos dominios siempre estarán sujetos a ciertas normas, que, dependiendo del proveedor, deben cumplir con fin de que no sea revocada la propiedad del dominio web, e incluso se evite la eliminación total de la página web de internet. Por otro lado, existen cierto tipo de empresas que sirven como intermediarias con el fin de mantener en el anonimato a la persona o institución dueña del dominio web.

Esto último genera la problemática respecto a la regulación del flujo de información, debido a que los proveedores que ofrecen ocultar información de las personas o instituciones titulares de los dominios web, se escudan en el hecho de que cada quien es responsable de los actos que realiza mediante el anonimato.

Por otro lado, redes informáticas convencionales como Facebook, Twitter o YouTube, tienen un sistema de selección de información, que, hasta cierto punto, es efectivo a la hora de eliminar contenido de dudosa reputación; asimismo cuentan con un conjunto de normas comunitarias, que armonizan las relaciones de los usuarios virtuales respecto a otros cibernautas.

## 8. RIESGOS DEL INTERNET PARA LOS NIÑOS NIÑAS Y ADOLESCENTES EN EL SALVADOR

Actualmente se hace más fácil el acceso, asimismo las herramientas digitales, debido al uso masivo de redes sociales por parte de los menores, donde encuentran una forma de interactuar muy diferente a la realidad misma, donde pueden ser quienes quieran ser. Es así que crean personajes en el mundo digital, *“el proceso por el cual los niños*

*interiorizan la estructura social (socialización) se lleva a cabo en los distintos espacios sociales en los que interactúan: uno de ellos es el internet"*[26]

De este postulado se entiende que ellos adoptan la apariencia física que deseen, o se comunican con cualquier persona desconocida sin el control debido de sus padres. Los niños que llegan a familiarizarse con el mundo digital, pueden llegar a la pre-adolescencia con plena consciencia del uso de medios electrónicos para la socialización, ya que a corta edad sus padres les proporcionan dispositivos móviles para su entretenimiento

Los niños representan una buena parte de los usuarios de internet con un fuerte uso en diversión, entretenimiento, tareas y para mantenerse en contacto con sus amigos, el número de niños que usan Internet se incrementan día a día, debido a la facilidad de acceso desde los centros escolares y desde su propia casa y con cualquier dispositivo móvil con conexión a internet, en algunos casos sin ningún tipo de regulación de horarios

Asimismo, el contenido multimedia no es del conocimiento de los padres, puesto que en muchas ocasiones no prestan mayor interés a este tipo de detalles. Debido a la diversidad de contenido disponible en la red, se pueden ver publicaciones inapropiadas de los amigos o de los amigos de los amigos en las redes sociales, y se pueden ser marcados o etiquetados en las fotografías.

Aunado a lo anterior, algunos menores de edad consideran de forma errónea al total de amigos en Facebook y su interacción, como una medida de aceptación por parte de todo el conglomerado de personas agregadas en redes sociales y confunden la idea del valor interpersonal, el conjunto de percepciones y la valía de la autoestima lo consideran proporcional con la popularidad en cuanto a la interacción.

Cabe destacar que "*En internet los niños, niñas y adolescentes experimentan roles sociales y van actualizando la imagen que tienen de sí mismos. Internet es un espacio que hace las veces de "la calle" o la "placita", de ese lugar público donde los adultos no dominan la interacción y donde los adolescentes sociabilizan y se definen a sí mismos en*

[26] Piscitelli, 2,006:182

*conjunto como su tribu, a su banda, a sus iguales. Es en esta interacción del espacio que hace propio donde se refuerza la identidad individual de las y los adolescentes.*

*En este espacio propio, de pertenencia con sus pares, donde comienza a tomar fuerza la identidad individual de los y las adolescentes. La interacción es el centro de interés y por eso los últimos cambios en las tecnologías y en sus aplicaciones, son cada vez más atractivos y relevantes para ellos"*[27]. Existen diferentes riesgos a los cuales los menores se exponen cuando interactúan en el internet en El Salvador, se presentan las siguientes:

a) Acceso de los niños a información de contenido inapropiado y nocivo: *"Existen webs que pese a contener información científica, pueden resultar inapropiadas y hasta nocivas* (pueden afectar a su desarrollo cognitivo y afectivo) *para niños por el modo en el que se abordan los temas o la crudeza de las imágenes"*[28] (sexo, violencia, drogas, determinados relatos históricos y obras literarias...). La multi-medialidad de Internet puede hacer estos contenidos aún más explícitos e impactantes.

b) El Acceso a información con contenido peligroso, inmoral e ilícito: "*Existe información poco recomendable (pornografía infantil, violencia, todo tipo de sectas...) y hasta con contenidos considerados delictivos que incitan a la violencia, el racismo, la xenofobia, el terrorismo, la pedofilia, el consumo de drogas, participar en ritos satánicos y en sectas ilegales, realizar actos delictivos"*[29]

c) Revelación de información: "*Ya sea de forma consciente, en una conversación de chat o en una red social, o inconscientemente, a través de engaños (estafas, falsas ofertas, sorteos o regalos)"*[30]. El menor de edad puede revelar información susceptible, personal o familiar, sin darse cuenta del alcance de la revelación de ello, asimismo el uso de aplicaciones o software que proporcionen la ubicación del menor facilitan la vulneración y la exposición para ser potenciales víctimas de algún ilícito.

---

[27] Explotación sexual comercial de los niños niñas y adolescentes, Instituto Interamericano del niño, la niña y adolescentes (INN), Organismo especializado de la OEA, de pág. 12

[28] https://sites.google.com/site/riesgosalusarinternet/home/tipos-de-riesgos

[29] http://wwwriesgos.blogspot.com/2017/03/acceso-informacion-peligrosa-inmoral.html

[30] https://www.aulaplaneta.com/2015/11/20/en-familia/cinco-peligros-para-los-menores-en-internet-y-como-prevenirlos/

A continuación, se presentan los resultados de una investigación realizada en esta región por la fundación Paniamor (2009), llamado: **"Adolescencia, Ciberespacio-Comunicación Mediada por Computadora y Violencia"** realizado en El Salvador, aporta elementos relevantes:

- *"Se reconoce la existencia de Violencia Social*[31] *en los espacios virtuales que frecuentan los niños, niñas y adolescentes, aunque las investigaciones se centren en las diferentes modalidades de violencia interpersonal, principalmente de carácter sexual y/o emocional.*

- *Se identifican expresiones de violencia en las que las personas menores de edad juegan un rol importante como receptores, pero también como productores y propagadores de violencia.*

- *Se reconocen las siguientes formas de violencia interpersonal: pornografía infantil, Morphing, Grooming o solicitación sexual, Flaming, Cyberbullying, exposición a contenido no deseado, Spamming y Robo y Fraude virtual.*

- *Señalan una tendencia creciente en las y los adolescentes a manifestar comportamientos sexuales riesgosos en sus interacciones a través de comunicación mediada por computadora. Entre estos comportamientos sobresale el Sexting, práctica asociada con la pornografía infantil sin mediación aparente de terceros.*

- *Destacan el alcance y potencial de influencia en el proceso de socialización de los y las adolescentes de este nuevo contexto. En las investigaciones analizadas esto se asocia con características propias del entorno virtual: mayor alcance geográfico, accesibilidad, permanencia indefinida, de material nocivo y /o ilegal, acceso indiscriminado y no cuantificable a personas menores de edad, anonimato, asi como la débil regulación de comportamientos inadecuados y la impunidad como consecuencia.*

[31] Violencia Social: A*cto con impacto social que afecta que atenta a la integridad física, psíquica o relacional de una persona o de un colectivo, siendo dichos actos llevados a cabo por un sujeto o por la propia comunidad. https://psicologiaymente.com/social/violencia-social*

- *Recalcan la ausencia de acompañamiento de adulto o bien la ineficacia de su intervención, lo cual aparece asociado al desconocimiento de los usos que las personas menores de edad hacen de la web y el desconocimiento general de las TIC. Esta situación propicia que las personas adultas pierdan su poder como referentes en el proceso de acompañamiento de las y los adolescentes con respecto al tema y en el establecimiento de límites en el uso del internet y acceso a contenidos. Esto le sucede tanto a padres como a educadores y a otros referentes adultos.*

- *Las investigaciones hacen mayormente hincapié en las conductas riesgosas en las que se colocan los y las adolescentes, habiendo poca referencia a conductas protectoras. Esto particularmente preocupa a Paniamor (ente investigador), dado que muchas veces son los adolescentes quienes ejercen la violencia sobre sus pares".*

En el Salvador existían programas televisivos matutinos y vespertinos, principalmente juveniles de presentación de videos musicales y de entretenimiento, donde se colocaban mensajitos al pie de la pantalla, con números de celulares de personas, en su mayoría hombres, que declaran tener de 20, 30 o 40 años de edad y desean conocer a mujeres o chicas de 15 años en adelante para iniciar una relación amistosa o de noviazgo. Esta práctica se registra en las radios del país, a toda hora se transmiten, bajo esta modalidad de recepción y derivación de mensajitos vía teléfonos móviles, el mismo tipo de mensajes[32].

Por otra parte, se han identificado en El Salvador dos direcciones Web que son utilizadas por tratantes de para contactar niños, niñas y adolescentes. En estas páginas web se ofrecen plazas para edecanes, o para realizar trabajos en casas en el extranjero, cubriendo los gastos completos de documentación, transporte y alimentación. Se ha registrado también el uso de redes sociales como Hi5, Facebook, entre otros, donde los tratantes suben perfiles falsos.

Luego de escoger a su futura víctima, se hace amigo de ellas, las investiga por medio de sus contactos que la propia víctima ofrece; los tratantes utilizan fuentes abiertas en internet, les piden el número de celular y de teléfono fijo luego de haber generado

[32] Fuente: Esudio de Explotación Sexual Comercial de Niños, Niñas y Adolescentes

confianza en la red social, llaman constantemente para sacar información a través de la ingeniería social[33].

Cuando tiene suficiente información de la víctima y de la familia, conciertan citas de trabajo donde les manifiestan a las víctimas que si no se van con ellos matarán a sus familias; según el Departamento de Delitos Tecnológicos- Interpol El Salvador, se han registrado un sinnúmero de casos de este tipo. El Instituto para el Desarrollo Integral de la Niñez y Adolescencia (ISNA) contabiliza por mes y por año los casos atendidos por Explotación Sexual Comercial de Niños, Niñas y Adolescentes.

Esta información es recogida y procesada por el Sistema de Información para la Infancia (SIPI), creando una base de datos electrónica que permite desagregar indicadores por edad, sexo, escolaridad, re victimización, procedencia, nacionalidad y tiempo de estadía bajo jurisdicción de una institución que brinde medidas de protección[34].

## 9. MATERIAL DE CONTENIDO EXPLICITO

Según el Diccionario de la Real Academia Española define explicito como *"aquello que expresa algo con claridad y determinación";* Esto es, cuando algo es explícito puede ser apreciado de forma evidente y sin ambigüedades.

La noción de explicito suele utilizarse con frecuencia para calificar los contenidos de películas, programas de televisión, música, obras, entre otros. De esta manera es posible diferenciar entre el contenido que sugiere determinadas situaciones de aquel que exhibe las acciones de forma directa o hace alusión a esas acciones de forma directa.

Si bien es cierto que el término explícito no se refiere de forma exclusiva al contenido que resulta nocivo para el consumo de cierto grupo de la población, siendo este los niños, niñas y adolescentes; por regla general, cuando se emplea la categoría de contenido explicito refiérase a aquel no apto para el consumo de ellos.

Teniendo en cuenta lo anterior el material de contenido explicito como aquel contenido multimedia o información que exprese de forma directa situaciones que resulten

[33] Ingeniería social: Es la práctica de obtener información confidencial a través de la manipulación de usos legítimos.

[34] Fuente: Estudio de Explotación Sexual Comercial de los Niños, Niñas y Adolescentes, Organización de lo Estados Americanos

dañinas al consumo de determinado sector de la población y, en especial, a los niños, niñas y adolescentes.

## 9.1 MATERIAL PORNOGRÁFICO DENTRO DEL CIBERESPACIO.

De acuerdo a las definiciones universales respecto de la pornografía, debe entenderse como la exhibición de contenidos sexuales en forma obscena con la finalidad de excitar al destinatario. La pornografía es la mera exhibición de genitales y de actos sexuales en cualquiera de sus formas.

En efecto la pornografía es la explotación ruin de los seres humanos y, principalmente de las mujeres. En efecto, la pornografía es una actividad que deforma, la psiquis humana además tiene una amplia correlación entre los delitos en contra de la libertad sexual de los individuos ya que dentro de este contenido fomenta actos como: la violación, agresión sexual, abuso de menores, entre otros.

El impacto negativo de la pornografía se maximiza en las mentes menos desarrolladas tales como de los niños, niñas y adolescentes. En este sentido es conveniente entonces dificultarle las posibilidades de corromper a la niñez y adolescencia, restringiendo su promoción comercial.

Hasta hace pocos años hablar de riesgos frente a la televisión y riesgos en internet eran cuestiones diferentes. Sin embargo, el fenómeno de convergencia mediática actual está llenando la separación que existía entre ambos medios, y cada vez son más los contenidos audiovisuales que, en formato digital, se ofrecen a través de internet.

La difusión de contenidos audiovisuales potencialmente perjudiciales a través de este medio, al igual que para el cine, el video, o la televisión, debe estar sujetos a ciertos límites y cautelas para salvaguardar a los menores, y por tanto, resultaría preocupante que en este momento, en que los menores cuentan con un acceso abierto a Internet, los poderes públicos los dejaran sin protección y sin asistencia a los padres y tutores.

### 9.1.1 PORNOGRAFIA INFANTIL (CHILDPORN)

No existe una opinión unánime a la hora de definir el término pornografía infantil pues la misma va a estar sujeta a multitud de observaciones cuyo contenido es necesario delimitar.

Tradicionalmente se ha considerado a la pornografía ejercida sobre menores una tipología o manifestación de otras conductas delictivas como, por ejemplo, la explotación infantil y la trata de personas, sin embargo, este primer término según la declaración marco en su artículo dos, referente a las infracciones relativas a la explotación sexual de los niños nos define la explotación infantil como:

*"a) coaccionar a un niño para que se prostituya o participe en espectáculos pornográficos, o lucrarse con ello o explotar de cualquier otra manera a un niño para tales fines; b) captar a un niño para que se prostituya o participe en espectáculos pornográficos; c) practicar con un niño actividades sexuales recurriendo a alguno de los medios siguientes: i) hacer uso de la coacción, la fuerza o la amenaza, ii) ofrecer al niño dinero u otras formas de remuneración o de atenciones a cambio de que se preste a practicar actividades sexuales, iii) abusar de una posición reconocida de confianza, autoridad o influencia sobre el niño"*[35].

Del mismo modo, en segundo término, también ha sido calificada como una exteriorización de la trata de seres humanos la cual, como señala expresamente la Asamblea General de Naciones Unidas, es:

*"la abducción, el transporte, el traslado, el cobijamiento o la recepción de un niño o el ofrecimiento de pago u otros beneficios para lograr el consentimiento de una persona a cuyo cargo esté un niño para los fines señalados en el párrafo 2 supra, así como con el*

[35] Artículo 2 Decisiones marco bajo la rúbrica "*Infracciones relacionadas con la explotación sexual de los niños"*

*objeto de utilizar, adquirir u ofrecer a un niño para la explotación sexual, incluida la producción de pornografía, o para que preste servicios pornográficos"*[36].

Bajo la perspectiva de Naciones Unidas, la pornografía infantil ha sido definida como:

*"toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales"*[37].

Tomando en cuenta la definición ad supra debemos entender que estamos frente a pornografía infantil en las siguientes situaciones:

a) Cuando el material presente a un niño real practicando o participando en un acto sexualmente explicito que incluya la exhibición de los genitales de un niño;

b) A una persona real que se presuma o parezca ser un niño perpetrando las acciones mencionadas en el literal a);

c) Imágenes simuladas de un niño realizando conductas inequívocamente de carácter sexual explícito en el cual se exhiba las partes íntimas del niño o niña con fines meramente sexuales.

## 10. CONVENCIÓN INTERAMERICANA DE LOS DERECHOS DEL NIÑO

La convención habla del respeto que se le debe dar al derecho de libertad de expresión que tienen todos los niños, así mismo; dice que ese derecho incluye la libertad de buscar, recibir y difundir informaciones e ideas de todo tipo, sin consideración de fronteras, ya sea oralmente, por escrito o impresas, en forma artística o por cualquier otro medio elegido por el niño.

[36] Véase, Nota de la Oficina del Alto comisionado de las Naciones Unidas para los Derechos Humanos, el Fondo de las Naciones Unidas para la Infancia y la Organización Internacional para las Migraciones sobre los proyectos de protocolo relativos al tráfico de migrantes y la trata de personas (A/ AC.254/27).

[37] Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía Asamblea General - Resolución A/RES/54/263 del 25 de mayo de 2000; artículo 2 literal c).

Lo anterior sin pasar por encima de ciertas restricciones que promueven el respeto a los derechos y reputación de los demás, la protección de la seguridad nacional o el orden público o para proteger la salud o la moral públicas. Así mismo prohíbe las intromisiones arbitrarias que afecten la honra y reputación de los niños porque menoscaban la integridad de los mismos.

Se sabe que los medios de comunicación desempeñan una función importante y se debe velar por que los niños tengan acceso a materiales e información de carácter nacional o internacional siempre y cuando tengan que ver con su bienestar social, espiritual, moral así como también su salud física y mental; por ende, se alienta a los medios a producir y difundir ese tipo de información.

La Convención establece que *"…a los niños impedidos física o mentalmente debe dárseles un trato especial donde se resguarden sus derechos mientras goce de una vida plena en la que se respete su dignidad y logre la integración social y el desarrollo individual, incluido su desarrollo cultural y espiritual, en la máxima medida posible mediante la cooperación internacional mediante el intercambio de información respecto de su salud…"*[38]

Se prohíbe la prostitución infantil porque se debe proteger a los niños contra la explotación económica o de trabajos que resulten nocivos para su salud física y mental, espiritual, moral y social mediante la adopción de medidas legislativas, administrativas, sociales y educacionales que respalden el pleno goce de las garantías constitucionales de los niños.

Existe el compromiso de los Estados Partes de proteger al niño contra todas las formas de explotación y abuso sexual, tomando las medidas adoptadas para erradicar el secuestro y la venta o la trata de niños para cualquier fin, aunadas a las que se enfocan en la recuperación física y mental de los niños que han sido sometidos a maltratos, abandono, explotación, abuso, tortura o penas crueles.

[38] https://www.un.org/es/events/childrenday/pdf/derechos.pdf

## 11. PROTOCOLO FACULTATIVO DE LA CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO RELATIVO A LA VENTA DE NIÑOS, PROSTITUCIÓN INFANTIL Y LA UTILIZACIÓN DE NIÑOS EN LA PORNOGRAFÍA

Los Estados Partes crearon este protocolo para darle mejor cumplimiento a la Convención Interamericana de los Derechos del Niño, haciendo énfasis en el objetivo de garantizar la protección de los menores contra la venta de niños, la prostitución infantil y la utilización de niños en la pornografía debido a la creciente trata internacional de menores para los fines mencionados.

Lo anterior debido a la profunda preocupación por la práctica difundida y continuada del turismo sexual, a la que los niños son especialmente vulnerables ya que fomenta directamente la venta de niños, su utilización en la pornografía y su prostitución, reconociendo que algunos grupos especialmente vulnerables, en particular las niñas, están expuestos a un peligro mayor de explotación sexual.

*"…La disponibilidad de pornografía infantil es cada vez mayor en Internet y otros medios tecnológicos modernos, en las conclusiones de la Conferencia Internacional de Lucha contra la Pornografía Infantil en la Internet (Viena, 1999) se pidió la penalización en todo el mundo de la producción, distribución, exportación, transmisión, importación, posesión intencional y propaganda de este tipo de pornografía…"*[39]

Resultaría más fácil erradicar la venta de niños, la prostitución infantil y la utilización de niños en la pornografía si se adopta un enfoque global que permita hacer frente a todos los factores que contribuyen a ello, en particular el subdesarrollo, la pobreza, las disparidades económicas, las estructuras socioeconómicas no equitativas, la disfunción de las familias, la falta de educación y la migración del campo a la ciudad.

Y otros no menos importantes como la discriminación por motivos de sexo, el comportamiento sexual irresponsable de los adultos, las prácticas tradicionales nocivas, los conflictos armados y la trata de niños, estimando que se deben hacer esfuerzos por

[39] https://www.ohchr.org/SP/ProfessionalInterest/Pages/OPSCCRC.aspx

sensibilizar al público a fin de reducir el mercado de consumidores que lleva a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.

Estimando también que es importante fortalecer la asociación mundial de todos los agentes, así como mejorar la represión a nivel nacional, tomando nota de las disposiciones de los instrumentos jurídicos internacionales relativos a la protección de los niños, ya que se tienen más de un convenio y convenciones que ayudan en gran manera a que la erradicación de dicho problema tenga más eficacia.

*"…La Convención sobre los Derechos del Niño goza de un inmenso apoyo que se demuestra a través de adhesión generalizada a la promoción y protección de los derechos del niño, reconociendo la importancia de aplicar las disposiciones del Programa de Acción para la Prevención de la Venta de Niños, la Prostitución Infantil y la Utilización de Niños en la Pornografía…"*[40]

# MARCO JURIDICO

## 1. NOCIONES INTRODUCTORIAS.

Según Hans Kelsen (1,881-1,973), jurista Austriaco nacionalizado estadounidense, establece que el ordenamiento jurídico está constituido por un sistema de normas jurídicas en el que dependen de una norma superior situando unas sobre otras sin que las inferiores contradigan a las superiores, cuya cúspide es la constitución política de un Estado, como una norma suprema del sistema normativo del referido Estado, la cual prevalece sobre cualquier otra ley, tratado, reglamento, ordenanza o decreto.

Los elementos que conforman la pirámide de Kelsen en nuestro sistema jurídico salvadoreño son los siguientes: 1. La Constitución de la República; 2. Tratados Internacionales; 3. Leyes secundarias y leyes especiales; y, 4. Decretos, reglamentos y ordenanzas municipales. Dicha clasificación es importante para poder entender eficazmente el conjunto de normas jurídicas utilizadas para esta investigación.

[40] https://www.ohchr.org/SP/ProfessionalInterest/Pages/OPSCCRC.aspx

## 2. CONSTITUCIÓN DE LA REPÚBLICA DE EL SALVADOR.

La Constitución de la República de El Salvador, constituye la norma fundamental y suprema, lo dicho anteriormente queda consagrado en su artículo 246 inc. 2 que señala: "La Constitución prevalecerá sobre todas las leyes y reglamentos...". Asimismo, los artículos 144 y 145Cn., establecen que los Tratados internacionales son leyes de la república, pero cuando estos entren en conflicto con otras leyes prevalecerán sobre las mismas, sin que alteren, restrinjan o afecten por ningún motivo las disposiciones establecidas en la constitución.

### LA PERSONA HUMANA Y SU IMPORTANCIA DENTRO DEL ESTADO SALVADOREÑO (Ámbito de Aplicación Art. 1 C.N).

En la referida norma se consignan los diferentes derechos individuales que posee la persona humana dentro de la sociedad salvadoreña, puntualizando en los derechos concernientes a la vida, y entre otros; además se establecen los tres fines del Estado, como lo son: la Justicia, la Seguridad Jurídica y el Bien Común. En este artículo se establecen, además, las garantías y libertades que tienen los individuos, y la protección que gozan frente al Estado.

### EL ESTADO COMO GARANTE DE BIENES JURÍDICOS PARA LA PERSONA HUMANA (Ámbito de Aplicación Art. 2 C.N)

La persona humana es el eje central dentro del Estado salvadoreño, a la cual se le deben garantizar una amplia gama de bienes jurídicos, entre ellos están el honor, la intimidad personal y familiar, entre otros.

A raíz de lo mencionado, es necesario decir que, la sociedad salvadoreña atraviesa en estos momentos una revolución tecnológica, lo cual ocasiona que las relaciones interpersonales evolucionen a pasos agigantados; es por ello que el ordenamiento jurídico debe mutar constantemente para no descuidar garantías constitucionales que puedan verse vulneradas por estos tipos de cambios.

### LA LIBERTAD DE EXPRESIÓN Y LA CENSURA (Ámbito de Aplicación Art. Art. 6 Inc. 1° y 6° C.N)

A todo individuo dentro de la República de El Salvador se le garantiza constitucionalmente el Derecho a la Libre Expresión, en todas sus formas, a excepción de que este vulnere o contribuya nocivamente al orden público de la sociedad, o bien sea utilizado para dañar la moral, el honor y la vida privada de otra persona.

**EL DERECHO DE LIBRE ASOCIACIÓN (Ámbito de Aplicación Art. Art. 7 C.N)**

Toda persona tiene derecho a asociarse libremente, siempre y cuando se realice dentro del marco legal, lo cual en la actualidad es ejercido por la sociedad mayormente a través del ciberespacio.

En cuanto a la libertad de prensa la constitución da plena garantía sobre la base de la opinión publicada de las empresas que proveen estos productos; en el ciberespacio la distribución de la información puede transmitirse en tiempo real y las publicaciones de los periódicos digitales cada vez tienen mayor notoriedad, dando mayor cobertura tomando en cuenta el nivel de acceso que tienen los ciberusuarios salvadoreños.

**LA PROHIBICIÓN DE LA INTERVENCIÓN DE LAS TELECOMUNICACIONES (Ámbito de Aplicación Art. 24 Inc. 2° y 3° C.N)**

Existe una expresa prohibición acerca de la interferencia y la intervención de las telecomunicaciones y de la correspondencia, sin embargo, de manera excepcional se podrán intervenir en un Proceso judicial mediante autorización de un juez de forma escrita y fundamentando las razones por las cuales es necesario acceder al contenido.

**APOYO DEL ESTADO SALVADOREÑO AL AVANCE CIENTÍFICO Y TECNOLÓGICO (Ámbito de Aplicación Art. Art. 53 C.N)**

El Salvador también está obligado apoyar el avance tecnológico que produzca el conglomerado social, esto incluye los avances informáticos, que al ser nuevas invenciones necesitan cierto tipo de regulaciones especial, debido a que los ordenamientos jurídicos

convencionales no siempre abarcan los fenómenos contemporáneos producto del avance científico.

## 3. TRATADOS INTERNACIONALES

Los Tratados Internacionales los cuales estén suscritos por El Salvador, al momento de estar suscritos pasan a ser leyes de la República, así como también son una herramienta para aplicarse en conjunto con otras leyes, con fin de suplir ciertos vacíos legales que puedan surgir.

### 3.1 PROTOCOLO FACULTATIVO DE LA CONVENCIÓN DE LOS DERECHOS DEL NIÑO RELATIVO A LA VENTA DE NIÑOS; PROSTITUCIÓN INFANTIL Y LA UTILIZACIÓN EN LA PORNOGRAFÍA

Suscrito el 13 de septiembre de 2002, Aprobado el 22 de noviembre de 2002 mediante Acuerdo Ejecutivo Nº 1033, Ratificado el 25 de febrero de 2004 mediante Decreto Legislativo Nº 280, Sancionado por la Presidencia de la República el 4 de marzo de 2004 y Publicado en el Diario Oficial Nº 57, Tomo Nº 362 del 23 de marzo de 2004. Ratificado en todas sus partes, pero expresándose una Declaración referida a la Extradición.

Este Protocolo constituye un instrumento clave en la readecuación de la legislación nacional de acuerdo a la Convención sobre los Derechos del Niño y en la implementación efectiva de la misma.

**PROTECCIÓN DE LOS MENORES DE EDAD FRENTE A LA PORNOGRAFÍA INFANTIL (Ámbito de Aplicación Art. 1 Protocolo Facultativo)**

Entrando en armonía con el ordenamiento jurídico vigente de la legislación salvadoreña, la citada normativa vendría a fortalecer los ataques en contra de las conductas atentatorias a la integridad de los infantes; abarcando asimismo las redes de pedofilia contenidas en algunas regiones oscuras del ciberespacio.

**PROMOCIÓN DE POLÍTICAS ESTATALES EN CONTRA DE LA PORNOGRAFÍA INFANTIL (Ámbito de Aplicación Art. 9 Cláusula 2. Protocolo Facultativo)**

El Estado salvadoreño está obligado a implementar programas sociales destinados a la concientización del público en general, por a través de medios apropiados, en lo relativo a la prevención de los delitos relacionados con la pornografía infantil, asimismo de los efectos perjudiciales ocasionados a las víctimas.

## 3.2 TRATADO DE LA ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL -OMPI-, SOBRE EL DERECHO DE AUTOR -WCT- 1,996

Ratificado por la República de El Salvador según el Decreto Legislativo número 322, del 11 de junio de 1,998, publicado en el D.O. Nº 121, Tomo 340, del uno de julio de 1,998. Es un arreglo particular adoptado en virtud del Convenio de Berna que trata de la protección de las obras y los derechos de sus autores en el entorno digital.

Además de los derechos reconocidos en el citado Convenio de Berna, se conceden determinados derechos económicos. El Tratado también se ocupa de dos objetos de protección por derecho de autor: i) los programas de computadora, con independencia de su modo o forma de expresión, y ii) las compilaciones de datos u otros materiales ("bases de datos").

## LOS PROGRAMAS DE ORDENADOR Y LOS DERECHOS DE AUTOR (Ámbito de Aplicación Art. 4 Tratado OMPI)

En virtud de la normativa citada, El Salvador reconoce que cualquier programa de ordenador, independientemente de su modo o forma, gozara plenamente de la protección de Derechos de Autor.

## LAS BASES DE DATOS INFORMÁTICOS (Ámbito de Aplicación Art. 5 Tratado OMPI)

Las bases o compilaciones de datos, pueden considerarse, dependiendo de disposición de contenidos, creaciones de carácter intelectual, en consecuencia, debe ser protegidas por los Derechos de Autor correspondientes.

## 4. LEYES SECUNDARIAS

Las leyes secundarias están subordinadas a una ley suprema, en este caso se someten a la Constitución de la Republica; estas normas jurídicas poseen una jerarquía

inferior, estas leyes son las que dan nacimiento a deberes jurídicos y derechos subjetivos. Las leyes secundarias desarrolladas en la presente investigación son las siguientes:

## 4.1 LEY DE TELECOMUNICACIONES

La Ley de Telecomunicaciones publicada en el Diario Oficial No. 218 Decreto 142 emitida el 06 de noviembre de 1997 tiene por objeto regular las actividades del sector telecomunicaciones, servicio público de telefonía, recursos esenciales y plan de numeración; lo anterior de conformidad con el articulo No. 110 de la Constitución, es deber del Estado regular y vigilar los servicios públicos, así como aprobar sus tarifas. La entidad responsable de aplicar y velar por el cumplimiento de las normas y regulaciones establecidas en esta Ley y su reglamento es la Superintendencia General de Electricidad y Telecomunicaciones.

### CONCESIÓN DE LA EXPLOTACIÓN DEL ESPECTRO RADIOELÉCTRICO (Ámbito de Aplicación Art. 7 Ley de Telecomunicaciones)

En El Salvador impera el respeto del Estado de derecho como un orden en el cual las leyes impuestas son respetadas en igualdad de condiciones y obligaciones contenidas en leyes y códigos previamente divulgados, esa así que se establece la concesión para la explotación del espectro radioeléctrico por parte de las empresas privadas; establece este mismo artículo las causales de revocación y la extinción de la explotación del servicio público.

### ENTIDAD TITULAR Y DIVISIÓN DEL ESPECTRO RADIOELÉCTRICO (Ámbito de Aplicación Art. 9 Ley de Telecomunicaciones)

Este artículo establece que el espectro radioeléctrico es propiedad del Estado salvadoreño, siendo un bien público pueden concederse los permisos de explotación del mismo a través de las operadoras de telecomunicaciones; asimismo establece que la institución responsable de la administración en sus diferentes facetas es la Superintendencia General de Electricidad y Telecomunicaciones, institución a la cual se le otorga la responsabilidad y la representación internacional en lo que respecta a la coordinación con los diferentes países del espectro radioeléctrico.

En cuanto a la división de frecuencias estas funcionan para evitar las interferencias entre las diferentes operadoras, es decir que se colocan en rangos de frecuencias de emisión diferentes, por ejemplo: cada Radiodifusora tiene un nivel de frecuencia de Mega Hertz en FM o AM; siendo una metáfora que el espectro radioeléctrico es una autopista, las frecuencias son los carriles por donde circulan las señales de comunicación.

**DERECHOS DEL CIUDADANO (Ámbito de Aplicación Art. 29 Ley de Telecomunicaciones)**

En el Literal a) se establece que los usuarios tienen derecho a acceder al servicio de telefonía pública y mantener comunicaciones sin interferencias ni intervenciones por parte de cualquier persona o institución, esto en respeto del Derecho de Intimidad Personal consagrado en la constitución en el cual toda persona tiene la facultad de mantener a salvo o en secreto esa parte esencial de información que mantiene apartada de la palestra de la sociedad.

Asimismo el literal d) es una extensión del derecho constitucional de intimidad en cuanto a la confidencialidad de los datos personales de los usuarios; las empresas que prestan el servicio de comunicaciones deben de resguardar con recelo éste tipo susceptible de información, es decir que las empresas no deben hacer uso indebido de ello, aunado a lo anterior es una enorme responsabilidad mantener las bases de datos al resguardo de cualquier ataque cibernético.

**INFRACCIONES MUY GRAVES (Ámbito de Aplicación Art. 34 Literal a) Ley de Telecomunicaciones)**

Este artículo contiene varios literales en cuanto a las infracciones que pudiesen cometer las operadoras de telecomunicaciones y las cataloga como infracciones Muy Graves, la más relevante y relacionada al tema de investigación es la vulneración en cuanto al secreto de la comunicación de los usuarios por parte de la empresa distribuidora del servicio cuando es de forma intencional y sin previa autorización judicial, y que vulnera derechos fundamentales de la persona que recibe el servicio.

**SANCIONES PARA LAS INFRACCIONES MUY GRAVES (Ámbito de Aplicación Art. 38 Ley de Telecomunicaciones)**

En este artículo forma parte del régimen de sanciones a las cuales se hacen acreedoras las empresas de telecomunicaciones previa resolución de las autoridades correspondientes; establece que las multas a las que se hace acreedor quien cometa sanciones muy graves, entre las que se relaciona que la persona que intervenga las comunicaciones del usuario de forma ilegal será sancionada con una multa de cinco mil colones por cada día en que la infracción se cometa.

**SUSPENSIÓN Y REVOCACIÓN DE LA CONCESIÓN (Ámbito de Aplicación Art. 42 Ley de Telecomunicaciones)**

Este artículo establece que las empresas que incumplan con tres o más resoluciones sancionatorias por haber cometido infracciones calificadas como graves o muy graves por la misma Ley, (tal como lo contiene en sus Arts. 37 y 38), y que de forma reiterada las cometan en un período de cinco años, asimismo este artículo establece que si transcurriere el plazo de la suspensión y la empresa concesionaria persiste en el incumplimiento se procederá a la revocación de la concesión por un plazo máximo de dos meses; no obstante, si la operadora de telecomunicaciones logra comprobar el cumplimiento de las resoluciones sancionatorias la suspensión podrá levantarse. Sin embargo, si el concesionario persiste en el incumplimiento, se procederá a la revocación, salvaguardando el derecho de defensa y contradicción previa el desarrollo de audiencia celebrada a la operadora, estas reglas también aplican a las concesiones para la explotación del espectro radioeléctrico.

**OBLIGACIÓN DE COOPERACIÓN CON LAS AUTORIDADES (Ámbito de Aplicación Art. 42 – A. Ley de Telecomunicaciones)**

Este artículo establece que las empresas de las redes comerciales de telecomunicaciones están obligadas a cooperar con el ente acusador como la Fiscalía General de la República o en las Diligencias de investigación de la Policía Nacional civil quienes son los encargados de recabar los indicios o medios probatorios cuando en el ejercicio de sus facultades investiguen delitos.

**FORMAS DE COLABORACIÓN EN LA INTERVENCIÓN DE LAS TELECOMUNICACIONES (Ámbito de Aplicación Art. 42 – B y 42 – C. Ley de Telecomunicaciones)**

Estos dos artículos son herramientas útiles para el combate de los delitos cometidos por medio de las tecnologías de la información y comunicación, puesto que facultan a darle seguimiento a la intervención de los números, direcciones de origen marcación o recepción de llamadas realizadas de teléfono de usuarios que se encuentren bajo investigación personas de interés o relacionadas al hecho investigado, asimismo permite el acceso a las bases de datos de las operadoras para facilitar la identificación de los involucrados en el ilícito penal.

**AUTORIZACIÓN MEDIANTE ORDEN JUDICIAL (Ámbito de Aplicación Art. 42 – D. Ley de Telecomunicaciones)**

Para la intervención de las telecomunicaciones se necesita una autorización judicial de forma escrita en la cual el agente investigador debe de fundamentar los motivos del por qué es necesaria la intervención, lo que intenta probar, los plazos y parte de la teoría fáctica en donde se establezca la participación del(la) imputado(a) al que desean intervenir sus comunicaciones.

**IMPOSICIÓN DE MULTA POR NEGATIVA EN COLABORAR CON LAS INTERVENCIONES (Ámbito de Aplicación Art. 42 – F. Ley de Telecomunicaciones)**

Cuando una empresa de telecomunicaciones se niegue a colaborar con las autoridades, establece este artículo que será sancionada con los montos establecidos en el Artículo 34 de esta misma ley; sin embargo, no será aplicable la disposición de Revocarle la

Concesión para la explotación del servicio público de telefonía; sin embargo, cuando la operadora argumente que no es posible la intervención por motivos técnicos el funcionario encargado de la investigación está facultado para informar a la Superintendencia General de Electricidad y Telecomunicaciones quien deberá resolver en las próximas 24 horas y esta resolución no admite recurso.

## 4.2 LEY ESPECIAL PARA LA INTERVENCION DE LAS TELECOMUNICACIONES

En el año 2010 es aprobada esta Ley en la Asamblea Legislativa, en el Decreto Legislativo No. 285, en el cual se establece como una herramienta de persecución penal contra la delincuencia grave, delincuencia organizada y transnacional, todo con la finalidad de darle legitimidad a la intervención de las telecomunicaciones sin afectar el derecho constitucional de secreto de las comunicaciones establecido en el Art. 24 de la carta magna donde se establece la inviolabilidad de la correspondencia (aplicada en tiempos modernos se interpreta el alcance a las diferentes tecnologías de información y comunicación); en este mismo artículo establece de manera expresa e inequívoca la prohibición de la interferencia de las telecomunicaciones, sin embargo también contiene la excepción a la intervención solamente cuando sea autorizada mediante una orden judicial, en la cual se deberá dejar por fuera toda la información que no sea pertinente o esté relacionada al caso investigado.

A través de esta Ley es que se faculta a la parte acusadora la intervención temporal de las telecomunicaciones haciendo uso de herramientas tecnológicas; siendo esta Ley de vital importancia en la investigación científica del delito, siempre y cuando el ente acusador obtenga la autorización judicial escrita, motivada, con plazos establecidos y la relación de los hechos donde se presume la participación de los involucrados.

### SECRETO DE LAS TELECOMUNICACIONES EN LAS INTERVENCIONES (Ámbito de Aplicación Art. 1. L. E. T)

Se establece como garantía el secreto de las telecomunicaciones y el derecho a la intimidad, exceptuándose cuando dicha intervención sea autorizada misma mediante una orden judicial en la cual el fiscal auxiliar presentará un escrito motivado, donde se hará uso de técnicas necesarias para intervenir cualquier tipo de comunicación.

### DELITOS DE PROCEDENCIA (Ámbito de Aplicación Art. 5. L. E. T)

Tal como lo establece este artículo solamente podrá utilizarse en el cometimiento de dieciséis tipos de delitos y los conexos que resultaren de ello, sin embargo, a criterio de este grupo de investigación solamente se tomaran en cuenta los delitos de a) Homicidio y su forma agravada, b) La Pornografía, utilización de menores de dieciocho años e incapaces o

deficientes mentales en pornografía, y posesión de pornografía y c) Comercio de personas, tráfico ilegal de personas, trata de personas y su forma agravada.

## 4.3 POLITICA DE PERSECUCIÓN PENAL DE LA FISCALÍA GENERAL DE LA REPÚBLICA DE EL SALVADOR

La Fiscalía General de la República constitucionalmente es el ente encargado dela coordinación de la investigación y el ejercicio de la Acción punitiva del Estado en los delitos de acción pública; entonces la política de persecución penal el Fiscal General establece los criterios y lineamientos del marco de la acción institucional para la consecución de fines institucionales

**PROCEDIMIENTO DE INTERVENCIÓN DEL AGENTE FISCAL (Ámbito de Aplicación Art. 33, 26 y 28. Política de Persecución Penal)**

Dentro de su articulado se encuentra la Intervención de las Telecomunicaciones, en la cual los fiscales auxiliares pueden promover dicha técnica como parte de la investigación científica del delito, dicha solicitud se eleva ante las direcciones fiscales correspondientes; esta solicitud se entrega al órgano jurisdiccional quien será el encargado de autorizar dicha diligencia siempre y cuando contenga los requisitos establecidos en la Constitución de la República y de las Leyes especiales establecidas.

Asimismo la Fiscalía General de la República establece dentro de su política de política de persecución penal la Unidades de Atención Especializada para las Mujeres, que también atienden a la niña, niño y adolescentes que hayan sido víctimas de delitos (incluidos los delitos relativos a su intimidad, imagen e indemnidad sexual), incluso si fueren testigos o acompañantes en diligencias de investigación o actos procesales, serán protegidos incluso en el programa de protección de testigos de la Unidad Técnica del Sector Justicia con la finalidad de atender en la medida de lo posible

## 4.4 CÓDIGO PENAL DE EL SALVADOR

Regula los delitos, faltas y sus penas. Así, el derecho penal, se aplica y responde al principio de mínima intervención, que establece que solo debe intervenir en aquellos

hechos más graves que transgreden los bienes jurídicos más importantes de la sociedad, dejando para otras ramas del derecho, las infracciones que no le interesa proteger.

En cuanto al derecho a la intimidad su protección se encuentra, en su título VI denominado delitos relativos al honor y la intimidad, regula en su capítulo II los delitos relativos a la intimidad, la violación de comunicaciones privadas.

Dispone de un catálogo de delitos, que protegen el derecho a la intimidad, entre ellos, el delito de violación de comunicaciones privadas regulado en el artículo 184, se tutela el bien jurídico intimidad, la acción constitutiva de delito que consiste en apoderarse de la comunicación escrita, soportes informáticos, documentos o el medio en que está, el secreto o los datos personales o familiares, es decir que mediante esa intromisión se vulnerara la intimidad de la persona, esta conducta tiene como objetivo descubrir los secretos, en otras palabras aquel conocimiento que pertenece exclusivamente a un número limitado de personas, y el revelar o divulgar a otras personas u otra depende únicamente de la voluntad de estas.

El artículo 185 del mismo cuerpo normativo regula la Violación Agravada de Comunicaciones; este tipo penal contiene una agravación, en cuanto a la calidad del sujeto activo, siempre que ejecuten las conductas descritas en el artículo 184 y tengan la calidad de sujetos encargados o responsables, asimismo el secreto este en un fichero, soporte informático.

El artículo 186 regula el delito de Captación de Comunicaciones, al igual que el delito anterior el bien jurídico protegido por el tipo penal, es la intimidad de la persona. La acción típica se ejecuta al interceptar, impedir o interrumpir una comunicación telegráfica o telefónica o la utilización de medios o artificios medios tecnológicos de escucha, transmisión o grabación del sonido, de la imagen o de cualquier otra señal de comunicación, es decir que incluye los modernos avances tecnológicos en comunicación, como el fax, el internet, lo que implica intrusismo informático, también denominado “hacking”, es decir el acceso sin autorización, a los archivos y bases de datos contenidos en los sistemas informáticos ajenos, aunque por lo general de grandes empresas o instituciones, al acceder sin consentimiento a la información que se considera secreta,

estando en presencia de intrusismo informático, aunque el tipo penal no lo regula expresamente

En cuanto a los delitos relativos a la libertad sexual se encuentran regulados en los artículos 172, 173, 173-A y 173-B del cuerpo legal en cuestión, los cuales están íntimamente relacionados con los delitos contenidos en el capítulo IV de la ley especial contra los delitos informáticos y conexos. Y para efectos de la presente investigación se desarrollan conjuntamente con el análisis de los delitos contenidos en la ley especial.

## 4.5 LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS

En materia penal también se encuentra la Ley Especial Contra los Delitos Informáticos y Conexos, fue creada el 4 de febrero del año 2,016. Así, contiene tres títulos, treinta y seis artículos, en el título I regula las disposiciones generales.

El objeto de la presente ley, según el artículo 1 es la protección los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, entre otros; es de esta manera que en esta ley se introducen los bienes jurídicos denominados“los sistemas informáticos” y “los datos informáticos”

El título II regula los delitos, el capítulo I (Art. 4 al 9 LEDIC) contiene un catálogo de delitos contra los sistemas tecnológicos de información esto es, a los delitos que tienen como finalidad última, explotar las vulnerabilidades de las Tecnologías de la Información e Información de manera tal que causen daños o acceder a datos e información sensible de los usuarios de las TIC’s, dentro de estos tipos penales el legislador busca proteger el bien jurídico de “los sistemas informáticos”.

El capítulo II (Art. 10 al 14 LEDIC) regula los delitos informáticos en este capítulo se regulan aquellas conductas que están tipificadas en el código penal común con la forma especial de cometimiento de las mismas siendo esta, a través de las TIC’s (verbigracia:

estafa informática, fraude informático, espionaje informático, entre otros). En ese sentido, resulta inminente delimitar los casos en los cuales nos encontramos frente a un delito regulado en la normativa penal común y encontrar el elemento diferenciador de los delitos contenidos en la ley especial.

En tal sentido, para establecer si una conducta es susceptible de ser tratada bajo la perspectiva de la normativa penal común debe existir una relación entre dos o más personas: la que comete el delito y la víctima. En este sentido si existe una relación debidamente acreditada entre el sujeto pasivo y el sujeto activo, esta conducta se subsume dentro de la tipificación de delito común; en cambio para ser tratada una conducta bajo la óptica de la ley especial debe existir una intervención en la transmisión de datos, es decir no debe existir una relación directa entre ambos sujetos.

Es así que resulta necesario identificar la manipulación del sistema informático que produzca el resultado que se pretende evitar, "…ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema…" tal como lo establece el artículo 10 de este título.

El capítulo III (Art.15 al 28 LEDIC) contiene los delitos Informáticos relacionados con el contenido de los datos, en estos artículos se tipifican los delitos que tienen que ver con los datos que se almacenan dentro de las Tecnologías de la Información y Comunicación es así, que en este capítulo el espíritu del legislador es proteger el bien jurídico de "los datos informáticos" bien jurídico introducido en el artículo 1 de esta ley.

El capítulo IV (Arts. 28 al 34 LEDIC) tiene el catálogo de delitos informáticos contra niñas, niños y adolescentes o personas con discapacidad; en el artículo 28 (Rel. Art. 172 Pn.) prohíbe cualesquiera formas de facilitación de material pornográfico a niños, niñas, adolescentes o personas con discapacidad que pudiere causar daños a la psiquis de los niños, niñas, adolescentes o personas con discapacidad con el objeto de proteger la integridad sexual de estos sujetos.

Asimismo, el material de contenido pornográfico que fuere a ser distribuido debe advertir que su contenido pudiere resultar nocivo a la integridad de los niños, niñas,

adolescentes o personas con discapacidad; obligando así a los productores de este tipo de material de forma "licita" a introducir esta advertencia al consumidor del material de contenido sexual explícito.

El artículo 29 de la LEDIC (Rel. Art. 173 Pn.) prohíbe cualquier tipo de utilización de niños, niñas, adolescentes o personas con discapacidad independientemente, sea por audio, imágenes estáticas y contenido audiovisual en material de contenido de naturaleza sexual independientemente si este exhibe escenas eróticas de forma explícita o de forma implícita; asimismo sin distinción de si la utilización de estos sujetos fuere real o simulada. Este delito se configura cuando el sujeto activo produce, fabrique, distribuya o facilite material pornográfico en el que se utilice a niños niñas o adolescentes.

En el artículo 30 de la Ley Especial Contra los Delitos Informáticos y Conexos (Rel. Art. 173-A Pn.), el legislador tipifica la acción de poseer material de contenido pornográfico que involucre la utilización de niños, niñas y adolescentes, sin distinción si sujeto poseedor del material de contenido sexual explicito tiene por objeto la distribución de este a terceros; solo con el hecho de la posesión de este material dentro de Tecnologías de la Información y Comunicación (llámese estos computadoras, soportes de almacenamiento USB, DVD, teléfonos celulares, entre otros) estableciéndose como pena para este delito de dos a cinco años de prisión.

En estos casos el Código Penal en el artículo 173-B establece casos en los que el delito de la posesión de material de contenido pornográfico en el cual se utilizaré menores de dieciocho años de edad adquiere la agravante en cualquiera de estos casos:

a) Que las actividades descritas en dichos artículos fueren cometidas por ascendientes, descendientes, hermanos, adoptantes, y parientes que se encuentren hasta en el cuarto grado de consanguinidad y en el segundo grado de afinidad;
b) Que las acciones fueren realizadas por funcionarios públicos, agentes de autoridad, empleados públicos y/o autoridades públicas como lo establece el artículo 39 del código penal;
c) Cualquier persona encargada de la tutela o vigilancia del niño, niña, adolescente o persona con discapacidad; y,

d) Toda persona prevaliéndose de las condiciones de superioridad, confianza, educativa, de trabajo o de cualquier otra relación que genere una condición de superioridad del sujeto activo sobre el sujeto pasivo.

En el caso del artículo 31 de la Ley Especial Contra los Delitos Informáticos y Conexos, regula la Corrupción de niños, niñas, adolescentes o personas con discapacidad a través de Tecnologías de Información y Comunicación; conceptualmente el término " Corrupción de Menores" ha sido problemático en el sentido de ser un término impreciso y por sus referencias moralizantes, desentendiéndose del principio de Taxatividad que exigen las leyes de naturaleza penal; el cual su delimitación de este delito queda en manos del Juzgador y en consecuencia quebranta el principio de seguridad jurídica.

El concepto de corrupción de niños, niñas, adolescentes o personas con discapacidad, puede referirse entonces a un estado en el que se ha deformado el sentido naturalmente sano de la sexualidad, sea por lo prematuro de su evolución o ya sea porque el sujeto pasivo llega a captar como normal la depravación de la actividad sexual. El artículo ad supra no hace una descripción precisa de la conducta que el legislador pretende penalizar sino se limita a establecer una pena para una conducta no delimitada y, como se mencionaba en el párrafo que antecede, deja en manos de la autoridad judicial la delimitación de la corrupción de niños, niñas, adolescentes o personas con discapacidad.

El espíritu de este artículo es el resguardo de la integridad sexual de los niños, niñas o adolescentes; castigando cualquier conducta orientada a corromper el desarrollo natural de la sexualidad de estos o aquellas conductas que facilitaren, promovieren la deformación del desarrollo natural de la sexualidad de los menores de dieciocho años o personas con discapacidad a través del uso de las tecnologías de la información y comunicación.

Asimismo, el inciso segundo del artículo en comento, establece la misma penalidad para los sujetos que propusieren a los niños, niñas, adolescentes o personas con discapacidad; participar en actividades de carácter sexual o la producción de material de contenido pornográfico mediante el uso de medios de comunicación electrónicos prevaleciéndose de las ventajas que estos ofrecen.

El acoso de niños, niñas, adolescentes o personas con discapacidad a través del uso de las TIC's regulado en el artículo 32 de la LEDIC describe la conducta consistente en realizar actos que hostiguen a los niños, niñas, adolescentes o personas con discapacidad que, inequívocamente, sugieran acciones que amenacen o afecten el desarrollo moral, psicológico o emocional de los niños, niñas adolescentes o personas con discapacidad haciendo uso de las Tecnologías de Información y Comunicación.

Nótese que el inciso primero de este artículo no refiere taxativamente a un hostigamiento de naturaleza propiamente sexual, sino que cualquier conducta que afecte la estabilidad psicológica o emocional del niño, niña, adolescente o persona con discapacidad; no obstante en el inciso segundo de este artículo se establece como agravante que el hostigamiento por parte del sujeto activo, haga referencia expresa a la realización de actos de naturaleza sexual de forma inequívoca, todo esto exigiendo (como elemento diferenciador del delito de acoso del artículo 165 del Código Penal) que la conducta sea realizada mediante el empleo de Tecnologías de la Información y Comunicación (redes sociales, aplicaciones de mensajería, entre otros).

Las agravantes contenidas en el artículo 33 de la Ley Especial Contra Delitos Informáticos y Conexos, para los delitos contenidos en este capítulo de la ley supra relacionada, al igual que el artículo 173-B del Código Penal, atienden a la calidad que tenga el sujeto activo respecto del sujeto pasivo.

El capítulo V (Art. 34 LEDIC) dispone los delitos contra el orden económico conteniendo el delito de suplantación en actos de comercialización el cual describe la conducta en la que el sujeto activo realiza actos de comercio de bienes o servicios en nombre de un tercero sin estar autorizado para la comercialización dichos bienes o servicios; utilizando los distintivos, señas comerciales, logotipos, marcas, etc. A través de las TIC's

## 4.5 LEY DE PROTECCION INTEGRAL DE LA NIÑEZ Y LA ADOLESCENCIA

El artículo 33 de la LEPINA en lo relativo a la protección de la salud sexual y reproductiva de los niños, niñas y adolescentes dicha ley establece que el Estado debe jugar un rol garante de programas orientados para el desarrollo natural de la personalidad delos

niños, niñas y adolescentes; asimismo el Estado, a través del Órgano Ejecutivo y el ministerio de Educación debe incluir en su plan de educación debe incluir políticas de educación sexual y reproductiva acordes al desarrollo evolutivo de los niños, niñas y adolescentes.

En el artículo 34 de la LEPINA se prohíbe la comercialización o simple distribución de material pornográfico o sustancias psicotrópicas por cualquier medio, en este sentido es menester la creación de mecanismos que limiten el acceso a los niños, niñas y adolescentes a las Tecnologías de la Información y de la Comunicación con la finalidad de resguardarla integridad personal y sexual de los niños, niñas y adolescentes; que aseguren el correcto desarrollo de la personalidad de estos.

## MARCO CONCEPTUAL

Para lograr una mayor comprensión en cuanto a la temática se muestra una serie de palabras claves utilizadas en la investigación cuyo concepto y definición que se consigna es el sentido en que deben entenderse.

**ALOJAMIENTO WEB**: (en inglés *web hosting*) es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía web.

**ARPANET**: (siglas en inglés de Advanced Research Projects Agency Network) como una de las redes creadas por encargo del **Departamento de Defensa de los Estados Unidos** para poder establecer un importante nexo de comunicación entre los distintos Organismos Gubernamentales de la nación.

**BANDA ANCHA**: Es una conexión o acceso a Internet de alta velocidad. La conexión a Internet de banda ancha puede ofrecerse a través de una empresa telefónica, un proveedor de servicios de Internet o una compañía de cable. Banda ancha, lo cual significa *ancho de banda amplio*, es una de las conexiones a Internet más rápidas disponibles para los consumidores de hoy en día.

**BIEN JURÍDICO**: En sentido general, aquel bien que el derecho ampara o protege. Su carácter jurídico deviene de la creación de una norma jurídica que prescribe una sanción para toda conducta que pueda lesionar dicho bien.

**BOTNET**: La palabra botnet es la combinación de los términos "robot" y "network" en inglés. Los cibercriminales utilizan virus troyanos especiales para crear una brecha en la seguridad de los ordenadores de varios usuarios, tomar el control de cada ordenador y organizar todos los equipos infectados en una red de "bots" que el cibercriminal puede gestionar de forma remota.

**CENSURA**: Acción de examinar una obra destinada al público, suprimiendo o modificando la parte que no se ajusta a determinados planteamientos políticos, morales o religiosos, para determinar si se puede o no publicar o exhibir

**CIBERACOSO**: El ciberacoso o ciberbullying es el acoso o la intimidación en internet. Puede producirse a través de un email, mensaje de texto, en un juego, o en un sitio de redes sociales. Esta práctica podría involucrar circular rumores o imágenes subidas al perfil de alguna persona o circuladas para que otros las vean, o crear un grupo o página para excluir a una persona.

**CIBERESPACIO**: es una **realidad virtual**. No se trata de un ámbito físico, que puede ser tocado, sino que es una construcción digital desarrollada con **computadoras** (ordenadores).

**CIBERCIUDADANO**: es un ciudadano en el ciberespacio o un ciudadano de internet. Es aquella persona que es usuaria de internet, en especial la que participa activamente. En inglés es "cybercitizen".

**CIBERDELITO**: también llamado delito informático o cibercrimen, se refiere a toda actividad ilícita que: (a) Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o (b) Tienen por objeto robo de información, robo de contraseñas, fraude a cuentas bancarias, entre otros.

**DERECHO A LA LIBERTAD DE EXPRESIÓN**: es el **derecho fundamental** que tienen las personas a decir, manifestar y difundir de manera libre lo que piensan sin por ello ser hostigadas. Como tal, es una **libertad civil y política**, relativa al ámbito de la vida pública y social, que caracteriza a los sistemas democráticos y es imprescindible para el respeto de los demás derechos.

**DERECHO A LA LIBERTAD DE PRENSA:** se denomina así al derecho que tienen los medios de comunicación de investigar e informar sin ningún tipo de limitaciones o coacciones, como la censura previa, el acoso o el hostigamiento.

**DERECHO AL LIBRE ACCESO A INTERNET:** es el derecho que posee toda persona para acceder a Internet con el fin de ejercer y disfrutar de sus derechos a la libertad de expresión entre otros derechos humanos fundamentales que conforman la democracia, de forma que los estados y las Naciones Unidas tienen la responsabilidad de garantizar que el acceso a Internet sea ampliamente disponible, no pudiendo restringir injustificadamente el acceso de una persona a Internet.

**DERECHOS DE AUTOR:** se refiere a los derechos que los creadores tienen sobre sus obras literarias y artísticas. Las obras que se prestan a la protección por derecho de autor van desde los libros, la música, la pintura, la escultura y las películas hasta los programas informáticos, las bases de datos, los anuncios publicitarios, los mapas y los dibujos técnicos.

**DERECHOS HUMANOS:** son las libertades fundamentales que tiene una persona por el simple hecho de haber nacido, sin los cuales no se puede vivir como tal.

**DERECHO INFORMÁTICO:** Ciencia y rama autónoma del Derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en aspectos como la regulación del medio informático en su expansión y desarrollo, y la aplicación idónea de los instrumentos informáticos.

**DOMINIO WEB:** es **el nombre único y exclusivo que se le da a un sitio web** en Internet para que cualquiera pueda visitarlo.

**ERA DIGITAL:** momento histórico de síntesis de información; es decir, la búsqueda incansable de descifrar la unidad mínima de información que se puede establecer entre un transmisor y un receptor.

**EVIDENCIA DIGITAL:** es cualquier valor probatorio de la información almacenada o transmitida en formato digital de tal manera que una parte o toda pueda ser utilizada en juicio.

**FRAUDE INFORMÁTICO:** consiste en la estafa o engaño que es realizado por medios cibernéticos a través de la utilización de un computador y/o vía Internet.

**GEOLOCALIZACIÓN:** Es la capacidad de conocer la posición geográfica (coordenadas) o ubicación de un objeto: teléfono, tableta, ordenador, entre otros**.**

**GLOBALIZACIÓN:** es un **proceso histórico de integración mundial en los ámbitos político, económico, social, cultural y tecnológico,** que ha convertido al mundo en un lugar cada vez más interconectado, en una aldea global.

**GROOMING:** Es un término que se utiliza para hacer referencia a todas las conductas o acciones que realiza un adulto para ganarse la confianza de un menor de edad, con el objetivo de obtener beneficios sexuales.

**HACKING:** es el conjunto de técnicas a través de las cuales se accede a un sistema informático vulnerando las medidas de seguridad establecidas originariamente

**HARDWARE:** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

**INFORMÁTICA:** Conjunto de conocimientos técnicos que se ocupan del tratamiento automático de la información por medio de computadoras.

**INFORMÁTICA JURÍDICA:** Conjunto de aplicaciones de la informática en el ámbito jurídico; es una técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica, necesaria para lograr dicha recuperación.

**INTERNET:** Es una **red de computadoras que se encuentran interconectadas a nivel mundial** para compartir información. Se trata de una red de equipos de cálculo que se relacionan entre sí a través de la utilización de un lenguaje universal.

**MALWARE:** es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.

**PISHSHING:** se refiere a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

**REDES SOCIALES:** Páginas web en la que los internautas intercambian información personal y contenidos multimedia de modo que crean una comunidad de amigos virtual e interactiva.

**SEGURIDAD INFORMÁTICA:** proceso de prevenir y detectar el uso no autorizado de un sistema informático.

**SEXTING:** actividad de enviar fotos, videos o mensajes de contenido sexual y erótico personal a través de dispositivos tecnológicos, ya sea utilizando aplicaciones de mensajería instantánea, redes sociales, correo electrónico u otra herramienta de comunicación.

**SOBERANÍA SUPRANACIONAL:** es un sistema político en el cual determinados estados ceden parte de sus atribuciones de gobierno (en mayor o menor medida, dependiendo del grado de supranacionalidad) a organismos internacionales que afectan a más de una nación.

**SOFTWARE:** es todo aquello que es intangible en la computadora, lo que no se puede tocar, como, por ejemplo, los programas y los sistemas operativos

**TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN:** Conocidas con las siglas TIC, son el conjunto de medios (radio, televisión y telefonía convencional) de comunicación y las aplicaciones de información que permiten la captura,

producción, almacenamiento, tratamiento, y presentación de informaciones en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética. Las TIC incluyen la electrónica como tecnología base que soporta el desarrollo de las telecomunicaciones, la informática y el audiovisual.

# CAPITULO III: MARCO METODOLÓGICO

## 1. TIPO DE INVESTIGACIÓN

En la presente investigación denominada "La Necesidad del Estado Salvadoreño de Regular Espacios Cibernéticos Frente al Uso de las Redes Sociales por parte de los Niños, Niñas y Adolescentes para Evitar la Depredación Sexual", se aplicó el método cualitativo, por ser el más idóneo para obtener los resultados esperados sobre la base de las opiniones jurídicas de expertos conocedores en dicha área, relacionada con la problemática objeto de la investigación, cuyos resultados se describieron y sistematizaron a fin de poder contar con información jurídica precisa en cada una de las respuestas que se obtuvieron de los entrevistados; esto permitió obtener una información impregnada de experiencia o práctica jurídica en este campo, para analizar la problemática de forma más efectiva desde el punto de vista de la legislación salvadoreña.

La presente investigación es descriptiva-explicativa, porque describe detalles de una situación, evento, personas, interacciones y comportamientos que son observables, de igual forma se incorporó lo que los participantes manifestaron, a partir de sus experiencias, sus actitudes, sus expectativas de manera más amplia en lo referente a los espacios cibernéticos.

## 2. DISEÑO DE INVESTIGACIÓN

El enfoque utilizado en esta investigación fue el no experimental, debido a que no se realizó ninguna manipulación de variables, ya que únicamente se analizó la legislación vigente en materia de derecho informático, para señalar los mecanismos de control que ejerce el Estado salvadoreño en el ciberespacio.

Bajo el enfoque no experimental el diseño metodológico de la investigación es transversal, donde se recolectaron datos en un solo momento y en un tiempo único, sin hacer referencia a épocas anteriores.

## 3. CONCEPTO DE HERMENÉUTICA

El término de hermenéutica deriva directamente del griego, que significa saber explicativo o interpretativo especialmente de las sagradas escrituras y del sentido de la palabra de los textos. Así, es fruto de la suma de la palabra hermeneuo que puede traducirse

como “yo descifro”, la palabra tekhné que significa “arte”, y el sufijo –tikos que es sinónimo de “relacionado a”. De ahí que literalmente se puede exponer que este término que nos ocupa es el arte de explicar textos o escritos, obras artísticas.

Para muchos la hermenéutica es un tipo de análisis de interpretación de los textos o escrituras que permiten tener bases para tener una lógica respuesta a un texto o investigación como la presente investigación realizada. Su utilización es una herramienta que nos permitió para encontrar mejores resultados dentro de la realidad a la cual nos hemos avocado, asimismo nos permitió llegar a concluir en una realidad verídica dentro del estudio de una investigación.

## 4. ETNOGRAFÍA COMO MÉTODO DE INVESTIGACIÓN

La etnografía es un método de estudio utilizado por los antropólogos para describir las costumbres y tradiciones de un grupo humano, que ayuda a conocer la identidad de una comunidad humana que se desenvuelve en un ámbito sociocultural concreto.

La etnografía implica la observación participante del investigador durante un periodo de tiempo determinado en el que se encontró en contacto directo con el fenómeno a estudiar, la investigación puede completarse con entrevistas para recabar mayor información y descubrir datos que son inaccesibles a simple vista para una persona que no convive directamente con esta realidad.

En cuanto a la utilidad del método, se vuelve imprescindible al momento de realizar una investigación, ya que permite al investigador interactuar con el fenómeno en cuestionamiento y así poder recibir y recolectar la información directamente del informante que se encuentra en contacto directo con el fenómeno que se estudió. Esta investigación se aplicó el método cualitativo utilizando las preguntas a profundidad, donde el entrevistado expone sus experiencias sobre la realidad objetiva sobre el fenómeno de estudio.

## 5. POBLACIÓN Y MUESTRA DE LA INVESTIGACIÓN

### 5.1. POBLACIÓN

El presente estudio, se constituye por toda la comunidad jurídica compuesta por los funcionarios o expertos vinculados en el tema problema de investigación.

## 5.2 MUESTRA

La muestra se conformó por un selecto grupo de expertos conocedores de la legislación vinculada a la problemática, objeto de la investigación, así como algunos funcionarios que aplican esta normativa del Derecho, en el área del Derecho Informático y las TIC's, específicamente los vinculados al control del ciberespacio.

El tipo de muestra se eligió de una forma no probabilística o muestra dirigida por criterios de selección, es decir, se adoptó atributos tales como: ser funcionarios públicos que laboran en instituciones relacionadas a la problemática objeto de la investigación; Tener conocimientos sobre la normativa relativas a los fenómenos informáticos en El Salvador, en donde la intención fue indagar sobre aspectos que regulan el ciberespacio y su efectividad.

### 5.2.1 CUADRO DE PRESENTACIÓN DE LA MUESTRA

| SUJETO | CARGO | INSTITUCIÓN |
|---|---|---|
| **Informante 1** | Magistrado de la Cámara de lo Penal de Occidente | Corte Suprema de Justicia. |
| **Informante 2** | Fiscal Auxiliar | Fiscalía General de la República |
| **Informante 3** | Abogado Particular | _____ |
| **Informante 4** | Sub Inspector | División Central de Investigación, de la Policía Nacional Civil. |
| **Informante 5** | Director | Superintendencia General de Electricidad y Telecomunicaciones. |

## 6. DISEÑO DE INSTRUMENTOS DE INVESTIGACIÓN

El Instrumento que se aplicó en la presente investigación, fue la entrevista estructurada, cuyo objetivo es la obtención de una interpretación de personas con conocimiento respecto a los mecanismos de control que ejerce el Estado salvadoreño en el ciberespacio, las cuales estarán constituidas por diversas preguntas abiertas, lo que permitió que los entrevistados proporcionaran mayor información.

## 6.1 INSTRUMENTOS PARA RECABAR LA INFORMACIÓN

a) **LA ENTREVISTA**: Este instrumento fue conformado por doce preguntas abiertas, sobre los aspectos más relevantes que permitieron evaluar los criterios y niveles de conocimiento, que manifestaron los entrevistados en lo relativo a los mecanismos de control que ejerce el Estado salvadoreño en el ciberespacio, la cual se aplicará de forma individual o personalizada.

b) **GRABACION DE AUDIO**: De esta manera se logró obtener la información de las respuestas dadas, de una forma más convincente y fidedigna, lo cual permitió, ampliar toda la información recabada en la aplicación de la entrevista.

c) **DOCUMENTAL:** Se buscó bibliografía, doctrina, y otros tipos de fuentes, que proporcionaron la información respecto al tema de investigación.

d) **VIRTUAL**: Se hicieron visitas a sitios web relacionados con el tema, así como también bibliotecas virtuales de las diferentes Universidades y, del Centro de Información Judicial de la Corte Suprema de Justicia.

## 7. PASOS EN LA RECOLECCIÓN DE DATOS

Las entrevistas se efectuaron en forma personal a cada uno de los entrevistados, tomando anotaciones y grabaciones, y para la recolección de datos se realizarán dos fases o etapas.

## 7.1 INMERSIÓN INICIAL EN EL CAMPO DE ESTUDIO

Esto significa que se eligieron, antes de recolectar los datos, a las personas idóneas para realizar la investigación. Se consideró necesario estudiar el ambiente en el que se desenvuelven, profesión a la que se dedican, y entender de qué manera le es útil o no a la investigación la persona identificada en la presente investigación. Esto permitió seleccionar la muestra que se utilizó para la recolección de datos.

## 7.2 RECOLECCIÓN DE DATOS PARA EL ANÁLISIS

Esto se llevo a cabo a través de la administración de entrevistas estructuradas, a la población establecida previamente en la elección de la muestra; es así que según la

población donde se recolectaron los datos, así se aplicaron los instrumentos indicados para obtener la información.

## 8. MODELO DE PROCESAMIENTO DE DATOS

Una vez concluido el vaciado de la información obtenida por medio de las entrevistas, se hizo un análisis e interpretación de los resultados, los cuales fueron sistematizados y clasificados por categoría de análisis.

Esto permitió formular conclusiones y recomendaciones, sin dejar de lado algún análisis porcentual cualitativo de la muestra obtenida.

### 8.1 MODELO A UTILIZAR PARA EL ANALISIS DE LOS DATOS

El modelo empleado para este tipo de análisis fue:

a) COMPARATIVO: Se realizaron comparaciones de cada una de las respuestas obtenidas por categorías lo que permitirá el análisis de las respuestas.
b) DESCRIPTIVO: Cada respuesta se describió por categorías lo que legitima la realización de las comparaciones para posteriormente efectuar el análisis.
c) INFERENCIAL: A partir de las respuestas obtenidas, se verificó la situación problemática.
d) TRIANGULACION: A través de esta técnica se analizó la información recabada por medio de diversas fuentes, como: las entrevistas, la legislación respectiva y la doctrina, lo que permitirá analizar la problemática desde diferentes perspectivas.

## 9. VACIADO DE LA INFORMACIÓN

Para el vaciado de la información, se procedió a utilizar la técnica de la codificación de las respuestas obtenidas para posteriormente se identificarán todas las frases, temas o conceptos que se vertieron, de manera que pudieran ser organizados e identificados para su análisis.

Otra técnica utilizada fue la categorización, la cual se aplicó a todos aquellos datos repetidos o comunes resultantes en la aplicación de la entrevista.

## 9.1 INSTRUMENTO PARA VACIAR LA INFORMACIÓN

Para el vaciado de la Información se utilizó un cuadro compuesto por celdas denominada Matriz. En este cuadro se concentró toda la información obtenida de todos los informantes clave, información clasificada conforme a las preguntas realizadas por medio del cuestionario y las diferentes respuestas obtenidas, cuyo objetivo fue facilitar el análisis de la información.

## 10. ANÁLISIS DE LA INFORMACIÓN

Para el análisis de la información se utilizó la Técnica de la Triangulación, que se entiende como la utilización de diferentes medios para comprobar un dato. Es una técnica que sirve para analizar los datos cualitativos. Se basa en analizar datos recogidos por medio de diferentes técnicas, lo cual permite analizar una situación desde diversos ángulos. Es un control cruzado empleando diferentes fuentes, instrumentos o técnicas de recogida de datos.

A las respuestas obtenidas se les suministró un tratamiento descriptivo, conformando categorías de las respuestas y se analizarán e interpretarán para poder darle respuesta a las preguntas de investigación que conllevaron a procurarle una solución jurídica al problema planteado.

Para cumplir con los objetivos de este trabajo de investigación y dar alternativas de solución bajo un ordenamiento jurídico al problema planteado, se tomó como base el método cualitativo, por ser un método que brinda las condiciones necesarias, precisas y puntuales para obtener los resultados esperados sobre la base de las opiniones de expertos conocedores del derecho aplicadores de la legislación relacionada con este tópico.

La investigación se realizó bajo en enfoque descriptivo explicativo, con ello se obtuvo una información empapada de experiencia o práctica jurídica, porque a través de la misma se obtendría un mejor análisis, las manifestaciones de los entrevistados, se puntualizaron en las propiedades y las características del fenómeno en estudio, como una forma de recolectar la información, así como explicar el problema planteado, explorando el por qué ocurre, en qué condiciones se presenta, debido a que esta temática ha sido estudiada en menores dimensiones.

En efecto, el trabajo de investigación tuvo como base la metodología cualitativa, en vista que, este tipo de temas, permitieron que se aplicaran técnicas por medio de las cuales se llegaran a descubrir y a recabar información de forma más científica que empírica en la actividad investigativa, sobre todo por la interrelación que se da al momento de aplicar las entrevistas a los diferentes conocedores y expertos en el derecho.

Esta metodología se aplicó en el abordaje de las preguntas de investigación que se plantearon para responder al tema problema objeto de este estudio: 1) ¿Cuáles son los instrumentos legales vigentes dentro del Ordenamiento Jurídico del Estado salvadoreño que contienen medidas de control para la censura o limitación al acceso al contenido explícito de los niños, niñas y adolescentes?; 2) ¿Cuáles son los beneficios de la aplicación de las medidas de control al acceso de contenido explícito por medio del uso de las TIC?; 3) ¿Cuáles son las instituciones del Estado Salvadoreño que aplican las medidas de control y protección de los niños, niñas y adolescentes?; 4) ¿Son eficaces dichas instituciones en la aplicación de las medidas de control y protección de los niños, niñas y adolescentes?; 5) ¿Cómo afecta en el desarrollo psicológico de los niños, niñas y adolescentes el consumo de material explícito a través de medios tecnológicos?; y 6) ¿Vulnera los Derechos fundamentales de los adultos la censura del ciberespacio con la aplicación de los medios de control de protección de los niños, niñas y adolescentes?

Para dar respuesta a estas interrogantes se utilizaron las siguientes técnicas cualitativas: 1) Entrevista estructurada, 2) Análisis de documentos.

Tal como se mencionó en el capítulo anterior, la entrevista es especialmente ventajosa, cuando se quiere profundizar en el plano investigativo, ya que esta técnica permite a los sujetos entrevistados, dar sus explicaciones al problema; debido a sus conocimientos y experiencias, construyen sus respuestas y sus argumentos de manera que se obtuviera la información más convincente y fidedigna.

Esta práctica permitió, en este caso, comprender las valoraciones emanadas de los sujetos, contrastarlas con la realidad para una mejor comprensión a profundidad sobre el problema de investigación.

Asimismo, con la aplicación de esta técnica, el entrevistador tuvo amplia libertad para responder a las preguntas o para las intervenciones, permitiendo toda la flexibilidad y confianza necesaria para cada caso particular. Esta flexibilidad permitió que el entrevistado configurará su respuesta; pensara lo que iba a decir, mostrará sus dudas y que expresara libremente sus puntos de vista sobre el problema, y la confianza permitió al grupo de investigación, despejar más sus dudas repreguntando sobre la misma respuesta.

Para proceder a la aplicación de la entrevista se diseñó como instrumento un cuestionario de preguntas abiertas, las cuales contienen los diferentes tópicos, en los que se deseó obtener la información necesaria de los sujetos clave de investigación. Este cuestionario, conformado por once preguntas, les sirvió a los investigadores para consolidar la recogida de información y para dirigir las entrevistas de modo que los sujetos tuvieran la oportunidad de dar su punto de vista y valoración de los mismos temas. Fue diseñado de tal manera que haga posible un análisis profundo de cada tópico.

Después que se perfiló el cuestionario, se sometió a la técnica del jueceo para la respectiva validación por parte de un profesional en métodos y técnicas de investigación.

Posteriormente aprobado, se establecieron contactos con los diferentes sujetos objeto de la muestra de investigación. Se entrevistará a cinco informantes clave: Magistrado de la Cámara de la primera Sección de Occidente, asimismo a un Perito especialista en el área de informática de la Policía Nacional Civil, a un Fiscal Auxiliar de la FGR, a un abogado particular aportando un punto de vista de una defensa técnica, y al Director de la Superintendencia General de Electricidad y Telecomunicaciones

Las entrevistas se realizarán previa aceptación de la misma por parte de los funcionarios. Durante la aplicación, con el consentimiento de los entrevistados se grabará la información; posteriormente se transcribirá y se organizará por categorías de análisis, creándose una matriz por categoría, en las cuales se vaciarán los datos recabados de cada pregunta contenida en el cuestionario, para facilitar su análisis.

En cuanto a la exploración de documentos se hizo una revisión de las diferentes leyes, jurisprudencias, tesis, libros y artículos científicos relacionados con el tema sobre el “La Necesidad del Estado Salvadoreño de Regular Espacios Cibernéticos Frente al Uso de

las Redes Sociales por parte de los Niños, Niñas y Adolescentes para Evitar la Depredación Sexual". Esto permitirá construir el marco de antecedentes, el marco teórico y el contexto de interpretación de las entrevistas.

Por último, el análisis de la información, tendrá como finalidad el contraste entre las opiniones de los entrevistados con lo que ocurre realmente en la práctica en las diferentes Instituciones Públicas, respecto al control que realiza el Estado salvadoreño en el ciberespacio. Las combinaciones de estas técnicas proporcionaron las herramientas necesarias para el análisis de los datos.

Para el tratamiento de los datos se establecerá un marco básico y abierto de categorías de análisis lo suficientemente general y flexible que captaron las categorías emergentes y que detectaron la interrelación entre las mismas.

## 11. TRIANGULACIÓN DE LA INFORMACIÓN

La triangulación de la información, esta técnica permitió obtener un análisis de los datos recogidos por medio de los diferentes instrumentos empleados. Esto permitió realizar un cruce de la información obtenida entre los informantes clave, bibliografía, doctrina de los tratadistas de derecho, y el análisis del grupo investigador, con el propósito de efectuar la triangulación de los datos, y llegar así a las conclusiones y recomendaciones respectivas que dejaron establecidas todos los datos que a lo largo de la presente investigación serán encontrados, y dieron así respuesta al problema.

### 11.1 RESULTADOS ESPERADOS

Cada instrumento de entrevista le dará respuesta a cada uno de los objetivos y a su vez a las preguntas de investigación que formaron parte del proceso de investigación. Todos estos datos serán fidedignos y reflejaron la opinión de los sujetos claves y no la de los investigadores.

Además, se constató el grado de conocimiento que tienen los funcionarios que están encargados de la administración de justicia en el país, asimismo de los funcionarios que se involucran como sujetos intervinientes en los procesos penales tanto en la investigación científica del Delito, como de la acusación penal ante el Órgano Jurisdiccional.

Cabe destacar que se suscitó un inconveniente con unos de los informantes postulados para enriquecer con conocimiento este trabajo de grado, en específico, sucedió con la Superintendencia General de Electricidad y Telecomunicaciones, puesto que el equipo de trabajo de la presente investigación, diligentemente realizo los trámites necesarios a fin solicitar un agente informante, para que resolviera los ítems planteados en la respectiva entrevista, a través de la Oficina de Información y Respuesta de la institución antes citada.

No obstante, al momento de haberse cumplido el plazo legal para que hubiese respuesta a nuestra solicitud, por medio de notificación electrónica de fecha diez de febrero de dos mil veinte, la SIGET por medio de la Unidad de Acceso a la Información y Transparencia (UAIT), declara que luego de hacer un análisis de los ítems proveídos con anterioridad correspondientes a la respectiva entrevista, llega a la conclusión de declarar incompetencia de la Superintendencia antes citada, para poder dar respuesta a las interrogantes propuestas por este grupo de trabajo, a fin de esclarecer ciertos puntos que han quedado pendientes de discusión en el presente trabajo de graduación.

Por lo cual, planteada la anterior situación, se agregará al final del presente trabajo una copia de la respectiva Solicitud de Información dirigida a la Oficina de Información y Respuesta de la SIGET, en la cual se refleja cual fue la información solicitada, y asimismo se anexará una copia de la resolución de la solicitud, en donde SIGET da su punto de vista al declararse incompetente para proporcionar la información requerida por este grupo de trabajo.

# CAPITULO IV: ANALISIS E INTERPETRACION DE LOS RESULTADOS

## 1. ANÁLISIS E INTERPRETACIÓN DE LOS DATOS

Es necesario en el estudio de la investigación llevada a cabo, puesto que con ello se realiza un paralelo o comparación de la teoría contenida en los diferentes libros de texto, con la realidad que se vive dentro de la etapa previa de las investigaciones, durante el proceso penal y la administración del espectro radioeléctrico, siendo de especial enriquecimiento el aporte que se obtenga por parte de los sujetos que son fuente de información; motivo por el cual entraremos al análisis e interpretación de las respuestas brindadas por cada persona entrevistada.

### 1.1 CONFIABILIDAD DE LA INVESTIGACIÓN

Es una cualidad esencial que estará impregnada en toda la investigación al momento de recolectar los datos, aunque se sostiene que cualquier método de investigación por su naturaleza puede llegar a tener un margen de error, la cual consiste en un 12%, puesto que el instrumento de la entrevista a profundidad tiende a producir datos cargados de subjetividad por parte de los entrevistados.

También se sostiene que se ha empleado correctamente los instrumentos, en donde, la entrevista logrará obtener con exactitud y consistencia lo esperado en la investigación.

### 1.2 SUPUESTOS Y RIESGOS DE LA INVESTIGACIÓN

En el momento que se empleará la metodología en la presente investigación, se podrá predecir las dificultades en la recopilación de los datos, a través de los canales que se efectuarán en el estudio, entre los cuales se mencionan:

a) SUPUESTOS: se sustentaron los resultados de la investigación, los cuales aportaron una información eficaz, fehaciente y debidamente acreditada.
b) RIESGOS: los sujetos de investigación dispondrían de un tiempo limitado debido a la naturaleza de sus labores que implicará trasladarse en diversas instituciones e incluso capacitaciones, por lo cual el grupo de investigación tomará en cuenta los factores: jurídicos, laborales, sociales y en cuanto a la viabilidad de entrevista.

## 1.3 MATRIZ DE RESPUESTAS EN LAS ENTREVISTAS.

La matriz de respuestas se determinará de acuerdo a los resultados obtenidos en las entrevistas, se vaciará la información de cada entrevista que se realizó, la cual se realizó en base a los objetivos y preguntas planteadas en la presente investigación, y luego permitirá al grupo de estudio realizar un análisis grupal en base a las respuestas.

| MATRIZ DE RESPUESTAS MÉTODO DE VACIADO DE INFORMACIÓN, ENTREVISTA REALIZADAS A DIFERENTES EXPERTOS EN CIENCIAS JURÍDICAS | | | |
|---|---|---|---|
| **PREGUNTAS** | **INFORMANTE 1**<br>**AGENTE FISCAL** | **INFORMANTE 2**<br>**MAGISTRADO CÁMARA PRIMERO DE LO PENAL** | **INFORMANTE 3**<br>**ABOGADO DE LA REPÚBLICA** |
| **1- ¿Qué entiende como "delitos informáticos y conexos" y cuáles son las características que debe reunir las conductas típicas para ser consideradas delitos de esta naturaleza?** | El informante expresó lo siguiente: *"Es un acto típico antijurídico cometido través de los medios tecnológicos".* | El informante expresó lo siguiente: *"Son todos aquellos delitos cometidos a través de medios tecnológicos pero en especial a los delitos contemplados en la ley especial de delitos informáticos y conexos. SI bien es cierto en el Código Penal se regulan ciertas conductas que podrían encajar dentro de los "Delitos Informáticos"… no lo asumimos de esa manera, pareciera ser que nosotros creemos que delitos informáticos son exclusivamente aquellos que están contemplados dentro de la Ley Especial de Delitos Informáticos y Conexos, pero en estricto sentido son todos aquellos cometidos, esencialmente, por medios tecnológicos… Una de los características más importantes, es que se haya hecho uso de las tecnologías en cualquiera de sus variantes; no simplemente a* | *El informante expresó lo siguiente: "Se considera que el Delito Informático es aquel que se comete a través del Internet, pero estamos hablando del Delito que utiliza medios informáticos para la comisión misma del hecho, pero se llega a la conclusión: que eso es indiferente que al final basta que el delincuente se valga de Tecnologías de la Información y Telecomunicación, independientemente con que utilice internet, independientemente que afecte sistemas informáticos; es decir se toma más en consideración el sistema que se está utilizando que son las TIC´S, ya sea un teléfono celular, una cámara inteligente, hasta un televisor inteligente todo eso se puede utilizar, entonces esa es la idea técnica de la consideración del delito, existen ideas equivocadas que estos delitos* |

| | | | |
|---|---|---|---|
| | | *través de un computador, teléfono; si no que en todas aquellas variantes en donde se utilizan inclusive algún tipo de dispositivo electrónico".* | *son cometidos solamente en el internet, está sumamente equivocado porque el vehículo para comisión del delito es el internet en la medida en que no sea un contacto físico esa sería una construcción bien amplia y que incluso si te pones a pensar que la idea del delito es la intersubjetividad en la comisión de estos delitos hay delitos en los que ni siquiera hay contacto sino que lo que hay es una especie de anonimato y una imposibilidad de identificar quién es el sujeto activo, siempre se identificará un hecho delictivo que sea basado en la realidad y con los instrumentos tradicionales del Derecho Penal no es posible demostrarlo, para ello se necesita hacer uso de una nueva configuración teórica para poder interpretarlo, por ejemplo la tentativa se penaliza en algunos casos, pero en los delitos informáticos la tentativa se da como delito consumado (si una persona ingresa ilegalmente a un sistema o base de datos, ya es un delito consumado)".* |

| | | | |
|---|---|---|---|
| **2- ¿Qué instrumentos legales actuales son implementados dentro del ordenamiento jurídico salvadoreño para ejercer control dentro del ciberespacio?** | El informante explica: *"Un control sobre el ciberespacio por parte del Estado como tal no hay, puede existir regulación dentro del seno familiar porque el Estado no puede regularnos nuestras redes sociales".* | El informante explica: *"En El Salvador, somos reacios respecto al control del ciberespacio debido a que este representa una evolución de gran escala más allá de las tecnologías "5g" que va a ser muy difícil tener la capacidad de controlarlo, ya que cada vez se abren nuevas vías para el control del internet o el control de las TICs y no solo exactamente del internet; La información, como mencionaba anteriormente, puede ser de tantas maneras. Significa que, por un momento podemos controlar sobre el internet, en estricto sentido, no será posible ejercer control sobre las otras vías de información y que, precisamente, puede tener acceso la mayoría de ciudadanos, específicamente los jóvenes. Como no existe una ley específica, desde mi punto de vista, que hable sobre cuáles van a ser los parámetros de la utilización del internet, horarios, contenidos, entre* | El informante explica: "*Pues tenemos ausencia de una normativa, que permita trascender o normar el ciberespacio porque al ciberespacio no lo controla nadie; sino tenemos control de ello, probablemente ni siquiera una ley va a permitir o negar el acceso, pero por lo menos disponemos de una Ley contra los Delitos informáticos, el Código Penal que sirve para la persecución de delitos pese a las limitaciones que tiene en cuanto a su alcance pero hay una necesidad bastante grande de ampliar las consideraciones y construcciones de la evidencia virtual, de la evidencia informática, los fundamentos de la evidencia virtual, por lo tanto creo que no tenemos más herramientas que eso, y una necesidad de ser parte al menos de los Estados que se han adherido al Convenio de Bruselas.*<br><br>*Por ejemplo la Deep Web, en* |

| | | | |
|---|---|---|---|
| | | *otros… No hay control y, como no existe ese control, estas tecnologías se prestan para la realización de hechos delictivos.*<br><br>*El único control al que nos podríamos referir dentro del internet es el "Control Parental" en el cual el padre de familia ejerza un poco de presión para verificar los contenidos a los que accesan los jóvenes, ya que de parte del Estado, la Dirección General de Espectáculos Públicos, Radio y Televisión perteneciente al Ministerio de Gobernación, en alguna medida, puede ejercer un control. En otras palabras, prácticamente el internet, no es controlable porque las vías de ingreso están bastante diversificadas y, en ese sentido, no podemos abarcarlas y si, algún día van a ser regulados, serán regulados de forma superficial.".* | *cuanto a tema ético sería conveniente cerrarlo puesto que nada bueno circula a través de esa parte de la red, sin embargo en cuanto a ciber seguridad pues no es muy conveniente para las agencias de inteligencia internacionales, puesto que es ahí donde se puede obtener información de los movimientos del crimen organizado, es como que te pongás una venda en los ojos y no sepas que está haciendo una persona que puede generarte a futuro algún problema, como que tengás un enemigo y le pongas un muro entre él y vos, esto en cuanto a ciber seguridad".* |
| **3- Conoce usted los riesgos a los cuales se exponen los niños, niñas, adolescentes y personas incapaces que tienen acceso a las Tecnologías de Información** | El Informante Manifiesta: *"Ser víctimas de un depredador sexual, puede ser un violador o un pedófilo; la mentalidad se verá afectada, habrá una* | El Informante Manifiesta: *"Los riesgos del internet son todos aquellos ataques que pueden sufrir los niños, niñas y adolescentes, tales como el "Ciberbullying",* | El Informante Manifiesta: "*Al no existir un debido control de parte de los padres, este no es un tema del Estado sino que le compete directamente a los* |

| | | | |
|---|---|---|---|
| **y Comunicación (llámese, celulares inteligentes, consolas de videojuegos, redes sociales, entre otros) de ser positiva su respuesta, describa los riesgos a los cuales están expuestos los sujetos relacionados ad supra y cuales instituciones estatales velan por la protección de estas potenciales víctimas.** | *sexualidad temprana. Le puede ayudar cualquier institución que le de apoyo, reorientándole sobre la conducta observada para no ser víctima de la misma".* | *"Stalking", "Grooming", "Sexting", todo ese tipo de conductas a medida de que el niño, niña o adolescente va adquiriendo ese tipo de inteligencia… a medida de que estos accedan a las TICs, adquieren ciertos compromisos; por ejemplo aquellos que en alguna medida adquieren acceso a tarjetas de débito podrían ser víctimas de estafas, transacciones oscuras… Pero específicamente, en mayor proporción nos referimos a los delitos de naturaleza sexual tales como "sexting", "stalking" o en el peor de los casos la pornografía infantil".* | *padres, los niños están expuestos a cualquier tipo de riesgos, imagínate algo a los que se exponen a algo directamente como intercambio de fotos, programación de citas con adultos y que sean depredadores sexuales, y no solamente se someten a temas de buyling o algo sino hasta sufrir temas de algo sexual, son una variedad de problemas que se han generado".* |
| **4- ¿Cuáles son las ventajas y desventajas del control estatal sobre el ciberespacio?** | El Informante expresó: *"El Estado no puede tener un control, para que el Estado controle mis libertades tiene que haber un motivo, no nos pueden coartar nuestra libertad sin fundamentos válidos, no puede haber un control per se sobre el ciberespacio, el contenido que está en el ciberespacio no puede regularse completamente".* | El Informante expresó: *"Ventajas si al caso está, más allá de la oposición que tienen los periodistas, las empresas de telecomunicaciones, porque van a alegar que es una censura previa y la constitución prohíbe la censura… Más allá de eso es bueno; pero una regulación vamos a clasificarlo así: a) una regulación "blanda" y b) existe una regulación "dura". Cuando hablamos de una regulación blanda nos referimos solo a aspectos tales como la "metadata" sobre informes del usuario, informes sobre al horario de* | El Informante expresó: "*Yo creo que como no es controlable el ciberespacio, te puedo decir que no tengo una respuesta para eso sino que es una desventaja no tener control en el ciberespacio, si la teoría te dice que es el quinto espacio que forma parte del control del Estado, ese quinto espacio del cual el Estado no tiene control, si te dijera una ventaja o una desventaja, prácticamente te estaría dando una respuesta imposible porque la desventaja es no tener el control sobre el* |

| | | | |
|---|---|---|---|
| | | *ciertos contenidos, pero sobre exactamente sobre el contenido de los programas sobre que el Estado imponga "lo que debemos ver" y que "no debemos ver", eso tampoco. Podrá ejercer cualquier otro tipo de control pero regularlo de una manera "dura" por así decirlo no se puede si va a graduar o a legislar algo del núcleo de la información, no es viable. Pero si lo hace desde el aspecto blando que tiene que ver con "los datos de los datos" entonces, ahí no habría ningún problema.*<br><br>*Lo que se pretende es que los contenidos que se van poner en las TIC´s pase ciertos filtros como de franjas horarias en las que el contenido va a estar disponible para determinados sector de la población. Por ejemplo; Petronilo está de vacaciones y quiere ver contenido triple X a las 9 de la mañana. El Estado puede poner ciertas normas que ese contenido solo estará disponible después de las 10 de la noche; por otro lado controlar con quién va a ver él ese contenido es algo en lo que el Estado no* | *ciberespacio, osea no hay forma. Pero es de tener cuidado, control desde la perspectiva tecnológica es difícil controlarlo puesto que hasta a los países más desarrollados es complicado mantener un control, pero si la vemos desde la perspectiva de control formal sería mediante la creación de una ley, pero esta no te garantiza pues que tecnológicamente sea efectiva, entonces estamos ante una especie de algo que se conoce como Derecho Simbólico o norma simbólica que se dedican en cualquier país y que al final no tienen una finalidad de control específico y real sino que solo la idea de que existe una ley y que esta ley ha llenado el vacío legal que se tenía".* |

| | | | |
|---|---|---|---|
| | | *debe inmiscuirse".* | |
| **5- ¿Considera necesario la existencia de normativas jurídicas que permitan al Estado ejercer control total sobre las tecnologías la información de y la comunicación?** | El Informante dijo: *"No puede haber un control total sobre las Tecnologías de la Información y la Comunicación y no es necesario que nos regulen totalmente; necesitamos una mayor supervisión de parte de los padres hacia los hijos para verificar sus conductas y darles la confianza para que se les acerquen a contarles lo que les está pasando mientras hacen uso de la red para poder actuar de mejor manera ante ello".* | El Informante dijo: *"Control total no. Siempre he dicho que el Estado debe mantenerse al margen de las libertades individuales, así de sencillo. Por eso yo digo que ese control blando debe atribuírsele a otras instituciones. Por Ejemplo; yo digo "Quiero ver X película que trata de volar cerebros en esos casos el Estado debe advertir la peligrosidad del contenido" es decir, debe existir un control menor pero no un control en estricto sentido, es decir, prohibitivo para ciertos programas no debería existir".* | El Informante dijo: "*Sí, por ejemplo la idea de la prevención, subir la pena a determinado delito eso no te garantiza que ya no se cometerá dicho delito, solo aquel que verdaderamente tiene la capacidad de entender el remedio de una norma y que le prohíbe hacer algo es el que se abstiene de cometer un delito, otros lo que hacen es buscar la manera de como evadir ese control; las compañías que ofrecen servicios de internet podrían en un momento dado mediante un control de ciber seguridad sobre ellos posiblemente podrían identificar a los usuarios, a niños que podrían tener acceso a un aparato tecnológico el niño no puede ir a comprar un celular, será el padre, se identifica el aparato,* |
| **6- ¿Qué impacto puede tener la censura estatal del ciberespacio frente a las libertades individuales de las personas dentro de la** | El Informante manifestó: *"No pueden censurarme totalmente porque me estarían coartando mis derechos; tenemos derecho a estar informados de los lo que está pasando en el país y* | El Informante manifestó: *"Mucho impacto. Una censura total, un control "duro" no es conveniente ya que ella limita la libertad de acceder a la información, la* | El Informante manifestó: *"Puede que sí, sería viable que en determinado momento se pueda llegar a controlar el ciber espacio, por ejemplo llegara a darse en un momento* |

| | | | |
|---|---|---|---|
| **sociedad?** | *fuera de él, no nos pueden aislar de la información, no pueden influir de esa manera en nuestra libertad de expresión y pensamiento".* | *autodeterminación informática donde el yo tengo además el deber de recibir información así también existe el derecho de exigir que la información llegue a mí de una forma íntegra y sin ningún tipo de sesgo… Para mí tiene que ser, definitivamente, no debe existir ese control o regulación sobre el ciberespacio sobre los aspectos "de fondo" por así llamarlo, de la información y respecto de las tecnologías ".* | *determinado mediante un control sobre las empresas que distribuyen el internet, talvez se podría tener un control, posiblemente se podría identificar que un menor de edad es el que está usando un dispositivo y la empresa que distribuye el internet podría controlarlo, pero si estamos hablando de censura como medio de control frente al uso porque puede impactar y hacer menos vulnerable a los menores, pero habría que establecer un parámetro hasta donde puede acceder un niño porque la Convención Internacional de los Derechos del niño te dice que es desde uno hasta los dieciocho años, pero si estamos hablando de censura restrictiva esa es imposible ya que es contraria a lo que establece la Constitución de la República porque podría afectar hasta los adultos; pero no pierda de vista que hay otros mecanismos factibles y menos dañinos que son parte de la prevención de las empresas que distribuyen el internet como el control parental".* |

| | | | |
|---|---|---|---|
| | | | |
| **7- Considera ¿A la censura estatal del ciberespacio Como única alternativa viable para la protección de los menores de edad frente a contenido potencialmente explicito dentro del internet?** | El informante expresó: *"No necesariamente, porque el control debe empezar en casa, los padres de familia o encargados deben supervisar el manejo que le dan los menores de edad al internet".* | El informante expresó: "*Siempre he estado en contra de la censura por parte del Estado ya que ella también limita mi libertad de expresión, claro, libertad de expresión no significa decir cualquier cosa, sino que libertad de expresión, mientras ella no afecte a un tercero. Si no, qué decir y expresarme de la forma que a mí me parece correcta dentro de los parámetros legales. Por eso no lo veo que haya necesidad de utilizar la censura como una prima ratio en materia del internet."* | El informante expone: "*No, no creo que sea viable al cien por ciento, además que es imposible sino es mediante mecanismos que sean contrarios a los Derechos fundamentales, siempre he creído que es mejor la orientación y comunicación de los padres hacia los hijos"* |

| | | | |
|---|---|---|---|
| **8- ¿Cuáles son las variables que afectan la eficacia del procedimiento judicial llevado a cabo en contra de los delitos cibernéticos referidos a la pornografía infantil?** | El Informante asegura: *"La falta de preparación por parte del ente fiscal y policial respecto a la investigación debido a la poca capacitación en la rama de delitos informáticos; además de no contar con tecnología de primera para facilitar la indagación y también por la poca cultura de denuncia".* | El informante manifestó: "*Aquí nos encontramos ante dos circunstancias; la primera: Cuales los son los tres tipos de delitos que se pueden dar? El primero en contra de los programas; el segundo tipo tiene que ver con los delitos cometidos en contra de la información. En el primero lo que se pretende es destruir programas; en el segundo lo que se pretende es extraer información y la otra es por medio de, es decir, utilizar la tecnología para cometer un delito; entonces si utilizamos la tecnología para ese tipo de delitos, ahí es donde de parte del agente persecutor están las dos vías, por ejemplo: "X buscó en OLX"... pero no se propone como una estafa en ese sentido, lo ponen ESTAFA CON UTILIZACIÓN DE UNA TECNOLOGÍA. En estos casos la investigación no se centra en el método si no que en el resultado. Cuando se trata de la pornografía de igual manera lo convierte en un delito tradicional, con la utilización de la Tecnología pero como elemento secundario. No le ven* | El informante manifiesta: *"Tenemos la ventaja de que cuando se trata de menores de edad existe la prohibición de difusión de imágenes o la información personal de los menores afectados, pero no deja de tener un tacto los prejuicios que se van arrastrando a través de la opinión pública, eso atañe a los legisladores, atañe a la policía, atañe al Fiscal, atañe a los jueces, atañe a medio mundo, entonces hay algunos casos en los que por un tema de arrastre de opinión pública este influya en la absolución o la condena, osea eso afectaría la eficacia del proceso y eso afectaría el tema de intuición y sana crítica con que se debe de resolver un caso, por ejemplo en un caso bastante mencionado de un Magistrado que se volvió muy mencionado, muchas personas emitieron sus opiniones y juicios de valor sin tan siquiera conocer cómo se dieron los hechos, hablaban con propiedad, sin tener acceso al expediente y los juzgadores sí conocían lo que había pasado porque estaban aplicando la* |

| | | | |
|---|---|---|---|
| | | *como un delito a través de la web y le dan prioridad a la investigación científica o a la utilización de los medios tecnológicos. El problema que existe en el país es que la FGR no quiere meterse de lleno a la investigación informática y se le da un tratamiento de un delito convencional, ese es el principal problema que presenta los delitos de pornografía infantil a través de los medios tecnológicos. Es una maraña de investigación en la cual no estamos en la capacidad nosotros, tanto el ente persecutor del delito para afrontar ese reto.* | *Ley, es un caso donde la opinión pública influye en casos".* |
| **9- ¿Cuáles son las políticas públicas aplicadas a nivel institucional para el control de la cibercriminalidad, en cualquiera de sus formas, a efectos de garantizar** | El informante manifiesta: *"Las acciones que realiza la FGR es que cuando hay un ilícito que cae bajo los parámetros de naturaleza "cibernéticos" se judicializa el caso bajo la ley especial y no el Código Penal* | El informante expresó: *"NINGUNA. De parte del Estado no existe ninguna política pública encaminada al combate de la cibercriminalidad, en donde todas las instituciones estén* | El informante expone: *"No, la verdad que no, esa cuestión tiene que ver con política general del Estado, si lo vemos como política general del Estado es dentro de ello hay un componente que es la política* |

| | | | |
|---|---|---|---|
| **protección integral de los niños, niña, adolescente y personas incapaces con acceso a las Tecnologías de la Comunicación e información?** | *aunque encaje en éste, pero destaca la característica de los medios a través de los cuales se cometen"* | *involucradas".* | *criminal, entonces el Estado a través de esos mecanismos es un poco invisible, pero que cumple grandes efectos de cuando se crea una ley el Estado siempre se pone de agredido, el gran problema es que esto tiene que ver mucho con la orientación que en un momento dado tenga el congreso o como está determinada la Asamblea y quien tiene la disponibilidad de decidir en un momento dado que se aprueba o que no se aprueba en una Ley entonces el Estado se dispone de eso como único mecanismo, está en el Art. 31 numeral 5 de la Constitución".* |
| **10- ¿Considera que dentro el ordenamiento jurídico actual, existe un tratamiento eficaz en contra de los delitos cibernéticos y en específico aquellos de índole sexual en contra de menores de edad?** | El informante expresó: *"Sí, porque en caso de in dubio pro reo nos vamos por el Código Penal, sin embargo hay que judicializar el caso bajo la ley especial; por tener penalidad más agravada, porque cuando se creó el Código Penal la tecnología no estaba tan avanzada".* | El Informante asegura: *"Un tratamiento eficaz a los delitos informáticos no existe, y como no existe ese tratamiento a los delitos de esta naturaleza, se le da paso a la impunidad y sobre todo a los cometidos en contra de los niños, niñas y adolescentes. Cuando hablamos de tratamiento, me refiero a la investigación. Como no hay forma, no hay manera y no hay* | El informante expresó: *"Si, por lo que he venido viendo el desarrollo de cómo han venido pasando, creo que podríamos ver de una nota 3 a 6, por lo que se está haciendo, hace 3 a 5 años estábamos iniciando en cuanto a los delitos informáticos, claro que hay grandes deficiencias en que a veces el policía a veces manipula cosas que pueden* |

| | | | |
|---|---|---|---|
| | | *los recursos para investigar estos delitos.".* | *afectar después en el resultado de un proceso pero eso es también falta de la debida capacitación de los agentes pero creo que se está trabajando en eso".* |
| **11- ¿Cuál es el impacto psicológico y social en el cual se ven inmersos las víctimas menores de edad, de delitos cibernéticos de índole sexual?** | El informante manifiesta: *"Temor, vergüenza, auto recriminación, inseguridad personal y social, baja autoestima, depresión, puede llegar a ser un repetidor de conductas si no se le da un tratamiento adecuado, la familia también sale afectada cuando no pudieron hacer nada sobre el hecho y sienten impotencia".* | *El informante manifiesta: "Temor, vergüenza, auto recriminación, inseguridad personal y social, baja autoestima, depresión, puede llegar a ser un repetidos de conductas si no se le da un tratamiento adecuado, la familia también sale afectada cuando no pudieron hacer nada sobre el hecho y sienten impotencia".* | El Informante asegura: *"Para los niños no creo que les afecte del momento respecto cuando hay daño sexual de por medio, pero en el medio en que un niño sufre una vulneración de esa naturaleza y se vaya desarrollando posiblemente en la medida en que el desarrollo le va permitiendo saber a qué fue sometido por ejemplo le afecte más en daño gradual y hay el tema de la indemnidad que es la preocupación principal cuando se habla de niños, cuando se habla de delitos con connotación sexual se pretende que el menor sea desarrollado en una sociedad respetando esa natural forma de desarrollarse osea nunca debe de ser sometido a una cuestión a una cuestión previo a la que no está preparado, en la medida en que el niño o niña comprenda al* |

| | | | |
|---|---|---|---|
| | | | *daño en al que ha sido sometido es ahí donde se manifiesta el daño psicológico".* |
| **12- ¿Cuáles son las principales falencias observables en el Estado salvadoreño para la positivización de la Ley Especial Contra los Delitos Informáticos y Conexos de manera que se logren reducir efectivamente los delitos de esta naturaleza?** | El informante asegura: *"Principalmente la tecnología, al no tener las licencias adecuadas para obtener la información, como en el caso de los iphone, falta actualizarnos tecnológicamente".* | El informante expresó: *"Lo que falta es preparación por parte del ente persecutor, dejar de tener miedo a investigar los delitos informáticos cometidos por medio de la tecnología… A encontrar las formas de cómo se puede encontrar la información."* | El informante manifiesta: *"En primer lugar se necesita una política idónea, inversión de recursos, la tecnificación, y agregar el compromiso en que el Estado debe de no solo en dar muestra de quererse adherirse formalmente al convenio de Budapest y suscribirlo, porque eso permitiría estar en la línea en la que los otros Estados están positivamente para no quedarnos con una Ley que se ve buena, pero que al final no se pueda ver el resultado, sin embargo se está aplicando y que desde hace algún tiempo está tomando relevancia".* |

| MATRIZ DE RESPUESTAS MÉTODO DE VACIADO DE INFORMACIÓN, ENTREVISTA REALIZADA A EXPERTO DE INVESTIGACIÓN DE DELITO INFORMATICO Y CONEXOS (DIVISIÓN CENTRAL DE INVESTIGACIONES DE LA POLICIA NACIONAL CIVIL) | |
|---|---|
| **PREGUNTAS** | **INFORMANTE 4** |
| 1. **¿Cuáles son los posibles riesgos a los que se exponen los niños, niñas y adolescentes al navegar por el internet**? | El informante expresó lo siguiente: *"En la actualidad existe una sobrexposición a los videojuegos por parte de los niños, niñas y adolescentes, y en mayor medida a aquellos Juegos Online, que necesariamente deben estar conectados al internet, es a partir de acá que surgen una variedad de riesgos, puesto que los menores de edad pueden ser persuadidos, por personas sin escrúpulos, para obtener de ellos información delicada (privada o financiera), fotos y videos explícitos (grooming, información financiera, sexting y sextorsión) lo cual puede conllevar un daño a la psiquis de las víctimas".* |
| **2. ¿Cuáles son los mecanismos de control del internet de los cuales dispone el Estado salvadoreño para el control del contenido multimedia que está disponible en el internet?** | El informante explica: *"Dentro de las investigaciones dirigidas en contra de los delitos informáticos, solo existen directrices, por parte de la Fiscalía General de la República, para el cómo realizar dichas investigaciones, no obstante, el control de los contenidos dentro del internet, en mayor medida, corresponden a los proveedores de Internet. En conclusión la División Central de Investigación de la PNC, se encarga únicamente de la investigación científica de los delitos informáticos".* |
| **3. ¿Cuál es el contenido multimedia ilícito que más se incauta en las investigaciones llevadas a cabo en el país?** | El Informante Manifiesta: *"Es el material relacionado al abuso sexual infantil, imágenes y videos".* |
| **4. ¿Cuáles son los criterios que se siguen para determinar que el material recabado sea útil para la investigación judicial de un posible delito informático?** | El Informante expresó: *"Se ocupa la Evidencia Digital la cual debe estar vinculada al hecho presuntamente delictivo, y aquella que no sea constitutiva de delito no puede ser tomada en cuenta".* |

| | |
|---|---|
| **5. ¿Cuáles son los criterios que se siguen para determinar que el material recabado sea útil para la investigación judicial de un posible delito informático?** | El Informante dijo: *"Que los criterios bajo los cuales se guían, son aquellos que se estipulan en el Código Procesal Penal vigente, en lo respectivo a la Prueba dentro de los procedimientos judiciales".* |
| **6. ¿Posee planes para la actualización de protocolos de protección de los niños, niñas y adolescentes para al combate de la depredación infantil en el ciberespacio?** | El Informante manifestó: *"Actualmente solo están ligados al ordenamiento jurídico actual, no obstante, cualquier política debe venir de la voluntad Estatal, y debe haber un principal enfoque a aquellas políticas educacionales para la prevención de posibles delitos informáticos".* |
| **7. ¿Cuáles el procedimiento sancionatorio que sigue en caso de que una empresa operadora de telecomunicaciones se niegue a colaborar con una investigación penal?** | El informante expresó: "La *División Central de Investigación de la PNC no tienen esta información , se espera que la Fiscalía General de la República genere acuerdo con dichas empresas*", |
| **8. ¿Cree usted que los límites legales establecidos actualmente violentan los derechos constitucionales de intimidad, inviolabilidad de las comunicaciones?** | El Informante asegura: *" Siempre y cuando los procedimientos para la intervención de las comunicaciones se realicen mediante la debida autorización judicial dada por la autoridad competente, no puede existir una vulneración a los derechos fundamentales de los individuos".* |

| MATRIZ DE ANÁLISIS DE LA INFORMACIÓN POR MEDIO DE LA TRIANGULACIÓN, ENTREVISTA A LA DELEGADA DE LA FGR | | | |
|---|---|---|---|
| PREGUNTA | DOCTRINA | RESPUESTA DE INFORMANTE | OPINIÓN DE GRUPO |
| **1. ¿Qué entiende como "delitos informáticos y conexos" y cuáles son las características que deben reunir las conductas típicas para ser consideradas delitos de esta naturaleza?** | Según la doctrina los delitos informáticos son: "todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro." | *"Es un acto típico antijurídico cometido través de los medios tecnológicos".* | La informante respondió de manera escueta, sin profundizar o detallar más allá de una simple respuesta, suponemos que es por falta de preparación doctrinaria y de práctica profesional en la rama de dichos delitos, puesto que parece una respuesta de un diccionario simple. |
| **2. ¿Qué instrumentos legales actuales son implementados dentro del ordenamiento jurídico salvadoreño para ejercer control dentro del ciberespacio?** | Existe una variedad de Leyes tanto Nacionales como Tratados Internacionales que tal como lo establece la Constitución de la República, si son reconocidos, firmados, ratificados forman parte de las Leyes de las cuales el Estado Salvadoreño puede hacer | *"Un control sobre el ciberespacio por parte del Estado como tal no hay, puede existir regulación dentro del seno familiar porque el Estado no puede regularnos nuestras redes sociales".* | Creemos que la informante no sabía que responder, puesto que sabemos que existen las leyes óptimas, desde un punto de vista, pero lo que se sucede es que hay poca aplicabilidad de la misma debido a la escasa cultura de denuncia y poca |

| | | | |
|---|---|---|---|
| | uso, reconocimiento, prevalencia de Derechos y Bienes Jurídicos. Entre estas Leyes tenemos: Código Penal, Ley Contra Delitos Informáticos y Conexos. | | preparación de las instituciones encargadas de la investigación. No existe ley que controle totalmente el ciberespacio, el control se da por parte de las empresas que prestan las plataformas de comunicación, es decir las redes sociales donde no puede circular cualquier tipo de contenido, limitan de cierta forma el público debido al daño sicológico que pueda recibir el espectador. |
| **3. ¿Cuáles son los riesgos a los cuales se exponen los niños, niñas, adolescentes y personas incapaces que tienen acceso a las Tecnologías de Información y Comunicación (llámese, celulares inteligentes, consolas de videojuegos, redes sociales, entre otros), de ser positiva su respuesta, describa los riesgos a los cuales están expuestos los sujetos relacionados ad supra y cuales instituciones estatales velan por la protección de estas potenciales víctimas?** | Dentro de los riesgos a los cuales se exponen los niños, niñas y adolescentes podemos marcar la diferencia entre los delitos con connotación sexual y los delitos comunes pero de los que se hace uso de las TIC´S para su finalidad, dentro de la primera categoría tenemos el grooming, el sexting, la sextorsión, revenge porn, stalking, y la siguiente categoría podemos mencionar la depredación sexual infantil, violación, secuestro, privación de libertad, estafa, entre otros. | *"Ser víctimas de un depredador sexual, puede ser un violador o un pedófilo; la mentalidad se verá afectada, habrá una sexualidad temprana. Le puede ayudar cualquier institución que le de apoyo, reorientándole sobre la conducta observada para no ser víctima de la misma".* | Consideramos que la informante se quedó corta con su respuesta, sabemos que los riesgos a los que se exponen los niños, niñas, adolescentes y personas incapaces son en parte la consecuencia de la poca o nula supervisión de los padres de familia o encargados, como bien sabemos que la tecnología no es mala sino el uso que se le puede dar, en el ciberespacio podemos encontrar de todo, pero nadie nos manda a buscar cosas ilícitas o que dañen la salud mental, las TICS fueron creadas con el fin de facilitar la vida al ser humano en cuanto a lo laboral, económico, comunicación a distancia, |

| | | | |
|---|---|---|---|
| | | | educación. Entre otros; no para buscar contenido nocivo como el que se encuentra en la deep web ni para convertirnos en agresores a través de la red. |
| **4. ¿Cuáles son las ventajas y desventajas del control estatal sobre el ciberespacio?** | En los países más avanzados tecnológicamente se argumenta que el control estatal del ciberespacio se debe a la protección de los intereses de Seguridad Nacional y de seguridad pública prueba de ello es que en sectores de capas profundas del internet es donde las agencias de inteligencia recolectan información del crimen organizado, sin embargo estos accesos requieren de conocimiento tecnológico avanzado para la navegación, sin lo cual los particulares no pueden acceder, es ahí donde nacen algunas polémicas si el ciberespacio debe de ser controlado totalmente por los Estados o si debe de permanecer esa fuente de información.<br>En cuanto a las desventajas se sabe que el ciberespacio no puede ser controlado localmente por los Estados sin que se ordene su bloqueo a diferentes dominios, también se plantea la idea que | *"El Estado no puede tener un control, para que el Estado controle mis libertades tiene que haber un motivo, no nos pueden coartar nuestra libertad sin fundamentos válidos, no puede haber un control per se sobre el ciberespacio, el contenido que está en el ciberespacio no puede regularse completamente".* | Pensamos que resulta difícil regular completamente el ciberespacio, pero de hacerlo efectivo, le serviría al Estado de herramienta para individualizar de cierta manera al sujeto activo para hacer efectiva la protección de los derechos de la persona humana, una desventaja sería para el conglomerado social en cuanto a la vulneración de la libertad de expresión, de pensamiento, de prensa y el acceso a la información por parte de las personas; debido a la censura del ciberespacio, se debe concientizar a los usuarios del uso moderado del ciberespacio. |

| | | | |
|---|---|---|---|
| | existan algoritmos que clasifiquen, adviertan y bloqueen la publicación de material multimedia o textos publicados en las redes sociales o en la comunicaciones a través de las plataformas más populares actualmente. | | |
| **5. ¿Es necesario la existencia de normativas jurídicas que permitan al Estado ejercer control total sobre las tecnologías la información de y la comunicación?** | Las normativas Jurídicas del sector de Derecho Penal son las expresión de imperio del Estado por sobre el elemento humano y de estricto cumplimiento, las mismas de acuerdo a diferentes teóricos tienen la finalidad de imponer penas a delitos, al imponer penas regular las conductas de los individuos dentro de la sociedad.<br>Las normas administrativas también son de obligatorio cumplimiento y rigen o determinan el comportamiento de los servidores públicos y de los particulares frente a la Administración pública; al relacionar los dos tipos de reglas se planifican lineamientos tanto entre las responsabilidades penales como las relaciones entre el Estado y los particulares en cuanto a la administración del ciberespacio. | *"No puede haber un control total sobre las Tecnologías de la Información y la Comunicación y no es necesario que nos regulen totalmente; necesitamos una mayor supervisión de parte de los padres hacia los hijos para verificar sus conductas y darles la confianza para que se les acerquen a contarles lo que les está pasando mientras hacen uso de la red para poder actuar de mejor manera ante ello".* | La informante no respondió bien lo que se le preguntó, es cierto que no es necesario un control total sobre las TICS, ya que una gran parte de usuarios son adultos y por ende saben discernir entre el bien y el mal, saben en qué delitos pueden incurrir, pues nadie puede alegar ignorancia de ley y tienen la potestad de supervisar lo que hacen los niños, niñas, adolescentes que habitan en sus hogares o están bajo su cargo. No necesitamos más leyes, sino que se necesita hacer efectivas las ya establecidas, que las instituciones encargadas de la investigación trabajen con eficacia para una mejor judicialización y así llegar a la condena en caso de encontrar culpable al agresor. |

| | | | |
|---|---|---|---|
| **6. ¿Qué impacto puede tener la censura estatal del ciberespacio frente a las libertades individuales de las personas dentro de la sociedad?** | Censura: Se refiere a la intervención que realiza un censor sobre el contenido o la forma de una obra, atendiendo razones morales, políticas, ideológicas, religiosas o de otro tipo, la censura de esta manera, se supone prevenir o limitar una expresión por considerar que sus contenidos pueden ser ofensivos o dañinos; La censura, por lo general, está asociada a la intención de un gobierno de impedir la difusión de información contraria a sus intereses. En las sociedades democráticas, la censura previa suele estar prohibida: es decir, los gobernantes no tienen derecho de impedir la publicación de ningún material. En caso que dicho material, una vez hecho público, incurra en un delito, la Justicia puede tomar las medidas correspondientes. | El Informante manifestó: *"No pueden censurarme totalmente porque me estarían coartando mis derechos; tenemos derecho a estar informados de los lo que está pasando en el país y fuera de él, no nos pueden aislar de la información, no pueden influir de esa manera en nuestra libertad de expresión y pensamiento".* | Sería un impacto negativo debido al hecho de coartar libertades garantizadas fundamentalmente en la Constitución, amordazando a las personas al no permitirles manifestar sus opiniones o pensamientos de manera oral o escrita. Para tener acceso a datos y contenidos de los usuarios debe ser por mandato judicial. Al establecer una censura total se estaría vulnerando el estado de derecho donde debe prevalecer la democracia. |
| **7. ¿Considera a la censura estatal del ciberespacio como única alternativa viable para la protección de los menores de edad frente a contenido potencialmente explícito dentro del internet?** | Se considera censura estatal como la acción que ejerce un gobierno que utiliza herramientas tecnológicas y jurídicas con la finalidad de supervisar, evaluar, sancionar , controlar y prohibir las actividades que realizan los ciudadanos en sus actividades | El informante expresó: *"No necesariamente, porque el control debe empezar en casa, los padres de familia o encargados deben supervisar el manejo que le dan los menores de edad al internet".* | No es la única alternativa, de hecho no es viable, debido a la vulneración de derechos que se daría, el contenido explicito que circula en la red debe ser controlado por las empresas que prestan los servicios y por las instituciones encargadas de la |

| | | | |
|---|---|---|---|
| | cotidianas. Durante el taller Libertad de Expresión en Internet: aspectos regulatorios en América Latina, organizado por el profesor Eduardo Bertoni, se analizó el rol que corresponde a los Gobiernos en la protección de la libertad de expresión en Internet y en la sanción de expresiones nocivas, tanto en forma directa como mediante la regulación de los intermediarios. También se evaluó la función que desempeñan los Gobiernos en la regulación de los proveedores de servicios de Internet para facilitar el libre flujo de información. | | investigación de los ciber delitos, además debe haber supervisión por parte de los padres de familia o encargados sobre el material que ven sus hijos. |
| **8. ¿Cuáles son las variables que afectan la eficacia del procedimiento penal llevado a cabo en contra de los delitos cibernéticos referidos a la pornografía infantil?** | Las medidas legales son cruciales para la prevención y el combate del delito cibernético, y se las requiere en todas las áreas, para que cubran la criminalización, los poderes procesales, la jurisdicción, la cooperación internacional y la responsabilidad de los proveedores de servicios de Internet. | El Informante asegura: *"La falta de preparación por parte del ente fiscal y policial respecto a la investigación debido a la poca capacitación en la rama de delitos informáticos; además de no contar con tecnología de primera para facilitar la indagación y también por la poca cultura de denuncia".* | En nuestro país se necesita más preparación profesional técnico científica para el proceso de investigación, se necesita más conocimiento de la materia por parte de los encargados de la investigación, más aparatos y sistemas tecnológicos que les faciliten el desenvolvimiento del procedimiento investigativo para principalmente individualizar al sujeto activo y para valorar la prueba. Se han hecho algunas capacitaciones en el exterior a agentes de la PNC que trabajan en el área de |

| | | | |
|---|---|---|---|
| | | | delitos cibernéticos y a algunos fiscales, pero estos esfuerzos no han sido suficientes, ya que la gente suele quedarse callada y no denunciar este tipo de delitos por distintas circunstancias. |
| **9. ¿Cuáles son las políticas públicas aplicadas a nivel institucional para el control de la ciber criminalidad, en cualquiera de sus formas, a efectos de garantizar protección integral de los niños, niñas, adolescentes y personas incapaces con acceso a las Tecnologías de la Comunicación e Información?** | La aplicación de la Ley de Delitos Informáticos y Conexos con el fin de proteger bienes jurídicos mediante vulneraciones a través de los medios tecnológicos. | El informante manifiesta: *"Las acciones que realiza la FGR es que cuando hay un ilícito que cae bajo los parámetros de naturaleza "cibernéticos" se judicializa el caso bajo la ley especial y no el Código Penal aunque encaje en éste, pero destaca la característica de los medios a través de los cuales se cometen"* | Consideramos que no existen diversas políticas públicas encaminadas para el control de los delitos cibernéticos más que la Ley de Delitos Informáticos y Conexos, y la suscripción al Convenio de Budapest, bastaría con lo que hay si se le diera aplicabilidad al darla a conocer más a la población para quienes se encuentran agraviados por un delito cibernético se atrevan a denunciar, no se ha creado ningún programa que trate sobre esta problemática que cada día crece afectando a muchas personas en su mayoría NNA. |
| **10. Dentro del ordenamiento jurídico actual, ¿Considera que existe un tratamiento eficaz en contra de los delitos cibernéticos y en específico aquellos de índole sexual en contra de menores de edad?** | 10. El 26 de febrero de 2016 se aprobó la Ley Especial contra Delitos Informáticos y Conexos, mediante el Decreto Legislativo No. 260, publicado en el Diario Oficial No. 40 Tomo No. 410, de la misma fecha; la cual sistematiza los tipos penales relacionados con la ciber | El informante expresó: *"Sí, porque en caso de in dubio pro reo nos vamos por el Código Penal, sin embargo hay que judicializar el caso bajo la ley especial; por tener penalidad más agravada, porque cuando se creó el Código Penal la tecnología no estaba tan* | Sí, porque entendemos que actúan bajo los parámetros que la ley ha establecido, buscando la aplicación de justicia en pro de los derechos fundamentales consagrados para prevenir o reprimir las conductas delictivas que vulneren tales derechos. |

| | | | |
|---|---|---|---|
| | delincuencia, generando en los operadores de justicia nuevos desafíos para su aplicación y sanción penal, por cuanto la referida normativa se encuentra relacionada con la utilización de tecnologías de la información y comunicación; de tal manera que la investigación, procesamiento y juzgamiento, están condicionadas a laplicación de actividades técnicas y periciales informáticas. | *avanzada".* | |
| **11. ¿Cuál es el impacto sicológico y social en el que se ven inmersos las víctimas menores de edad, de delitos cibernéticos de índole sexual?** | 11. A través de estudios psicológicos se descubrió que los daños que causan eventos de violencia sexual en los NNA son diversos, entre los delitos informáticos que implican acoso, sexting se encuentran: sentimientos negativos de culpa, vergüenza, culpa o ira, ansiedad, depresión, pérdida progresiva de confianza propia; en los casos que implica acceso carnal y haberse utilizado las TICS como medio de comunicación para consumar el hecho además de las anteriores secuelas psicológicas se encuentran: problemas emocionales, problemas de relaciones interpersonales, problemas de conductas y adaptación social, funcionales, | El informante manifiesta: "Temor, vergüenza, auto recriminación, inseguridad personal y social, baja autoestima, depresión, puede llegar a ser un repetidor de conductas si no se le da un tratamiento adecuado, la familia también sale afectada cuando no pudieron hacer nada sobre el hecho y sienten impotencia". | Opinamos que la informante tiene razón en los sentimientos que que llegan a la víctima luego de la agresión, principalmente la recriminación, sabemos que se ven inmersos en una serie de emociones negativas que les afecta su psiquis a temprana edad por la exposición de su imagen e intimidad por agresores y acosadores sexuales que a través de engaños se han ganado su confianza y al verse defraudados por estos se sienten avergonzados, deprimidos e inseguros, donde incluso a veces llegan a atentar contra su vida misma al sentirse dañados y vulnerables. |

| | | | |
|---|---|---|---|
| | revictimización, sexuales, transmisión intergeneracional, abuso de drogas y/o alcoholismo, entre otros. | | |
| **12. ¿Cuáles son las principales falencias observables en el Estado Salvadoreño para la positivización de la Ley Especial contra los Delitos Informáticos y Conexos de manera que se logren reducir efectivamente los delitos de esta naturaleza?** | Para Luigi Ferrajoli, el deterioro de la forma de la ley, la falta de certeza generalizada a causa de la incoherencia y la inflación normativa, representan no solo un factor de ineficacia en los derechos de las personas, sino también el terreno más fecundo para la corrupción y el arbitrio. La intención de tipificar los delitos informáticos, debe ser evitar la inseguridad jurídica en la que pueden estar las personas en relación con ella. Es por ello que los tipos penales, en concordancia con la necesidad de garantizar la seguridad jurídica de los sujetos en que hacen uso de las tecnologías deben gozar de la generalidad y abstracción suficiente como para adaptarse a los cambios vertiginosos de las tecnologías. | El informante asegura: *"Principalmente la tecnología, al no tener las licencias adecuadas para obtener la información, como en el caso de los iphone, falta actualizarnos tecnológicamente".* | Creemos que la informante no entendió bien la pregunta, consideramos que respondió en cuanto a la dificultad que tienen para acceder a los sistemas operativos de algunos dispositivos para realizar la investigación requerida; si bien cierto, el avance de la tecnología ha ayudado en gran manera al desarrollo de las distintas áreas en que se desenvuelve el ser humano, pero a la vez ha traído herramientas que ayudan a la comisión de delitos y de cierta manera las empresas proveedoras dan cierto tipo de protección, como google, iphone, facebook, entre otros. |

| MATRIZ DE ANÁLISIS DE LA INFORMACIÓN POR MEDIO DE LA TRIANGULACIÓN, ENTREVISTA AL MAGISTRADO DE LA CAMARA DE LO PENAL DE OCCIDENTE | | | |
|---|---|---|---|
| PREGUNTA | DOCTRINA | RESPUESTA DE INFORMANTE | OPINIÓN DE GRUPO |
| **1. ¿Qué entiende como "delitos informáticos y conexos" y cuáles son las características que deben reunir las conductas típicas para ser consideradas delitos de esta naturaleza?** | Según la doctrina los delitos informáticos son: *"todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro."* | El informante expresó lo siguiente: *"Son todos aquellos delitos cometidos a través de medios tecnológicos pero en especial a los delitos contemplados en la ley especial de delitos informáticos y conexos. SI bien es cierto en el Código Penal se regulan ciertas conductas que podrían encajar dentro de los "Delitos Informáticos"… no lo asumimos de esa manera, pareciera ser que nosotros creemos que delitos informáticos son exclusivamente aquellos que están contemplados dentro de la Ley Especial de Delitos Informáticos y Conexos, pero en estricto sentido son todos aquellos cometidos, esencialmente, por medios tecnológicos… Una de los características más importantes, es que se haya hecho uso de las tecnologías en cualquiera de sus variantes; no simplemente a través de un computador, teléfono; si no que en todas aquellas variantes en donde se utilizan inclusive algún tipo de dispositivo electrónico".* | Los delitos informáticos en concordancia con la doctrina y lo expuesto por el informante podrían ser, no solo hechos aislados contenidos dentro de la Ley Especial Contra los Delitos Informáticos y Conexos; sino también aquellos actos u omisiones típicas, antijurídicas y culpables que se cometen contra un sujeto pasivo sobre el cual se causa un agravio a un bien jurídico tutelado por el Estado, en los cuales se emplean las Tecnologías de la Información y la Comunicación ya sea esta última como medio o como fin en sí misma. |

| | | | |
|---|---|---|---|
| **2. ¿Qué instrumentos legales actuales son implementados dentro del ordenamiento jurídico salvadoreño para ejercer control dentro del ciberespacio?** | Existe una variedad de Leyes tanto Nacionales como Tratados Internacionales que tal como lo establece la Constitución de la República, si son reconocidos, firmados, ratificados forman parte de las Leyes de las cuales el Estado Salvadoreño puede hacer uso, reconocimiento, prevalencia de Derechos y Bienes Jurídicos. Entre estas Leyes tenemos: Código Penal, Ley Contra Delitos Informáticos y Conexos. | El informante explica: *"En El Salvador, somos reacios respecto al control del ciberespacio debido a que este representa una evolución de gran escala más allá de las tecnologías "5g" que va a ser muy difícil tener la capacidad de controlarlo, ya que cada vez se abren nuevas vías para el control del internet o el control de las TICs y no solo exactamente del internet; La información, como mencionaba anteriormente, puede ser de tantas maneras. Significa que, por un momento podemos controlar sobre el internet, en estricto sentido, no será posible ejercer control sobre las otras vías de información y que, precisamente, puede tener acceso la mayoría de ciudadanos, específicamente los jóvenes. Como no existe una ley específica, desde mi punto de vista, que hable sobre cuáles van a ser los parámetros de la utilización del internet, horarios, contenidos, entre otros… No hay control y, como no existe ese control, estas tecnologías se prestan para la realización de hechos delictivos.*<br>*El único control al que nos podríamos referir dentro del internet es el "Control Parental" en el cual el padre de familia ejerza un* | En el país las leyes existentes no se encuentran en armonía con el avance de las tecnologías de manera tal, que no es posible regular el tráfico de datos dentro del ciberespacio. De alguna manera, con el Código Penal y la Ley Especial Contra los delitos informáticos y Conexos el legislador busca prevenir determinadas conductas que contravengan el orden público en las cuales se utilicen las Tecnologías de Información y Comunicación. Sin embargo, a pesar de esos esfuerzos no existe una ley específica en la cual se establezcan los parámetros para la utilización de las TIC´s. |

| | | | |
|---|---|---|---|
| | | *poco de presión para verificar los contenidos a los que accesan los jóvenes, ya que de parte del Estado, la Dirección General de Espectáculos Públicos, Radio y Televisión perteneciente al Ministerio de Gobernación, en alguna medida, puede ejercer un control. En otras palabras, prácticamente el internet, no es controlable porque las vías de ingreso están bastante diversificadas y, en ese sentido, no podemos abarcarlas y si, algún día van a ser regulados, serán regulados de forma superficial.".* | |
| **3. ¿Cuáles son los riesgos a los cuales se exponen los niños, niñas, adolescentes y personas incapaces que tienen acceso a las Tecnologías de Información y Comunicación (llámese, celulares inteligentes, consolas de videojuegos, redes sociales, entre otros), de ser positiva su respuesta, describa los riesgos a los cuales están** | Dentro de los riesgos a los cuales se exponen los niños, niñas y adolescentes podemos marcar la diferencia entre los delitos con connotación sexual y los delitos comunes pero de los que se hace uso de las TIC´S para su finalidad, dentro de la primera categoría tenemos el grooming, el sexting, la sextorsión, revenge porn, stalking, y la siguiente categoría podemos mencionar la depredación sexual infantil, violación, | El Informante Manifiesta: *"Los riesgos del internet son todos aquellos ataques que pueden sufrir los niños, niñas y adolescentes, tales como el "Ciberbullying", "Stalking", "Grooming", "Sexting", todo ese tipo de conductas a medida de que el niño, niña o adolescente va adquiriendo ese tipo de inteligencia… a medida de que estos accedan a las TICs, adquieren ciertos compromisos; por ejemplo aquellos que en alguna medida adquieren acceso a tarjetas de débito podrían ser víctimas de estafas, transacciones oscuras… Pero específicamente, en mayor proporción nos referimos a los delitos de naturaleza sexual tales como* | Como grupo opinamos que los riesgos a los cuales se exponen los niños, niñas y adolescentes que tienen acceso a las Tecnologías de Información y de la Comunicación son bastante amplios; es importante advertir que estos sujetos generalmente, no poseen una orientación adecuada sobre el correcto uso de las tecnologías y de los riesgos que pueden encontrarse haciendo uso de las mismas de manera de prevenir que los niños, niñas y adolescentes sean víctimas de posibles depredadores sexuales quienes se escudan tras los |

| | | | | |
|---|---|---|---|---|
| | **expuestos los sujetos relacionados ad supra y cuales instituciones estatales velan por la protección de estas potenciales víctimas?** | secuestro, privación de libertad, estafa, entre otros. | *"sexting", "stalking" o en el peor de los casos la pornografía infantil".* | beneficios que ofrecen las diferentes tecnologías para facilitar el cometimiento de los delitos informáticos. En cuanto a las instituciones encargadas de la protección de la niñez y la adolescencia es el CONNA el encargado de la aplicación de políticas públicas para atender a las niños, niñas y adolescentes víctimas de Delitos Informáticos. |
| **4.** | **¿Cuáles son las ventajas y desventajas del control estatal sobre el ciberespacio?** | En los países más avanzados tecnológicamente se argumenta que el control estatal del ciberespacio se debe a la protección de los intereses de Seguridad Nacional y de seguridad pública prueba de ello es que en sectores de capas profundas del internet es donde las agencias de inteligencia recolectan información del crimen organizado, sin embargo estos accesos requieren de conocimiento tecnológico avanzado para la navegación, sin lo cual los particulares no pueden acceder, es ahí donde nacen | El Informante expresó: *"Ventajas si al caso está, más allá de la oposición que tienen los periodistas, las empresas de telecomunicaciones, porque van a alegar que es una censura previa y la constitución prohíbe la censura… Más allá de eso es bueno; pero una regulación vamos a clasificarlo así: a) una regulación "blanda" y b) existe una regulación "dura". Cuando hablamos de una regulación blanda nos referimos solo a aspectos tales como la "metadata" sobre informes del usuario, informes sobre al horario de ciertos contenidos, pero sobre exactamente sobre el contenido de los programas sobre que el Estado imponga "lo que debemos ver" y que "no debemos ver", eso tampoco. Podrá ejercer cualquier otro tipo de control pero regularlo de una manera "dura" por así decirlo no se puede si va a* | El control sobre el ciberespacio en primera instancia, es imposible aplicarlo sin afectar los Derechos Fundamentales consagrados dentro de la Constitución, tratados internacionales, entre otros; puesto que este control presupone coartar ciertas libertades de los individuos en el pleno goce de sus derechos que hacen uso de las tecnologías de la información y de la comunicación; en este sentido, el Estado no debe aplicar un control que limite el contenido al cual el usuario quiere acceder sino, la forma en la cual el usuario tendrá acceso a determinada esfera de la información a través de las TIC's, tales como: establecer |

| | | | |
|---|---|---|---|
| | algunas polémicas si el ciberespacio debe de ser controlado totalmente por los Estados o si debe de permanecer esa fuente de información.<br>En cuanto a las desventajas se sabe que el ciberespacio no puede ser controlado localmente por los Estados sin que se ordene su bloqueo a diferentes dominios, también se plantea la idea que existan algoritmos que clasifiquen, adviertan y bloqueen la publicación de material multimedia o textos publicados en las redes sociales o en la comunicaciones a través de las plataformas más populares actualmente. | *graduar o a legislar algo del núcleo de la información, no es viable. Pero si lo hace desde el aspecto blando que tiene que ver con "los datos de los datos" entonces, ahí no habría ningún problema.*<br><br>*Lo que se pretende es que los contenidos que se van poner en las TIC´s pase ciertos filtros como de franjas horarias en las que el contenido va a estar disponible para determinados sector de la población. Por ejemplo; Petronilo está de vacaciones y quiere ver contenido triple X a las 9 de la mañana. El Estado puede poner ciertas normas que ese contenido solo estará disponible después de las 10 de la noche; por otro lado controlar con quién va a ver él ese contenido es algo en lo que el Estado no debe inmiscuirse".* | franjas horarias al contenido explicito, rangos de edad para los cuales la información puede ser consumida, advertencias sobre contenido explícito o sensible para sectores de la población vulnerables, tales como son los niños, niñas y adolescentes; entre otros. Por otro lado es importante la aplicación de controles informales del ciberespacio para la protección de los niños, niñas y adolescentes, tal como en control parental sobre el contenido al cual tendrán acceso los niños, niñas y adolescentes bajo su cuido. Aunado a ello creemos que es necesario que el Estado implemente políticas públicas sobre la concientización de los padres de los riesgos a los cuales se encuentran expuestos dentro del ciberespacio. |
| **5. ¿Es necesario la existencia de normativas jurídicas que permitan al Estado ejercer control total sobre las tecnologías la información de y la comunicación?** | Las normativas Jurídicas del sector de Derecho Penal son las expresión de imperio del Estado por sobre el elemento humano y de estricto cumplimiento, las mismas de acuerdo a diferentes teóricos tienen la finalidad de imponer penas | El Informante dijo: *"Control total no. Siempre he dicho que el Estado debe mantenerse al margen de las libertades individuales, así de sencillo. Por eso yo digo que ese control blando debe atribuírsele a otras instituciones. Por Ejemplo; yo digo "Quiero ver X película que trata de volar cerebros en esos* | Como grupo creemos que, como lo ha expresado el informante, el Estado debe mantenerse al margen de las libertades de cada individuo. Esto es, no debe aplicarse control sobre los contenidos que estarán disponibles para los usuarios de las tecnologías de la información |

| | | | |
|---|---|---|---|
| | a delitos, al imponer penas regular las conductas de los individuos dentro de la sociedad.<br>Las normas administrativas también son de obligatorio cumplimiento y rigen o determinan el comportamiento de los servidores públicos y de los particulares frente a la Administración pública; al relacionar los dos tipos de reglas se planifican lineamientos tanto entre las responsabilidades penales como las relaciones entre el Estado y los particulares en cuanto a la administración del ciberespacio. | *casos el Estado debe advertir la peligrosidad del contenido" es decir, debe existir un control menor pero no un control en estricto sentido, es decir, prohibitivo para ciertos programas no debería existir".* | y de la comunicación; sino que el Estado debe regular la forma en la que los usuarios van tener acceso a determinados contenidos; pero no controles sobre el fondo del contenido en cualesquiera de sus formas (siempre y cuando el contenido no altere el orden público) de manera que estos controles no coarten Derechos Fundamentales del individuo. |
| **6. ¿Qué impacto puede tener la censura estatal del ciberespacio frente a las libertades individuales de las personas dentro de la sociedad?** | Censura: Se refiere a la intervención que realiza un censor sobre el contenido o la forma de una obra, atendiendo razones morales, políticas, ideológicas, religiosas o de otro tipo, la censura de esta manera, se supone prevenir o limitar una expresión por considerar que sus contenidos pueden ser | El Informante manifestó: *"Mucho impacto. Una censura total, un control "duro" no es conveniente ya que ella limita la libertad de acceder a la información, la autodeterminación informática donde el yo tengo además el deber de recibir información así también existe el derecho de exigir que la información llegue a mí de una forma íntegra y sin ningún tipo de sesgo… Para mí tiene que ser,* | Como lo mencionamos anteriormente, no es víable que el Estado aplique una censura sobre el ciberespacio debido a que, a consecuencia de esta censura, presupondría un menoscabo a las libertades de los individuos que hacen uso de las TIC's, independientemente de si reúnen los requisitos para el consumo de ciertos contenidos dentro del ciberespacio. Sin embargo, |

| | | | |
|---|---|---|---|
| | ofensivos o dañinos; La censura, por lo general, está asociada a la intención de un gobierno de impedir la difusión de información contraria a sus intereses. En las sociedades democráticas, la censura previa suele estar prohibida: es decir, los gobernantes no tienen derecho de impedir la publicación de ningún material. En caso que dicho material, una vez hecho público, incurra en un delito, la Justicia puede tomar las medidas correspondientes. | *definitivamente, no debe existir ese control o regulación sobre el ciberespacio sobre los aspectos "de fondo" por así llamarlo, de la información y respecto de las tecnologías ".* | consideramos importante que el Estado, armonice la legislación con el desarrollo tecnológico de forma tal que sea posible identificar al usuario previo a acceder a determinados contenidos dentro del ciberespacio así como también franjas horarias dentro de las cuales el contenido estará disponible para los usuarios. |
| **7. ¿Considera a la censura estatal del ciberespacio Como una alternativa viable para la protección de los menores de edad frente a contenido potencialmente explicito dentro del internet?** | Se considera censura estatal como la acción que ejerce un gobierno que utiliza herramientas tecnológicas y jurídicas con la finalidad de supervisar, evaluar, sancionar , controlar y prohibir las actividades que realizan los ciudadanos en sus actividades cotidianas. Durante el taller Libertad de Expresión en Internet: aspectos regulatorios en | El informante expresó: "*Siempre he estado en contra de la censura por parte del Estado ya que ella también limita mi libertad de expresión, claro, libertad de expresión no significa decir cualquier cosa, sino que libertad de expresión, mientras ella no afecte a un tercero. Si no, qué decir y expresarme de la forma que a mí me parece correcta dentro de los parámetros legales. Por eso no lo veo que haya necesidad de utilizar* | La censura estatal no es propia de los Estados democráticos en los cuales prevalezca el Estado de derecho. Como ya hemos mencionado anteriormente, la censura presupone una vulneración flagrante a los derechos fundamentales de los individuos y, más específicamente, a los libertades de los individuos. No obstante ello, el Estado debe estar a la vanguardia de la revolución |

| | | | |
|---|---|---|---|
| | América Latina, organizado por el profesor Eduardo Bertoni, se analizó el rol que corresponde a los Gobiernos en la protección de la libertad de expresión en Internet y en la sanción de expresiones nocivas, tanto en forma directa como mediante la regulación de los intermediarios. También se evaluó la función que desempeñan los Gobiernos en la regulación de los proveedores de servicios de Internet para facilitar el libre flujo de información. | *la censura como una prima ratio en materia del internet."* | tecnológica, capacitar y dotar de las herramientas necesarias a las instituciones encargadas de la tutela y protección de uno de los sectores más vulnerables de la población como lo son los niños, niñas y adolescentes; para la aplicación de políticas públicas encaminadas a velar por el desarrollo psicológico y social integral de los niños, niñas y adolescentes de los niños, niñas y adolescentes. |
| **8. ¿Cuáles son las variables que afectan la eficacia del procedimiento judicial llevado a cabo en contra de los delitos cibernéticos y principalmente a aquellos de índole sexual cometidos contra niños, niñas y adolescentes?** | Las medidas legales son cruciales para la prevención y el combate del delito cibernético, y se las requiere en todas las áreas, para que cubran la criminalización, los poderes procesales, la jurisdicción, la cooperación internacional y la responsabilidad de los proveedores de servicios de Internet. | El informante manifestó: "*Aquí nos encontramos ante dos circunstancias; la primera: Cuales los son los tres tipos de delitos que se pueden dar? El primero en contra de los programas; el segundo tipo tiene que ver con los delitos cometidos en contra de la información. En el primero lo que se pretende es destruir programas; en el segundo lo que se pretende es extraer información y la otra es por medio de, es decir, utilizar la tecnología para cometer un delito; entonces si utilizamos la tecnología* | Las variables que tienen afectan la eficacia de los procedimientos judiciales contra los delitos informáticos se dan en atención al tipo de delito que se consuma. En primera instancia los delitos en los cuales la tecnología es el fin del acto ilícito, una de las variables que afectan los procesos judiciales es la dificultad para individualizar al sujeto activo y la valoración probatoria pues estos factores exigen una investigación técnica más compleja sobre el delito. En |

| | | | |
|---|---|---|---|
| | | *para ese tipo de delitos, ahí es donde de parte del agente persecutor están las dos vías, por ejemplo: "X buscó en OLX"… pero no se propone como una estafa en ese sentido, lo ponen ESTAFA CON UTILIZACIÓN DE UNA TECNOLOGÍA. En estos casos la investigación no se centra en el método si no que en el resultado. Cuando se trata de la pornografía de igual manera lo convierte en un delito tradicional, con la utilización de la Tecnología pero como elemento secundario. No le ven como un delito a través de la web y le dan prioridad a la investigación científica o a la utilización de los medios tecnológicos. El problema que existe en el país es que la FGR no quiere meterse de lleno a la investigación informática y se le da un tratamiento de un delito convencional, ese es el principal problema que presenta los delitos de pornografía infantil a través de los medios tecnológicos. Es una maraña de investigación en la cual no estamos en la capacidad nosotros, tanto el ente persecutor del delito para afrontar ese reto.* | cuanto a los delitos en los cuales se utiliza a las TIC's como medio para el cometer el ilícito, los factores más importantes a considerar para la eficacia de los procesos judiciales tiene que ver con la especialización de los sujetos investigadores y persecutores del delito en el país como lo es la Fiscalía General de la República; la facilidad de acceso a las TIC's por parte de los usuarios y el hecho de que no existan los controles a los que hemos hecho referencia previamente, los delitos de esta naturaleza son cometidos con facilidad y frecuencia. No obstante lo anterior, existe una cultura bastante marcada en los agentes encargados de la persecución e investigación del delito, en el cual este último no les da el tratamiento como delitos informáticos si no, como delitos comunes. |
| **9. ¿Cuáles son las políticas públicas aplicadas a nivel** | | El informante expresó: *"NINGUNA. De parte del Estado no existe* | Hasta la fecha no se conoce de ninguna política pública |

| | | | |
|---|---|---|---|
| **institucional para el control de la cibercriminalidad, en cualquiera de sus formas, a efectos de garantizar protección integral de los niños, niñas, adolescente y personas incapaces con acceso a las Tecnologías de la Comunicación e información?** | | *ninguna política pública encaminada al combate de la cibercriminalidad, en donde todas las instituciones estén involucradas".* | encaminada a la prevención de los delitos de esta naturaleza. |
| **10. ¿Considera que dentro el ordenamiento jurídico actual, existe un tratamiento eficaz en contra de los delitos cibernéticos y en específico aquellos de índole sexual en contra de menores de edad?** | El 26 de febrero de 2016 se aprobó la Ley Especial contra Delitos Informáticos y Conexos, mediante el Decreto Legislativo No. 260, publicado en el Diario Oficial No. 40 Tomo No. 410, de la misma fecha; la cual sistematiza los tipos penales relacionados con la ciber delincuencia, generando en los operadores de justicia nuevos desafíos para su aplicación y sanción penal, por cuanto la referida normativa se encuentra relacionada con la utilización de tecnologías de la información y comunicación; de tal | El Informante asegura: *"Un tratamiento eficaz a los delitos informáticos no existe, y como no existe ese tratamiento a los delitos de esta naturaleza, se le da paso a la impunidad y sobre todo a los cometidos en contra de los niños, niñas y adolescentes. Cuando hablamos de tratamiento, me refiero a la investigación. Como no hay forma, no hay manera y no hay los recursos para investigar estos delitos.".* | Según el informante, a pesar de la existencia de la Ley de Especial Contra los Delitos Informáticos y Conexos, no existe un tratamiento eficaz para los delitos de esta naturaleza y, en consecuencia, da lugar a la impunidad de los mismos principalmente, a los delitos de naturaleza sexual cometidos a través de las TIC's. El informante enfatiza en las falencias respecto a la investigación de estos delitos. En razón de ello, como grupo incitamos que es menester para el Estado invertir en desarrollo tecnológico para las instituciones encargadas de la persecución e investigación del delito. |

| | | | |
|---|---|---|---|
| | manera que la investigación, procesamiento y juzgamiento, están condicionadas a laplicación de actividades técnicas y periciales informáticas. | | |
| **11. ¿Cuál es el impacto psicológico y social en el cual se ven inmersos las víctimas menores de edad, de delitos cibernéticos de índole sexual?** | A través de estudios psicológicos se descubrió que los daños que causan eventos de violencia sexual en los NNA son diversos, entre los delitos informáticos que implican acoso, sexting se encuentran: sentimientos negativos de culpa, vergüenza, culpa o ira, ansiedad, depresión, pérdida progresiva de confianza propia; en los casos que implica acceso carnal y haberse utilizado las TICS como medio de comunicación para consumar el hecho además de las anteriores secuelas psicológicas se encuentran: problemas emocionales, problemas de relaciones interpersonales, problemas de conductas y adaptación | El informante manifiesta: *"Temor, vergüenza, auto recriminación, inseguridad personal y social, baja autoestima, depresión, puede llegar a ser un repetidos de conductas si no se le da un tratamiento adecuado, la familia también sale afectada cuando no pudieron hacer nada sobre el hecho y sienten impotencia".* | Como grupo consideramos que a los niños, niñas y adolescentes al haber sido víctimas de un delito de índole sexual a través de las TIC's según lo expresado por el informante, concuerda con estudios psicológicos sobre los daños que causan los eventos de violencia que implica el flamming, sexting, "revengeporn", entre otros; lo cual implica una auto recriminación, baja autoestima y depresión. |

| | | | |
|---|---|---|---|
| | social, funcionales, revictimización, sexuales, transmisión intergeneracional, abuso de drogas y/o alcoholismo, entre otros. | | |
| **12. ¿Cuáles son las principales falencias observables en el Estado salvadoreño para la positivización de la Ley Especial Contra los Delitos Informáticos y Conexos de manera que se logren reducir efectivamente los delitos de esta naturaleza?** | Para Luigi Ferrajoli, el deterioro de la forma de la ley, la falta de certeza generalizada a causa de la incoherencia y la inflación normativa, representan no solo un factor de ineficacia en los derechos de las personas, sino también el terreno más fecundo para la corrupción y el arbitrio. La intención de tipificar los delitos informáticos, debe ser evitar la inseguridad jurídica en la que pueden estar las personas en relación con ella. Es por ello que los tipos penales, en concordancia con la necesidad de garantizar la seguridad jurídica de los sujetos en que hacen uso de las tecnologías deben gozar de la generalidad y abstracción suficiente como para adaptarse a los cambios vertiginosos de las tecnologías. | El informante expresó: *"Lo que falta es preparación por parte del ente persecutor, dejar de tener miedo a investigar los delitos informáticos cometidos por medio de la tecnología… A encontrar las formas de cómo se puede encontrar la información. ".* | Según la información que se extrae del informante, manifiesta que es observable la falta de preparación del ente persecutor para investigar los delitos de naturaleza informática; el deber del Estado es dotar de recursos tanto técnicos como instrumentales al ente Fiscal para garantizar la eficacia de la Ley Especial Contra los Delitos Informáticos y Conexos. Por otro lado, generar políticas públicas con la finalidad de prevenir la delincuencia informática y salvaguardar la indemnidad sexual de los niños, niñas y adolescentes quienes son potenciales víctimas. |

| MATRIZ DE RESPUESTAS MÉTODO DE VACIADO DE INFORMACIÓN, ENTREVISTA REALIZADA A ABOGADO DE LA REPÚBLICA, EXPERTO EN EJERCER DEFENSA TÉCNICA EN CUANTO A LA INVESTIGACIÓN DE DELITOS INFORMATICOS Y CONEXOS | | | |
|---|---|---|---|
| **PREGUNTAS** | **DOCTRINA** | **RESPUESTA INFORMANTE** | **OPINIÓN DE EQUIPO** |
| **1. ¿Qué entiende como "delitos informáticos y conexos" y cuáles son las características que debe reunir las conductas típicas para ser consideradas delitos de esta naturaleza?** | Según la doctrina los delitos informáticos son: "todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro." | *El informante expresó lo siguiente: "Se considera que el Delito Informático es aquel que se comete a través del Internet, pero estamos hablando del Delito que utiliza medios informáticos para la comisión misma del hecho, pero se llega a la conclusión, que eso es indiferente que al final basta que el delincuente se valga de Tecnologías de la Información y Telecomunicación, independientemente con que utilice internet, independientemente que afecte sistemas informáticos; es decir se toma más en consideración el sistema que se está utilizando que son las TIC´S, ya sea un teléfono celular, una cámara inteligente, hasta un televisor inteligente todo eso se puede utilizar, entonces esa es la idea técnica de la consideración del delito, existen ideas equivocadas que estos delitos son cometidos solamente en el* | El informante expone ampliamente su respuesta a la pregunta, puesto que ubica el universo del que comprenden los delitos informáticos, ya que aunque existe abundante información al respecto, en la práctica muchos desconocen la estructura típica de los delitos, la valoración de la prueba, la individualización de los sujetos activos y no pueden diferenciar los métodos de cómo se investigan; también cabe recalcar que esto es como un efecto dominó, en la cual los ciudadanos no tienen la cultura de denunciar que han sido víctimas de delitos, por ende no se judicializan ni se les proporciona una pronta y cumplida justicia. |

| | | | |
|---|---|---|---|
| | | *internet, está sumamente equivocado porque el vehículo para comisión del delito es el internet en la medida en que no sea un contacto físico esa sería una construcción bien amplia y que incluso si te pones a pensar que la idea del delito es la intersubjetividad en la comisión de estos delitos hay delitos en los que ni siquiera hay contacto sino que lo que hay es una especie de anonimato y una imposibilidad de identificar quién es el sujeto activo, siempre se identificará un hecho delictivo que sea basado en la realidad y con los instrumentos tradicionales del Derecho Penal no es posible demostrarlo, para ello se necesita hacer uso de una nueva configuración teórica para poder interpretarlo, por ejemplo la tentativa se penaliza en algunos casos, pero en los delitos informáticos la tentativa se da como delito consumado (si una persona ingresa ilegalmente a un sistema o base de datos, ya es un delito consumado)".* | |
| **2. ¿Cuáles son los** | Existe una variedad de Leyes | El informante explica: "*Pues* | Como grupo opinamos que |

| | | | |
|---|---|---|---|
| **instrumentos legales actuales que son implementados dentro del ordenamiento jurídico salvadoreño para ejercer control dentro del ciberespacio?** | tanto Nacionales como Tratados Internacionales que tal como lo establece la Constitución de la República, si son reconocidos, firmados, ratificados forman parte de las Leyes de las cuales el Estado Salvadoreño puede hacer uso, reconocimiento, prevalencia de Derechos y Bienes Jurídicos. Entre estas Leyes tenemos: Código Penal, Ley Contra Delitos Informáticos y Conexos. | *tenemos ausencia de una normativa, que permita trascender o normar el ciberespacio porque al ciberespacio no lo controla nadie; sino tenemos control de ello, probablemente ni siquiera una ley va a permitir o negar el acceso, pero por lo menos disponemos de una Ley contra los Delitos informáticos, el Código Penal que sirve para la persecución de delitos pese a las limitaciones que tiene en cuanto a su alcance pero hay una necesidad bastante grande de ampliar las consideraciones y construcciones de la evidencia virtual, de la evidencia informática, los fundamentos de la evidencia virtual, por lo tanto creo que no tenemos más herramientas que eso, y una necesidad de ser parte al menos de los Estados que se han adherido al Convenio de Bruselas.*<br>*Por ejemplo la Deep Web, en cuanto a tema ético sería conveniente cerrarlo puesto que nada bueno circula a través de esa parte de la red, sin embargo en cuanto a ciber seguridad pues no es muy conveniente* | aunque no exista una Ley que taxativamente regule al ciberespacio, de alguna forma las Leyes mencionadas en la Doctrina, permiten configurar el material multimedia y los datos que circulen a través de las redes sociales y el internet ya que en cierta forma las personas que tienen acceso a las TIC´S, pueden ser víctimas de delitos informáticos como de ser victimarios y más cuando los primeros son niñas, niños y adolescentes sin algún tipo de supervisión por parte de los adultos o en dado caso no tienen orientación de las consecuencias de las actividades que realicen en redes sociales o los accesos y contactos que tengan en cualquier sitio de internet.<br>Si bien es cierto, en la pregunta y en la respuesta del entrevistado no se mencionan las Leyes nacionales y Tratados internacionales que protejan los Derechos de los niños, niñas y adolescentes; como grupo creemos que la sola configuración de tipos penales que sirvan de herramientas para la investigación, la |

| | | | |
|---|---|---|---|
| | | *para las agencias de inteligencia internacionales, puesto que es ahí donde se puede obtener información de los movimientos del crimen organizado, es como que te pongás una venda en los ojos y no sepas que está haciendo una persona que puede generarte a futuro algún problema, como que tengás un enemigo y le pongas un muro entre él y vos, esto en cuanto a ciber seguridad".* | individualización de los sujetos pasivos y castigo de los delitos informáticos, permiten de manera positiva ejercer control del ciberespacio, puesto que prevalece el interés público de perseguir y reprimir los delitos por sobre los intereses de los particulares que puedan hacer uso del ciberespacio para cometer los ilícitos. |
| **3. ¿Cuáles son riesgos a los cuales se exponen los niños, niñas, adolescentes y personas incapaces que tienen acceso a las Tecnologías de Información y Comunicación (llámese, celulares inteligentes, consolas de videojuegos, redes sociales, entre otros)? y de ser positiva su respuesta, describa los riesgos a los cuales están expuestos los sujetos relacionados ad supra y cuales** | Dentro de los riesgos a los cuales se exponen los niños, niñas y adolescentes podemos marcar la diferencia entre los delitos con connotación sexual y los delitos comunes pero de los que se hace uso de las TIC´S para su finalidad, dentro de la primera categoría tenemos el grooming, el sexting, la sextorsión, revenge porn, stalking, y la siguiente categoría podemos mencionar la depredación sexual infantil, violación, secuestro, privación de libertad, estafa, entre otros. | El Informante Manifiesta: "*Al no existir un debido control de parte de los padres, este no es un tema del Estado sino que le compete directamente a los padres, los niños están expuestos a cualquier tipo de riesgos, imagínate algo a los que se exponen a algo directamente como intercambio de fotos, programación de citas con adultos y que sean depredadores sexuales, y no solamente se someten a temas de buyling o algo sino hasta sufrir temas de algo sexual, son una variedad de problemas que se han generado".* | Como grupo opinamos que se han expuesto de manera amplia los delitos a los cuales se exponen, asimismo opinamos que aunque los niños, niñas y adolescentes tienen acceso a las TIC´S, muchos no tienen una orientación idónea de parte de adultos responsables al respecto del uso positivo de las redes sociales y el contenido multimedia al cual pueden acceder. En cuanto a la protección de las víctimas creemos que el ISNA, como representante de políticas públicas encaminadas a la protección de la niñez y adolescencia, no ha hecho |

| | | | |
|---|---|---|---|
| **instituciones estatales velan por la protección de estas potenciales víctimas?** | | | pública hasta esta fecha una estrategia o un plan integral que tenga incidencia en los delitos informáticos que se dan contra de este sector de la población, la FGR y PNC, aunque no protegen de forma permanente a cada individuo, de forma secundaria a través de la investigación y posterior condena de los sujetos activos de estos delitos permiten la protección de otros menores que pueden ser potenciales víctimas. |
| **4. ¿Cuáles son las ventajas y desventajas del control estatal sobre el ciberespacio?** | En los países más avanzados tecnológicamente se argumenta que el control estatal del ciberespacio se debe a la protección de los intereses de Seguridad Nacional y de seguridad pública prueba de ello es que en sectores de capas profundas del internet es donde las agencias de inteligencia recolectan información del crimen organizado, sin embargo estos accesos requieren de conocimiento tecnológico avanzado para la navegación, sin lo cual los particulares no pueden acceder, es ahí donde nacen algunas polémicas si el ciberespacio | El Informante expresó: "*Yo creo que como no es controlable el ciberespacio, te puedo decir que no tengo una respuesta para eso sino que es una desventaja no tener control en el ciberespacio, si la teoría te dice que es el quinto espacio que forma parte del control del Estado, ese es el quinto espacio del cual el Estado no tiene control, si te dijera una ventaja o una desventaja, prácticamente te estaría dando una respuesta imposible porque la desventaja es no tener el control sobre el ciberespacio, osea no hay forma. Pero es de tener cuidado, control desde la* | Como grupo opinamos que el control total estatal del ciberespacio en primer lugar es casi imposible de aplicarlo tecnológicamente sin vulnerar los Derechos Fundamentales de los ciber usuarios, en segundo lugar creemos que los avances tecnológicos no deben de socavar los esfuerzos del combate de los delitos informáticos, sino más bien debe de fortalecerse las herramientas de entendimiento con el sector privado que son los que proveen el internet y con los que proveen las plataformas de comunicación.<br>No obstante, también creemos |

| | | | |
|---|---|---|---|
| | debe de ser controlado totalmente por los Estados o si debe de permanecer esa fuente de información.<br>En cuanto a las desventajas se sabe que el ciberespacio no puede ser controlado localmente por los Estados sin que se ordene su bloqueo a diferentes dominios, también se plantea la idea que existan algoritmos que clasifiquen, adviertan y bloqueen la publicación de material multimedia o textos publicados en las redes sociales o en la comunicaciones a través de las plataformas más populares actualmente. | *perspectiva tecnológica es difícil controlarlo puesto que hasta a los países más desarrollados es complicado mantener un control, pero si la vemos desde la perspectiva de control formal sería mediante la creación de una ley, pero esta no te garantiza pues que tecnológicamente sea efectiva, entonces estamos ante una especie de algo que se conoce como Derecho Simbólico o norma simbólica que se dedican en cualquier país y que al final no tienen una finalidad de control específico y real sino que solo la idea de que existe una ley y que esta ley ha llenado el vacío legal que se tenía".* | que los controles informales del ciberespacio son importantes para un mejor uso del mismo, puesto que son los mismos usuarios los que a través de popularidad de búsqueda los que en algunos casos configuran las preferencias del contenido visualizado en los motores de búsqueda; aunado a lo anterior se tiene que aumentar el control parental de parte de los padres junto con la concientización de estos hacia los NNA. |
| **5. ¿Considera necesaria la existencia de normativas jurídicas que permitan al Estado ejercer control total sobre las tecnologías la información de y la comunicación?** | Las normativas Jurídicas del sector de Derecho Penal son las expresión de imperio del Estado por sobre el elemento humano y de estricto cumplimiento, las mismas de acuerdo a diferentes teóricos tienen la finalidad de imponer penas a delitos, al imponer penas regular las conductas de los individuos dentro de la sociedad. | El Informante dijo: "*Sí, por ejemplo la idea de la prevención, subir la pena a determinado delito eso no te garantiza que ya no se cometerá dicho delito, solo aquel que verdaderamente tiene la capacidad de entender el remedio de una norma y que le prohíbe hacer algo es el que se abstiene de cometer un delito, otros lo que hacen es buscar la* | Como grupo opinamos que no son necesarias leyes que en estricto sentido regulen el ciberespacio con una intervención total, sino que se debe de trabajar en la eficacia y eficiencia de las leyes ya establecidas para una idónea investigación, judicialización y posterior condena de quien resulte penalmente responsable; puesto que una intervención |

| | | | |
|---|---|---|---|
| | Las normas administrativas también son de obligatorio cumplimiento y rigen o determinan el comportamiento de los servidores públicos y de los particulares frente a la Administración pública; al relacionar los dos tipos de reglas se planifican lineamientos tanto entre las responsabilidades penales como las relaciones entre el Estado y los particulares en cuanto a la administración del ciberespacio. | *manera de como evadir ese control; las compañías que ofrecen servicios de internet podrían en un momento dado mediante un control de ciber seguridad sobre ellos posiblemente podrían identificar a los usuarios, a niños que podrían tener acceso a un aparato tecnológico el niño no puede ir a comprar un celular, será el padre, se identifica el aparato".* | total del Estado salvadoreño dentro del ciberespacio con la finalidad de contrarrestar la comisión de delitos informáticos solamente puede hacerse mediante la vulneración sistemática de Derechos fundamentales de todos los ciber usuarios |
| **6. ¿Qué impacto puede tener la censura estatal del ciberespacio frente a las libertades individuales de las personas dentro de la sociedad?** | Censura: Se refiere a la intervención que realiza un censor sobre el contenido o la forma de una obra, atendiendo razones morales, políticas, ideológicas, religiosas o de otro tipo, la censura de esta manera, se supone prevenir o limitar una expresión por considerar que sus contenidos pueden ser ofensivos o dañinos; La censura, por lo general, está asociada a la intención de un gobierno de impedir la difusión de información contraria a sus intereses. En las sociedades democráticas, la censura previa | El Informante manifestó: *"Puede que sí, sería viable que en determinado momento se pueda llegar a controlar el ciber espacio, por ejemplo llegara a darse en un momento determinado mediante un control sobre las empresas que distribuyen el internet, talvez se podría tener un control, posiblemente se podría identificar que un menor de edad es el que está usando un dispositivo y la empresa que distribuye el internet podría controlarlo, pero si estamos hablando de censura como medio de control frente al uso* | A criterio grupal consideramos que no es viable la censura estatal del ciberespacio, debido a que se estarían violentando Derechos Fundamentales de todos los ciber usuarios independientemente de la edad de los mismos, sin embargo, si en el futuro se puedan establecer algoritmos de identificación de usurarios, lectura de seguimientos del contenido compartido a través de redes sociales, deberán establecerse a iniciativa de las plataformas que brindan el servicio, no obstante creemos que las operadoras |

| | | | |
|---|---|---|---|
| | suele estar prohibida: es decir, los gobernantes no tienen derecho de impedir la publicación de ningún material. En caso que dicho material, una vez hecho público, incurra en un delito, la Justicia puede tomar las medidas correspondientes. | *porque puede impactar y hacer menos vulnerable a los menores, pero habría que establecer un parámetro hasta donde puede acceder un niño porque la Convención Internacional de los Derechos del niño te dice que es desde uno hasta los dieciocho años, pero si estamos hablando de censura restrictiva esa es imposible ya que es contraria a lo que establece la Constitución de la República porque podría afectar hasta los adultos; pero no pierda de vista que hay otros mecanismos factibles y menos dañinos que son parte de la prevención de las empresas que distribuyen el internet como el control parental".* | distribuidoras del internet y cualquier agencia estatal de inteligencia solamente deberán tener acceso a los datos y material multimedia de los usuarios solamente mediante autorización judicial. Bajo el mismo punto de vista creemos que la censura estatal no es propia de los Estados Democráticos donde prevalezca el Estado de Derecho ya que deja a criterio de terceros la facultad de la libertad de expresión, libertad de prensa, derecho al acceso de la información y lo más importante, la libertad de pensamiento. |
| **7. ¿Considera a la censura estatal del ciberespacio como única alternativa viable para la protección de los menores de edad frente a contenido potencialmente explicito dentro del internet?** | Se considera censura estatal como la acción que ejerce un gobierno que utiliza herramientas tecnológicas y jurídicas con la finalidad de supervisar, evaluar, sancionar , controlar y prohibir las actividades que realizan los ciudadanos en sus actividades cotidianas. Durante el taller Libertad de Expresión en | El informante expone: "*No, no creo que sea viable al cien por ciento, además que es imposible sino es mediante mecanismos que sean contrarios a los Derechos fundamentales, siempre he creído que es mejor la orientación y comunicación de los padres hacia los hijos"* | Como grupo, consideramos que la censura estatal no es viable, sino que casi imposible su aplicación sin que se violenten los Derechos fundamentales de los ciber usuarios; no obstante, el material potencialmente explícito que actualmente circula debe de ser contenido con el fortalecimiento tecnológico y capacitación de |

| | | | |
|---|---|---|---|
| | Internet: aspectos regulatorios en América Latina, organizado por el profesor Eduardo Bertoni, se analizó el rol que corresponde a los Gobiernos en la protección de la libertad de expresión en Internet y en la sanción de expresiones nocivas, tanto en forma directa como mediante la regulación de los intermediarios. También se evaluó la función que desempeñan los Gobiernos en la regulación de los proveedores de servicios de Internet para facilitar el libre flujo de información. | | las instituciones encargadas de la investigación de los delitos informáticos. |
| **8. ¿Cuáles son las variables que afectan la eficacia del procedimiento judicial llevado a cabo en contra de los delitos cibernéticos referidos a la pornografía infantil?** | Las medidas legales son cruciales para la prevención y el combate del delito cibernético, y se las requiere en todas las áreas, para que cubran la criminalización, los poderes procesales, la jurisdicción, la cooperación internacional y la responsabilidad de los proveedores de servicios de Internet. | El informante manifiesta: *"Sí, tenemos la ventaja de que cuando se trata de menores de edad existe la prohibición de difusión de imágenes o la información personal de los menores afectados, pero no deja de tener un tacto los prejuicios que se van arrastrando a través de la opinión pública, eso atañe a los legisladores, atañe a la policía, atañe al Fiscal, atañe a los jueces, atañe a medio mundo, entonces hay algunos casos en los que por un tema de arrastre* | La eficacia de la judicialización de las investigaciones de los delitos informáticos depende de muchas variables como la individualización del sujeto activo, la valoración de la prueba, la especialización de los investigadores, fiscales y peritajes realizados.<br>La facilidad de acceso a las TICS por parte de los usuarios es generalizado y al no existir un control previo al contenido compartido ni a los datos personales de los usuarios, la pornografía infantil y similares |

| | | | |
|---|---|---|---|
| | | *de opinión pública este influya en la absolución o la condena, osea eso afectaría la eficacia del proceso y eso afectaría el tema de intuición y sana crítica con que se debe de resolver un caso, por ejemplo en un caso bastante mencionado de un Magistrado que se volvió muy mencionado, muchas personas emitieron sus opiniones y juicios de valor sin tan siquiera conocer cómo se dieron los hechos, hablaban con propiedad, sin tener acceso al expediente y los juzgadores sí conocían lo que había pasado porque estaban aplicando la Ley, es un caso donde la opinión pública influye en casos".* | son delitos que fácilmente se cometen.<br>No obstante, en nuestro país se han hecho grandes avances tanto tecnológicos, como esfuerzos internacionales de implementación de herramientas jurídicas para la persecución de este tipo de delitos, sin embargo en la actualidad se ha presenciado un aumento en la cultura de denuncia por parte de las víctimas y eso es positivo para la investigación científica de los delitos informáticos, el acceso a la justicia y la protección de parte del Estado hacia los NNA. |
| **9. ¿Cuáles son las políticas públicas aplicadas a nivel institucional para el control de la ciber criminalidad, en cualquiera de sus formas, a efectos de garantizar protección integral de los niños, niña, adolescente y personas incapaces** | La aplicación de la Ley de Delitos Informáticos y Conexos con el fin de proteger bienes jurídicos mediante vulneraciones a través de los medios tecnológico | *El informante expone: "No, la verdad que no, esa cuestión tiene que ver con política general del Estado, si lo vemos como política general del Estado es dentro de ello hay un componente que es la política criminal, entonces el Estado a través de esos mecanismos es un poco invisible, pero que cumple grandes efectos de cuando se crea una ley el* | Nuestra opinión la argumentamos con la expectativa de la entrada del nuevo gobierno en cuanto a la legislación de los delitos informáticos que afectan a los NNA, sin embargo hasta la fecha no se conoce un programa integral y novedoso que esté relacionado con el tema investigado; no obstante, coincidimos con la opinión |

| | | | |
|---|---|---|---|
| **con acceso a las Tecnologías de la Comunicación e información?** | | *Estado siempre se pone de agredido, el gran problema es que esto tiene que ver mucho con la orientación que en un momento dado tenga el congreso o como está determinada la Asamblea y quien tiene la disponibilidad de decidir en un momento dado que se aprueba o que no se aprueba en una Ley entonces el Estado se dispone de eso como único mecanismo, está en el Art. 31 numeral 5 de la Constitución".* | vertida de nuestro informante en el sentido que la política criminal de la FGR, debería obtener mayor relevancia este tipo de delitos, sin embargo aunque se cuenta con la Unidad Especializada de Delitos Informáticos, esta solo se encuentra como sede en la capital, no existen regionales pero capacitan a los fiscales. |
| **10. Dentro del ordenamiento jurídico actual, ¿Considera que existe un tratamiento eficaz en contra de los delitos cibernéticos y en específico aquellos de índole sexual en contra de menores de edad?** | El 26 de febrero de 2016 se aprobó la Ley Especial contra Delitos Informáticos y Conexos, mediante el Decreto Legislativo No. 260, publicado en el Diario Oficial No. 40 Tomo No. 410, de la misma fecha; la cual sistematiza los tipos penales relacionados con la ciber delincuencia, generando en los operadores de justicia nuevos desafíos para su aplicación y sanción penal, por cuanto la referida normativa se encuentra relacionada con la utilización de tecnologías de la información y comunicación; de tal manera que la | El informante expresó: *"Si, por lo que he venido viendo el desarrollo de cómo han venido pasando, creo que podríamos ver de una nota 3 a 6, por lo que se está haciendo, hace 3 a 5 años estábamos iniciando en cuanto a los delitos informáticos, claro que hay grandes deficiencias en que a veces el policía a veces manipula cosas que pueden afectar después en el resultado de un proceso pero eso es también falta de la debida capacitación de los agentes pero creo que se está trabajando en eso".* | Como grupo creemos que en cuanto al ordenamiento jurídico, las leyes que se encargan de la investigación, e imposición de las penas si bien es cierto que ha avanzado, se necesita mayor eficacia y eficiencia en la misma, por ejemplo se sebe de descentralizar los laboratorios científicos ya que hasta la fecha solamente se tiene en la DCI de San Salvador, se pueden crear laboratorios con equipo especializado y personal cualificado en regionales en Occidente y Oriente del país; por otra parte también creemos que el Estado Salvadoreño debe |

| | | | |
|---|---|---|---|
| | investigación, procesamiento y juzgamiento, están condicionadas a la aplicación de actividades técnicas y periciales informáticas. Las relaciones entre las partes contratantes. La importancia de cada una de esas normas es diferente y va de mayor a menor, por lo cual las inferiores toman su fundamento de las inmediatamente superiores. A esa jerarquización o escalonamiento es a lo que Merkl y Kelsen denominaron "pirámide jurídica". | | de formar parte del Tratado de Budapest, como parte del compromiso internacional de combatir los Delitos Informáticos. |
| **11. . ¿Cuál es el impacto psicológico y social en el cual se ven inmersos las víctimas menores de edad, de delitos cibernéticos de índole sexual?** | A través de estudios psicológicos se descubrió que los daños que causan eventos de violencia sexual en los NNA son diversos, entre los delitos informáticos que implican acoso, sexting se encuentran: sentimientos negativos de culpa, vergüenza, culpa o ira, ansiedad, depresión, pérdida progresiva de confianza propia; en los casos que implica acceso carnal y haberse utilizado las TICS como medio de comunicación para consumar | El Informante asegura: *"Para los niños no creo que les afecte del momento respecto cuando hay daño sexual de por medio, pero en el medio en que un niño sufre una vulneración de esa naturaleza y se vaya desarrollando posiblemente en la medida en que el desarrollo le va permitiendo saber a qué fue sometido por ejemplo le afecte más en daño gradual y hay el tema de la indemnidad que es la preocupación principal cuando se habla de niños, cuando se habla de* | Como grupo opinamos que el informante expone de manera general lo que los principales teóricos ya dan a conocer, puesto que los NNA, en un principio no comprenden las consecuencias de lo que han sido víctimas, sino que gradualmente y conforme desarrollan y comprenden el mundo que les rodea es que entienden las dimensiones del daño, debido a que aunque presenten los daños psicológicos estos no pueden ser identificados por ellos. |

| | | | |
|---|---|---|---|
| | el hecho además de las anteriores secuelas psicológicas se encuentran: problemas emocionales, problemas de relaciones interpersonales, problemas de conductas y adaptación social, funcionales, revictimización, sexuales, transmisión intergeneracional, abuso de drogas y/o alcoholismo, entre otros. | *delitos con connotación sexual se pretende que el menor sea desarrollado en una sociedad respetando esa natural forma de desarrollarse osea nunca debe de ser sometido a una cuestión a una cuestión previo a la que no está preparado, en la medida en que el niño o niña comprenda al daño en al que ha sido sometido es ahí donde se manifiesta el daño psicológico".* | |
| 12. **¿Cuáles son las principales falencias observables en el Estado salvadoreño para la positivización de la Ley Especial Contra los Delitos Informáticos y Conexos de manera que se logren reducir efectivamente los delitos de esta naturaleza?** | Según el diccionario de español falencia: es una equivocación, idea falsa, carencia o defecto.<br>La positivización de Derechos debe de ser comprendida como la síntesis de un proceso político y jurídico, cuyas etapas comprenden la construcción conceptual de los derechos y libertades y su consiguiente protección a través de la definición de un orden legal. | *"En primer lugar se necesita una política idónea, inversión de recursos, la tecnificación, y agregar el compromiso en que el Estado debe de no solo en dar muestra de quererse adherirse formalmente al convenio de Budapest y suscribirlo, porque eso permitiría estar en la línea en la que los otros Estados están positivamente para no quedarnos con una Ley que se ve buena, pero que al final no se pueda ver el resultado, sin embargo se está aplicando y que desde hace algún tiempo está tomando relevancia".* | Como grupo creemos que la opinión vertida por el informante es concluyente en que el Estado debe generar los recursos, la especialización, actualización de recursos tanto de tecnológicos, de elementos humanos especializados en el área, de creación de una Unidad de Atención a víctimas menores de edad en la PGR o en la FGR, en la cual se establezcan planes estratégicos con la finalidad de velar por los Derechos vulnerados y elaboración de planes didácticos en conjunto con el Ministerio de Educación para difundir la prevención de los Delitos Informáticos en los NNA, en las escuelas, colegios |

| | | | |
|---|---|---|---|
| | | | e institutos nacionales; por otro lado coincidimos con el informante en que el Estado Salvadoreño debe de adherirse al convenio de Budapest, para adquirir un mayor compromiso a nivel internacional en cuanto a los delitos informáticos confiere. |

| MATRIZ DE ANÁLISIS DE LA INFORMACIÓN POR MEDIO DE LA TRIANGULACIÓN, ENTREVISTA REALIZADA A EXPERTO DE INVESTIGACIÓN DE DELITO INFORMATICO Y CONEXOS (DIVISIÓN CENTRAL DE INVESTIGACIONES DE LA POLICIA NACIONAL CIVIL) | | | |
|---|---|---|---|
| **CATEGORÍA DE PREGUNTA** | **DOCTRINA** | **RESPUESTA DE INFORMATE** | **OPINIÓN DE GRUPO** |
| 1-) Riesgos existentes dentro del internet que pueden afectar a los niños, niñas y adolescentes. | El internet al ser concebida como aquella red inalámbrica mundial para el intercambio de datos; presupone un riego para aquellos usuarios con cierto grado de inmadurez emocional, en donde se encuentran enmarcados los niños, niñas y adolescentes, pues la lista de riesgos a los que se enfrentan al navegar por internet se pueden resaltar los siguientes: Contenido Inapropiado (como pornografía, violencia explícita, inducción a la drogadicción, entre otros); Ciberacoso; y Revelación de Información privada (Personal, familiar y económica). | El informante expresó lo siguiente: *"En la actualidad existe una sobrexposición a los videojuegos por parte de los niños, niñas y adolescentes, y en mayor medida a aquellos Juegos Online, que necesariamente deben estar conectados al internet, es a partir de acá que surgen una variedad de riesgos, puesto que los menores de edad pueden ser persuadidos, por personas sin escrúpulos, para obtener de ellos información delicada (privada o financiera), fotos y videos explícitos (grooming, información financiera, sexting y sextorsión) lo cual puede conllevar un daño a la psiquis de las víctimas".* | Efectivamente, las generaciones actuales tienen una sobrexposición a los dispositivos electrónicos que tienen acceso a internet, en especial a aquellos relacionados a los videojuegos, en los cuales muchas veces vienen integrados sistemas de interacción con otros usuarios, facilitando chats o incluso comunicaciones en tiempo real por medio de audio e incluso por video. Razón por la cual, los menores de edad tienen cierta facilidad de toparse con desconocidos en tan abismales centros de interrelaciones; naturalmente, debido a la concurrencia de personas en esos sitios, con frecuencia los menores de edad se enfrentan a individuos con malas intenciones, que pueden derivar en grooming, sexting, sextorsión o divulgación de información económica delicada. |
| 2-) Mecanismos de Control de contenido multimedia | El uso de Internet como tal es incontrolable. Su estructura en | El informante explica: *"Dentro de las* | Debido a la magnitud del alcance universal de la "red de redes", es |

| | | | |
|---|---|---|---|
| contenido en el internet ejercidos por el Estado salvadoreño. | red facilita que lo que se censure en un sitio reaparezca en otro. Pero su funcionamiento requiere de unos protocolos y convenios globales que posibiliten la circulación de información, los cuales incluyen procedimientos de asignación de números IP y nombres de dominio (como http://www.pce.es o http://alteritat.net) a cada sitio de Internet y la correspondencia entre ellos. A ello es a lo que se refiere el "control de Internet" a debate en la Cumbre Mundial de la Sociedad de la Información en Túnez. Y siendo el caso de El Salvador, no existe un método regulado legalmente para controlar los contenidos vertidos dentro del internet del cual hace uso la población salvadoreña. | *investigaciones dirigidas en contra de los delitos informáticos, solo existen directrices, por parte de la Fiscalía General de la República, para el cómo realizar dichas investigaciones, no obstante, el control de los contenidos dentro del internet, en mayor medida, corresponden a los proveedores de Internet. En conclusión la División Central de Investigación de la PNC, se encarga únicamente de la investigación científica de los delitos informáticos".* | fácil visualizar cuan complicado es ejercer un control formal y extenso sobre el Internet. Por lo cual, en nuestro país no es la excepción, no existe un control formal de los contenidos vertidos en el ciberespacio; por lo que en los casos de los delitos informáticos, la División Central de Investigación de la PNC, únicamente se encarga de la investigación científica de los referidos delitos, siempre y cuando sigan las directrices planteadas por la Fiscalía General de la República. |
| 3-) Contenido multimedia ilícito incautado en las investigaciones dirigidas al combate del ciberdelito que afecte a menores de edad. | En su mayoría de investigaciones, el contenido con posible carga probatoria en un juicio penal en el cual se ventila la comisión de un ciberdelito en el cual resulto afectado un menor de edad, suele ser aquel en cual se aprecia abuso sexual infantil realizado por parte del incoado o por un tercero. | El Informante Manifiesta: *"Es el material relacionado al abuso sexual infantil, imágenes y videos".* | En la actualidad, en la sociedad salvadoreña, ocurren ciertos hechos que atentan contra la sexualidad de los niños, niñas y adolescentes, y en el ámbito de los cibercrímenes no es la excepción, pues uno de los acontecimientos mas condenables es la proliferación de depredares sexuales que se ocultan a través del anonimato, para poder ejercer su influencia negativa en los menores |

| | | | |
|---|---|---|---|
| | | | de edad. |
| 4-) Criterio para determinar la utilidad del material recabado en la investigación como posible prueba de la comisión de un posible delito informático. | Cada elemento recabado dentro de una investigación judicial tendrá valor probatorio siempre y cuando cumpla con el Principio de Licitud (que el elemento probatorio se haya recolectado sin haber afectado a algún derecho fundamental consagrado en la Constitución), y con el Principio de Fiabilidad (que la prueba no haya sido manipulada, y que exista plena vinculación con el hecho presuntamente delictivo). | El Informante expresó: *"Se ocupa la Evidencia Digital la cual debe estar vinculada al hecho presuntamente delictivo, y aquella que no sea constitutiva de delito no puede ser tomada en cuenta".* | De acuerdo con Código Procesal Penal vigente, en su artículo 175, se consagra el principio de la legalidad de la prueba en el cual manda al Juzgador dejar fuera cualquier elemento probatorio obtenido de maneras ilícitas, derivados de violaciones de derechos constitucionales; asimismo en el artículo 177, plantea la utilidad y pertinencia de la prueba, y que hacen referencia a que el elemento probatorio debe ser útil para desentrañar la verdad histórica de la comisión de un delito, y asimismo, el elemento de convicción debe estar relacionado directa o indirectamente con el hecho punible, con la identidad del autor, con la penalidad de los cómplices y participes o a la credibilidad de los peritos. |
| 5-) Limite legales que tienen las investigaciones dirigidas al combate del cibercrimen para poder intervenir las comunicaciones o la información privada de los incoados. | La investigación de los ciberdelitos puede afectar a varios derechos fundamentales dependiendo de la diligencia de la investigación judicial a realizar. Así, por ejemplo, la intimidad personal, el secreto de las comunicaciones y la protección de datos personales, puede resultar afectada al | El Informante dijo: *"Que los criterios bajo los cuales se guían, son aquellos que se estipulan en el Código Procesal Penal vigente, en lo respectivo a la Prueba dentro de los procedimientos judiciales".* | Ciertamente, es el Código Procesal vigente, el cual estipula las reglas para obtención de los elementos probatorios, asimismo estipula las excepciones para la obtención de ciertos elementos de convicción relacionados a algunos delitos de realización compleja. |

| | | | |
|---|---|---|---|
| | acceder a dispositivos electrónicos; inclusive puede ser vulnerada la inviolabilidad del domicilio, dado el caso de que las autoridades se vean obligadas a incautar algún dispositivo electrónico que se encuentre en el domicilio de un posible victimario. | | |
| 6-) Protocolos de protección para los niños, niñas y adolescentes, frente a la depredación sexual infantil dentro del ciberespacio | Según el Estado Mundial de la Infancia de la UNICEF (2017) Las empresas de tecnología e internet deberían tomar medidas para evitar que sus redes y servicios sean utilizados por delincuentes para recopilar y distribuir imágenes de abuso sexual infantil o cometer otras violaciones contra los niños. Dado que en el caso de El Salvador no existe un monopolio estatal del control del Internet. | El Informante manifestó: *"Actualmente solo están ligados al ordenamiento jurídico actual, no obstante, cualquier política debe venir de la voluntad Estatal, y debe haber un principal enfoque a aquellas políticas educacionales para la prevención de posibles delitos informáticos".* | Se deja entre ver que es necesaria la voluntad estatal de nuestro país para poder emitir políticas dirigidas a la protección de los menores de edad, puesto que actualmente solo contamos con las normativas dictaminadas por todos los tratados a los cuales esta suscrito El Salvador, dirigido a la protección de la niñez y adolescencia. Asimismo, es necesaria la cooperación de terceros, tales como los proveedores de internets, para realizar planes de prevención y contingencia a la hora que los menores de edad se encuentren propensos a sufrir algún ataque de un posible depredador sexual. |
| 7-) Procedimiento sancionatorio aplicado a la negativa de una empresa operadora de telecomunicación de colaborar en la investigación | El incumplimiento de la obligación de adecuación o complementación de los sistemas por los operadores y del deber de éstos de garantizar la conectividad con el Centro serán | El informante expresó: "La *División Central de Investigación de la PNC no tienen esta información , se espera que la Fiscalía General de la República* | Claro esta el hecho de que la PNC, no esta ligada a las empresas de telecomunicación, por lo que la Fiscalía General de la República debe proceder de acuerdo a lo estipulado a la Ley de Intervención |

| | | | |
|---|---|---|---|
| del ciberdelito. | consideradas faltas muy graves de conformidad con la Ley de Telecomunicaciones | *genere acuerdo con dichas empresas*", | de la Telecomunicaciones, y que, en caso de incumplir con el deber de cooperación, deben ser sancionadas de acuerdo a la Ley de Telecomunicaciones y en especifico las contempladas en su artículo 34. |
| 8-) Derechos constitucionales relacionados a la intimidad e inviolabilidad de las telecomunicaciones personales de las comunicaciones. | Los principales vulnerados son la intimidad personal, el secreto de las comunicaciones y la protección de datos personales, y en algunos casos la inviolabilidad del domicilio | El Informante asegura: *" Siempre y cuando los procedimientos para la intervención de las comunicaciones se realicen mediante la debida autorización judicial dada por la autoridad competente, no puede existir una vulneración a los derechos fundamentales de los individuos".* | La Constitución en sus Artículos 2, 20 y 24, consagran los derechos de la intimidad personal, el secreto de las comunicaciones y la inviolabilidad de la morada, respectivamente, que tiene todo ser humano dentro del territorio salvadoreño, no obstante, por razones de investigación de la comisión de ciertos ilícitos, se concibe legitima la vulneración de los derechos mencionados anteriormente, siempre y cuando se realicen mediante la respectiva autorización judicial emitida por autoridad competente y debidamente fundamentada. |

# CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

## 1. CONCLUSIONES

Luego de finalizar la investigación titulada como "LA NECESIDAD DEL ESTADO SALVADOREÑO DE REGULAR ESPACIOS CIBERNÉTICOS FRENTE AL USO DE LAS REDES SOCIALES POR PARTE DE LOS NIÑOS, NIÑAS Y ADOLESCENTES PARA EVITAR LA DEPREDACIÓN SEXUAL" es procedente enunciar las siguientes conclusiones:

**a)** El ciberespacio comprendido como aquel espacio generado a partir de los aparatos cibernéticos; genera una especie de mutación en el concepto tradicional de la soberanía de los Estados, en el sentido de que genera un nuevo ámbito en donde los Estados deberían ejercer su jurisdicción, es decir, el concepto de soberanía se ve obligado a adaptarse para no extinguirse, en un nuevo universo metafísico creado a partir de las nuevas tecnologías. Y en esta reformulación conceptual nos vemos obligados a pensar en un lugar despojado de toda idea física de "lugar"; De esta forma vemos una soberanía a-territorial. A su vez, las nuevas relaciones que nazcan de la interrelación de los ciudadanos que se congregan en la red de redes, nos plantea el perfil de un individuo anónimo, incluso despojado de toda conciencia cívica.

**b)** Que el anonimato proveído por el uso del internet a los cibernautas puede provocar en ellos el realizar conductas condenables por el Derecho Penal; y al tratarse de un metaverso gigantesco que está al alcance de cualquier persona sin importar la edad, es natural que exista un sector de usuarios de la internet que no tienen una madurez psíquica para afrontar los sitios web con información cuestionable vertidos en el ciberespacio; razón por lo cual los hace presa fácil de depredadores cibernéticos.

**c)** En el caso de El Salvador, únicamente existe una normativa relacionada íntimamente con los hechos punibles realizados a través de medios cibernéticos, la cual es la "Ley Especial Contra Delitos Informáticos y Conexos", y cuando estuviesen involucradas victimas que fueren menores de edad, será vinculante toda la normativa relacionada a proteger la niñez y la adolescencia; razón por la cual resulta alarmante la precariedad del ordenamiento jurídico para regular los medios cibernéticos, aunado a la falta de preocupación para legislar a favor de prevenir y combatir los delitos informáticos, lo cual ha desencadenado una escasez de personal capacitado en el actuar jurídico de

instituciones tales como Juzgados, Procuraduría General de la República y Fiscalía General de la República.

**d)** Actualmente se cuenta con una red de inteligencia dedicada a la investigación científica de los delitos informáticos, pero enfrentan carencias presupuestarias a consecuencia de la poca voluntad política para invertir en la prevención y combate de los ciberdelitos, razón por lo cual únicamente cuentan con una unidad central, resultando difícil la persecución efectiva del cibercrimen a nivel nacional.

**e)** La censura estatal de contenidos dentro del ciberespacio, es una tarea titánica para el actual sistema de Gobierno, ya sea por razones de falta de actualización de aparataje cibernético o por falta de voluntad política, lo anterior trae como consecuencia que son los proveedores de internet los que tienen que mantener un estándar de control de contenidos multimedia dentro del ciberespacio, y por otra parte recae en la familia salvadoreña la protección de los menores a la hora que estos navegan en la red de redes.

**f)** Actualmente el sistema judicial, no posee una herramienta que obligue al agresor a reparar los daños ocasionados a las víctimas de ciberdelitos de índole sexual, puesto que, aun ajusticiando a los autores del cibercrimen, el daño que estos ocasionan al divulgar información sensible de la víctima en una red tan amplia como el internet, se vuelve irreparable, debido a la facilidad de viralizar y multiplicar datos entre los cibernautas.

**g)** Lo determinante para evitar la depredación sexual dentro del ciberespacio en perjuicio de la niñez y la adolescencia, no es cuan rígidas son o serán las penas previstas en el ordenamiento jurídico para los ciberdelitos; para poder evitar estas cuestiones, el Estado debe invertir en políticas educacionales dirigidas a las escuelas y principalmente a los padres de los menores de edad, puesto que la línea de defensa más eficaz para evitar la proliferación de estas conductas y sus consecuentes víctimas, es la protección que deben brindar los padres de los menores de edad dentro sus hogares, ya que aun en los Estados más desarrollados es complicado el control total del ciberespacio, y en el caso de El Salvador, debe primar la conciencia social sobre los peligros existentes en el ciberespacio y comprender la responsabilidad que tiene la sociedad para cuidar a sus futuras generaciones.

**h)** Se concluye que en un Estado de Derecho y Democrático como lo es el Estado Salvadoreño no es viable la censura previa del contenido multimedia compartido de los ciber usuarios, debido a que la misma representaría una violación flagrante derechos fundamentales del elemento humano que consagra la Constitución de la república más específicamente en las libertades individuales de cada uno de los ciudadanos, Derechos tales como la libertad de expresión, libertad de pensamiento y la libertad de acceso a la información entre otros, no obstante se concluye que es muy positivo que nuestro país forme parte de los Estados que penalicen los Delitos Informáticos que perjudiquen a los Niños, Niñas y Adolescentes.

## 2. RECOMENDACIONES

A partir de lo anterior, el grupo de trabajo toma a bien a enlistar las siguientes recomendaciones:

a) ***A la Asamblea Legislativa*:** para la eficaz lucha y prevención en contra del cibercrimen, es de vital importancia que El Salvador suscriba el Tratado de Budapest en Contra de los Ciberdelitos, para que surjan consecuencias positivas tales como la cooperación internacional entre los países parte, con el fin de compartir ideas, mecanismos, herramientas y personal, para actuar ante la inminente revolución informática, a la globalización y los consecuentes peligros que surjan en un mundo cada vez más interconectado.

b) Es necesaria la creación de un mecanismo jurídico para la regulación de espacios de interconexión cibernética, denominados coloquialmente como "*ciber café*", para la eficaz investigación científica de los delitos informáticos, para permitir una eficiente individualización de posibles cibercriminales.

c) ***Al Gobierno de El Salvador*:** Se debe solicitar el apoyo del Gobierno en turno para facilitar políticas de prevención del cibercrimen a través del Ministerio de Educación, fomentando en las instituciones educativas la promoción de escuelas de capacitación para padres y para alumnos, con el fin de concientizar a la población de las virtudes y peligros que tiene ahora la sociedad en un mundo interconectado.

d) Es necesario que las instituciones encargadas de la investigación científica de delitos informáticos, obtengan un mayor presupuesto económico para promoción de

investigaciones eficaces, y asimismo puedan desconcentrar que tiene la unidad central de investigación de delitos informáticos de la Policía Nacional Civil, y así colocar, al menos algunas, delegaciones bajo este mismo enfoque en las zonas geográficas del país (Occidental, Central, Paracentral y Oriental).

e) ***Se recomienda a las plataformas de redes sociales:*** que provean de la manera más transparente y comprensible las cláusulas, términos de condiciones y de servicio, debido a que los ciber usuarios en muchas ocasiones no las comprenden, o en determinado caso no se detienen a leerlas, no obstante, recomendamos que las mismas no deben de perder la connotación jurídica que tienen hasta el momento.

***f) Se recomienda a la Policía Nacional Civil y a la Fiscalía General de la República:*** Gestionar la capacitación de Personal más cualificado para la Investigación de los Delitos Informáticos, con ese capital humano la PNC debería fundar laboratorios científicos y tecnológicos, dividirlos en Regionales Occidental y Oriental para un análisis pericial eficiente, eficaz y oportuno; asimismo la Fiscalía General de la República se recomienda establecer Unidades de Delitos Informáticos ya que durante el desarrollo de la investigación pudimos constatar que en estas importantísimas Unidades solamente existen las capacitaciones a su personal, sin crear una dependencia o unidad especializada.

***g) Se recomienda al CONNA Y AL ISNA:*** Establecer protocolos de atención psicológica especial a los Niñas, Niñas y Adolescentes que hayan sido víctimas de Delitos Informáticos, a darle seguimiento a éstos casos e involucrar a los padres a la concientización y responsabilidades cuando se navega por el ciberespacio.

***h) Se recomienda al Ministerio de Educación:*** Establecer la didáctica óptima, necesaria y oportuna de acuerdo al grado académico y edad del educando para llevar a cabo campañas de información, prevención y consecuencias de los Delitos Informáticos, esto con la finalidad de concientizar a los Niños, Niñas y Adolescentes acerca de los riesgos que corren al navegar por el ciberespacio, al tipo de contenido o materia multimedia al que pueden acceder y a difundir cuáles son sus Derechos desde la primera infancia hasta la mayoría de edad.

## REFERENCIAS BIBLIOGRAFICAS

## LIBROS


a) Kleinsteuber, H. El surgimiento del ciberespacio: la palabra y la realidad en Vidal, J. (2002). La ventana global. Madrid: Taurus.
b) Marc Porat, Global Implications of the Information, (1978). Global Implications of Information Society. Journal of Communication, 28(1): 70-80.
c) Palan, R. (2006). The offshore world: sovereign markets, virtual places, and nomad millionaires. Estados Unidos de América: Cornell University Press.
d) Jiménez, W. G. & Meneses, O. (2017). Derecho e Internet: introducción a un campo emergente para la investigación y práctica jurídicas. Revista Prolegómenos Derechos y Valores.
e) Téllez, J. Derecho Informático. 4ta. Edición. México: McGraw-Hill. 2009.
f) PÉREZ LUÑO, Antonio Enrique. "Manual de informática y derecho", Editorial Ariel S.A., Barcelona, 1996.
g) Ríos Estavillo, Juan José, Derecho e informática en México: informática jurídica y derecho de la informática / México: Universidad Nacional Autónoma de México, 1997; pag. 70.
h) PERRITT, Henry H., "Internet: ¿Una amenaza para la soberanía?", Indiana Journal of Global Legal Studies, 1998, vol. 5, p. 423.
i) CABANELLAS DE LAS CUEVAS, Guillermo - MONTES DE OCA, Ángel, Derecho de Internet, cit.
j) AOKI, Keith, "Soberanías múltiples y superpuestas. Liberalismo, doctrina libertaria, soberanía nacional, propiedad intelectual 'global' e Internet", Indiana Journal of Global Legal Studies, 1998, vol. 5, p. 443.
k) PELLET LASTRA, Arturo, Teoría del Estado, LexisNexis, Buenos Aires, 2003.
l) Ziewitz, M. and Brown, I. 2013. A prehistory of Internet governance. En: Brown, I.Research Handbook on Governance of the Internet. Cheltenham: Edward Elgar.
m) TÉLLEZ AGUILERA, A. Nuevas Tecnologías. Intimidad y protección de datos, Edisofern, 2001, pp. 21 y ss.
n) SIEBER, U. Computerkriminalität und Strafrecht, München, 1977, p. 23.

o) Diccionario de la lengua española (de la Real Academia Española), vigésima segunda edición enmendada.

**LEYES**

a) Constitución de la República de El Salvador.
b) Código Penal de El Salvador.
c) Ley Especial Contra los Delitos Informáticos y Conexos.
d) Ley de Telecomunicaciones.
e) Ley de Protección Integral de la Niñez y la Adolescencia.
f) DECRETO N° 133, D. O. N° 196 Tomo N° 409 Fecha: 26 de octubre de 2015, Ley de Firma electrónica.
g) El Convenio sobre Ciberdelincuencia del Consejo de Europa.
h) La Convención para combatir Delitos con Tecnología de la Información de la Liga de los Estados Árabes.
i) El Acuerdo de Cooperación para combatir Delitos.
j) Decreto nº 534, de 2 de diciembre de 2010. Ley de Acceso a la Información Pública. (Diario Oficial número 70, tomo nº 371, de 8 de abril de 2011).
k) Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía Asamblea General - Resolución A/RES/54/263 del 25 de mayo de 2000; artículo 2 literal c).
l) Tratado de la Organización Mundial de la Propiedad Intelectual -OMPI-, sobre el derecho de autor -wct- 1,996

# ANEXOS

**SIGET** SUPERINTENDENCIA GENERAL DE ELECTRICIDAD Y TELECOMUNICACIONES

**Superintendencia General de Electricidad y Telecomunicaciones**
**Unidad de Acceso a la Información y Transparencia**

OIR Oficina de Información y Respuesta

# Solicitud de Información

Número

Información del Solicitante

| | | | |
|---|---|---|---|
| Nombres | Mynor Leonel | Apellidos | Martínez Pineda |
| Tipo de documento | DUI | Número de doc. | 05561635 - 1 |
| Edad | 22 | Sexo | X masculino ☐ femenino |
| Teléfono de contacto | 7450 - 4648 | Nivel Educativo | Universitario |
| Departamento | Santa Ana | Nacionalidad | Salvadoreña |
| Municipio | San Sebastián Salitrillo | | |

Datos para que se le notifique

Forma de Notificación: X Correo Electrónico; ☐ Correo Certificado; ☐ Fax; ☐ Presencial; ☐ Cartelera

Detalle para notificación: Correo Electrónico: mynorpnd@gmail.com

Persona comisionada para notificaciones:_____
(Deberá identificarse en el acto)

Información Solicitada (Descripción clara y precisa)

1- ¿Cuáles son los mecanismos de control del internet de los cuales dispone el Estado salvadoreño para el control del contenido multimedia que está disponible en el ciberespacio?; 2- ¿Cuál es el rol que desempeña la Superintendencia General de Electricidad y Telecomunicaciones en cuanto a la colaboración en el procedimiento de la investigación de los delitos informáticos?; 3- ¿Cuáles son los mecanismos de protección de los niños, niñas y adolescentes en El Salvador con los que cuenta la SIGET, para controlar el contenido multimedia que circula en el ciberespacio?; 4- Como especialista en el área de telecomunicaciones ¿Tiene planes de actualización en cuanto a los protocolos de entendimiento interinstitucional con la FGR y la PNC de protección de los niños, niñas y adolescentes para el combate de la depredación sexual?; 5- En el proceso de investigación ¿Cómo delimita el acceso a la intervención de las comunicaciones de los usuarios sin afectar el Derecho a la intimidad, Derecho a libertad de expresión, Inviolabilidad de la comunicaciones y hábeas Data a partir de la autorización judicial?; 6- ¿Cuáles son los límites que tiene un profesional de su área para intervenir las comunicaciones o el acceso a la información de contenido susceptible de los incoados?; 7- Teniendo en cuenta el Marco Jurídico actual ¿Considera que los límites legales establecidos violentan Derechos Constitucionales como el Derecho a la Intimidad y el Derecho a la Inviolabilidad de las Telecomunicaciones?; 8- ¿Considera necesaria la aplicación de leyes especiales o el funcionamiento de un ente que determine la factibilidad o idoneidad de material multimedia o de contenido personal que circule en el ciberespacio para combatir los delitos que están en detrimento de la integridad física o psicológica de los niños, niñas y adolescentes en El Salvador? Si No, fundamente su respuesta; 9- ¿Cuál es el procedimiento sancionatorio que sigue la Superintendencia General de Electricidad y Telecomunicaciones en el caso que una empresa operadora de telecomunicaciones se niegue a colaborar en la investigación dentro de un proceso penal?; 10- ¿Cuáles son los protocolos de entendimiento que tiene la Superintendencia General de Electricidad y Telecomunicaciones con las empresas distribuidoras de telecomunicaciones en cuanto a la colaboración de investigación de delitos informáticos?; 11- ¿Cuáles son los delitos informáticos más comunes en los cuales ha colaborado la Superintendencia General de Electricidad y Telecomunicaciones en conjunto con la Fiscalía General de la República?; 12- ¿Actualmente la Superintendencia General de Electricidad y Telecomunicaciones realiza campañas de concientización dirigida a los niños, niñas y adolescentes con la finalidad de combatir la depredación sexual?; 13- ¿Garantiza la Superintendencia General de Electricidad y Telecomunicaciones el acceso fiable y seguro a las Tecnologías de Información y Comunicación a los niños, niñas y adolescentes?

Forma de entrega de la Información

| | | | | | |
|---|---|---|---|---|---|
| ☐ CD | ☐ Fotocopia | X Correo Electrónico | ☐ OIR - San Salvador | | |
| ☐ DVD | ☐ Fotocopia Certificada | ☐ Correo Certificado | ☐ Centro de Atención al Usuario- Santa Ana: 7ª. Calle Oriente, entre Av. Independencia Sur y 1ª. Av. Sur, #3, Barrio Santa Cruz. Teléfono: 2447-8415 | | |
| ☐ USB | ☐ Fax | ☐ Consulta Directa | ☐ Centro de Atención al Usuario-San Miguel: Centro de Gobierno de San Miguel, 8ª. Av. Sur y 15ª. Calle Oriente, San Miguel. Teléfono: 2661-4056 | | |

**Notas:**
- La información es **GRATUITA**
- Si requiere información en dispositivos: CD, DVD, USB, estos serán proporcionados por el solicitante o interesado
- Los costos asumidos por el solicitante son: a) de reproducción (determinados de acuerdo a los precios establecidos en la tabla autorizada por la Institución), b) envío por correo certificado, mensajería; c) las tasas respectivas en caso se requiera copias certificadas. La entrega estará sujeta al comprobante de pago, en caso se requiera, y a los plazos de entrega de la empresa de correos.
- La solicitud se tendrá por admitida al cumplir con los datos requeridos en el presente formulario, caso contrario se le hará la prevención respectiva..

Firma/ impresión dactilar (Huella) | Fecha y hora de presentación | Sello

SIGET
SUPERINTENDENCIA GENERAL DE ELECTRICIDAD Y TELECOMUNICACIONES

GOBIERNO DE EL SALVADOR

**SIPV N.° 028-2020**

**SUPERINTENDENCIA GENERAL DE ELECTRICIDAD Y TELECOMUNICACIONES (SIGET), UNIDAD DE ACCESO A LA INFORMACIÓN Y TRANSPARENCIA (UAIT),** a las dieciséis horas del día diez de febrero del año dos mil veinte.

A sus antecedentes la solicitud de información, remitida al correo electrónico institucional oir@siget.gob.sv interpuesta a las diecisiete horas con cincuenta y dos minutos del día veintiocho de enero del año dos mil veinte, no siendo hora hábil según el Art. 81 de la Ley de Procedimientos Administrativos (LAP); tomándose como fecha y hora hábil de ingreso el día veintinueve de enero del año dos mil diecinueve; por el ciudadano **MYNOR LEONEL MARTÍNEZ PINEDA**. Que en la petición solicitó:

*1- ¿Cuáles son los mecanismos de control del internet de los cuales dispone el Estado salvadoreño para el control del contenido multimedia que está disponible en el ciberespacio?; 2- ¿Cuál es el rol que desempeña la Superintendencia General de Electricidad y Telecomunicaciones en cuanto a la colaboración en el procedimiento de la investigación de los delitos informáticos?; 3- ¿Cuáles son los mecanismos de protección de los niños, niñas y adolescentes en El Salvador con los que cuenta la SIGET, para controlar el contenido multimedia que circula en el ciberespacio?; 4- Como especialista en el área de telecomunicaciones ¿Tiene planes de actualización en cuanto a los protocolos de entendimiento interinstitucional con la FGR y la PNC de protección de los niños, niñas y adolescentes para el combate de la depredación sexual?; 5- En el proceso de investigación ¿Cómo delimita el acceso a la intervención de las comunicaciones de los usuarios sin afectar el Derecho a la intimidad, Derecho a libertad de expresión, Inviolabilidad de la comunicaciones y hábeas Data a partir de la autorización judicial?; 6- ¿Cuáles son los límites que tiene un profesional de su área para intervenir las comunicaciones o el acceso a la información de contenido susceptible de los incoados?; 7- Teniendo en cuenta el Marco Jurídico actual ¿Considera que los límites legales establecidos violentan Derechos Constitucionales como el Derecho a la Intimidad y el Derecho a la Inviolabilidad de las Telecomunicaciones?; 8- ¿Considera necesaria la aplicación de leyes especiales o el funcionamiento de un ente que determine la factibilidad o idoneidad de material multimedia o de contenido personal que circule en el ciberespacio para combatir los delitos que*

*están en detrimento de la integridad física o psicológica de los niños, niñas y adolescentes en El Salvador? Si No, fundamente su respuesta; 9- ¿Cuál es el procedimiento sancionatorio que sigue la Superintendencia General de Electricidad y Telecomunicaciones en el caso que una empresa operadora de telecomunicaciones se niegue a colaborar en la investigación dentro de un proceso penal?; 10- ¿Cuáles son los protocolos de entendimiento que tiene la Superintendencia General de Electricidad y Telecomunicaciones con las empresas distribuidoras de telecomunicaciones en cuanto a la colaboración de investigación de delitos informáticos?; 11- ¿Cuáles son los delitos informáticos más comunes en los cuales ha colaborado la Superintendencia General de Electricidad y Telecomunicaciones en conjunto con la Fiscalía General de la República?; 12- ¿Actualmente la Superintendencia General de Electricidad y Telecomunicaciones realiza campañas de concientización dirigida a los niños, niñas y adolescentes con la finalidad de combatir la depredación sexual?; 13- ¿Garantiza la Superintendencia General de Electricidad y Telecomunicaciones el acceso fiable y seguro a las Tecnologías de Información y Comunicación a los niños, niñas y adolescentes?..* (SIC)

**ÉSTA UNIDAD PARA DAR RESPUESTA A DICHA SOLICITUD HACE LAS CONSIDERACIONES SIGUIENTES:**

I. Que la solicitud fue presentada en la fecha citada y previo a su admisión formal del requerimiento se verifico cumpliese con lo que disponen los Arts. 66 inciso quinto de la Ley de Acceso a la Información Pública en lo sucesivo LAIP o Ley, relacionado con los Arts. 52, 54 del Reglamento de la Ley de Acceso a la Información Pública (RLAIP), en consonancia a lo establecido en al 72 de la Ley de Procedimientos Administrativos (LPA); constatado lo anterior, se continuo el trámite de Ley correspondiente.

II. La suscrita precisa que tal como señala el Art. 4 de la Ley de Creación de la Superintendencia General de Electricidad y Telecomunicaciones (LCSIGET), ésta entidad entre sus facultades tiene: *Competencia Art. 4.- La SIGET es la entidad competente para aplicar las normas*

*contenidas en tratados internacionales sobre electricidad y telecomunicaciones vigentes en El Salvador; en las leyes que rigen los sectores de Electricidad y de Telecomunicaciones; y sus reglamentos; así como para conocer del incumplimiento de las mismas.*

III. La LAIP atribuye al Oficial de Información, en el artículo 50 letras b. y d. funciones como: Recibir y diligenciar las solicitudes, gestionar y entregar la información requerida, garantizando el derecho de acceso que asiste a toda persona reconocido en el Art. 1 LAIP; asimismo, el artículo 70 de la Ley establece que: *El Oficial de información transmitirá la solicitud a la unidad administrativa que tenga o pueda poseer la información, con el objeto de que ésta la localice, verifique su clasificación y, en su caso, le comunique la manera en que se encuentra disponible.* En cumplimiento de tales funciones se envió la petición a la Gerencia de Telecomunicaciones (GT).

**RAZONAMIENTO DE RESPUESTA A LA PETICIÓN:**

IV. La Gerencia de Telecomunicaciones de la SIGET, con base a la información que resguarda y genera, según las facultades establecidas en la Ley de Creación de la SIGET (Art. 5), el Reglamento de la Ley de Creación de la SIGET y la normativa vigente del sector de las telecomunicaciones, en respuesta manifestó:

Que a la fecha de recepción de esta solicitud, no se cuenta con esta información, ya que la SIGET no es la institución competente para regular sobre el tema de espacios cibernéticos frente al usos de las redes sociales por parte de los niños, niñas y adolescentes para evitar la depredación sexual; debido a que las atribuciones legales conferidas a través de la Ley de Creación de la SIGET, Reglamento de la Ley de Creación de la SIGET, Ley de Telecomunicaciones y el Reglamento de la Ley de Telecomunicaciones; además de la normativa vigente referente al rubro telecomunicaciones; establecen únicamente que la Superintendencia es la entidad encargada de administrar, gestionar y monitorear el espectro radioeléctrico; siendo este el conjunto de ondas radioeléctricas que se propagan sin guía

artificial por debajo de los 3,000 GHZ y se divide en bandas de frecuencias, las cuales pueden atribuirse a diferentes servicios radioeléctricos para utilizarse en diferentes áreas geográficas y períodos; además la SIGET es la autoridad competente para verificar la regularidad de las condiciones de los títulos habilitantes; entendiéndose como títulos habilitantes como el acto administrativo que otorga esta institución para la concesión, autorización o licencia para la utilización y explotación del espectro radioeléctrico; así como para la prestación de servicios públicos de telecomunicaciones.

Las atribuciones legales de esta entidad, están definidas en el artículo 5 de la Ley de Creación de esta Superintendencia, en relación a lo establecido en Ley de Telecomunicaciones, artículos 1 y 2, entre otros, los cuales se transcriben:

*Objeto*

*Art. 1. ...Asimismo, se establece que la Superintendencia General de Electricidad y Telecomunicaciones, será la entidad responsable de aplicar y velar por el cumplimiento de las normas y regulaciones establecidas en esta Ley y su reglamento.*

*Las actividades de telecomunicaciones realizadas por los operadores de servicios de: a) radiodifusión sonora de libre recepción; b) televisión de libre recepción; c) distribución sonora por suscripción, a través de cable o medios radioeléctricos; y, d) distribución de televisión por suscripción a través de cable o medios radioeléctricos; estarán sujetas al régimen especial que establece el Título VIII de esta Ley.*

*La SIGET en el ejercicio de sus funciones deberá recabar de los operadores de redes Comerciales de telecomunicaciones, la información técnica que resulte necesaria para verificar el cumplimiento de la ley, sus reglamentos y de las normas que resulten aplicables. (19)*

*La SIGET deberá realizar por sí, o por medio de los peritos o auditores autorizados y designados para ello, y supervisados por personal de la SIGET, las inspecciones que considere necesarias con el fin de comprobar la veracidad de la información aportada, en la medida que resulte necesario para el ejercicio de sus funciones. (19)*

*La SIGET es la entidad encargada de administrar, gestionar y monitorear el espectro radioeléctrico; y es la autoridad competente para verificar la regularidad de las condiciones de los títulos habilitantes, así como para aplicar las sanciones o medidas correctivas que correspondan.*

*Fines*

*Art. 2. Las normas de la presente Ley se aplicarán atendiendo a los siguientes fines:*

*a. Fomentar el acceso universal, la asequibilidad y la aprehensión de las Tecnologías de la Información y la Comunicación que permitan el ejercicio pleno de los derechos a la libertad de expresión, de información, y difusión del pensamiento, para reducir la brecha digital y contribuir a la inclusión social;(20)*

*b. Protección de los derechos de los usuarios, de los operadores, proveedores de servicios de telecomunicaciones; así como de las personas en general.(6)(8)*

*c. Desarrollo de un mercado de telecomunicaciones competitivo en todos sus niveles; y,*

*d. Garantizar el uso racional, eficiente y equitativo del espectro radioeléctrico, así como su actualización, reordenamiento o reorganización para su optimización, que permita la introducción de nuevos servicios, mejorar los existentes, y la armonización con otros países, acorde a la Constitución de la República y los Tratados Internacionales suscritos, adheridos y ratificados por la República de El Salvador, que regulen las actividades del sector de telecomunicaciones.*

V. En referencia a lo solicitado, con base al derecho de asistencia para el acceso a la información y al auxilio en la elaboración de las solicitudes, establecido en el artículo 68 de la LAIP; esta Unidad, hace referencia a lo previsto en la Ley de Protección Integral de la Niñez y Adolescencia (LEPINA) que tiene por finalidad garantizar el ejercicio y disfrute pleno de los derechos y facilitar el cumplimiento de los deberes de toda niña, niño y adolescente en El Salvador, para cuyo efecto crea el Sistema Nacional de Protección Integral de la Niñez y Adolescencia, cual tiene como obligaciones, lo dictado en los Arts. 25, 29, 30, 103, entre otros de la Ley de Protección Integral de la Niñez y Adolescencia, siendo el Sistema Nacional de

Protección Integral de la Niñez y Adolescencia el conjunto coordinado de órganos, entidades o instituciones, públicas y privadas, cuyas políticas, planes y programas tienen como objetivo primordial garantizar el pleno goce de los derechos de las niñas, niños y adolescentes en El Salvador, el Sistema se encuentra conformado según establece el artículo 105 de la LEPINA, el cual dice:

*Artículo 105.- Composición del Sistema de Protección Integral El Sistema de Protección estará integrado por:*

*a) El Consejo Nacional de la Niñez y de la Adolescencia;*

*b) Los Comités Locales de Derechos de la Niñez y de la Adolescencia;*

*c) Las Juntas de Protección de la Niñez y de la Adolescencia;*

*d) Las Asociaciones de Promoción y Asistencia;*

*e) El Instituto Salvadoreño para el Desarrollo Integral de la Niñez y la Adolescencia;*

*f) El Órgano Judicial;*

*g) La Procuraduría General de la República;*

*h) La Procuraduría para la Defensa de los Derechos Humanos; e,*

*i) Los miembros de la Red de Atención Compartida.*

Por lo anterior, el solicitante, si así lo estima conveniente, puede acudir ante dichas entidades públicas, por medio de sus respectivas Unidades de Acceso a la Información Pública, a realizar las consultas pertinentes.

VI. Después de admitidas las solicitudes deberá al analizarse el contenido de estas según el Art. 55 del Reglamento de la Ley de Acceso a la Información Pública, con el objeto de establecer si la información será entregada o fundar su negativa; del estudio de la petición se establece que conforme a lo señalado previamente, la SIGET, no es la entidad encargada de regular espacios cibernéticos frente al usos de las redes sociales por parte de los niños, niñas y adolescentes para evitar la depredación sexual, por lo tanto no se posee información; debiendo dictar la resolución de mérito como preceptúa el Art. 56 del mismo cuerpo regulatorio.

SIGET
SUPERINTENDENCIA GENERAL DE ELECTRICIDAD Y TELECOMUNICACIONES

GOBIERNO DE EL SALVADOR

**POR TANTO:**

Ésta oficina en nombre de la Superintendencia General de Electricidad y Telecomunicaciones fundamentada en los Arts. 62, 65 y 72 letra c de la LAIP, basada en los fines de facilitar a toda persona el derecho de acceso a la información pública **RESUELVE:**

a) Declarase incompetente esta Superintendencia para conocer sobre la solicitud de acceso a información del ciudadano **MYNOR LEONEL MARTÍNEZ PINEDA**, según lo manifestado en el considerando IV de esta resolución.
b) Remítase a la dirección electrónica, que se consignó en la solicitud, ésta providencia administrativa en modalidad digital, gratuitamente como preceptúan los artículos 4 letra g. 61 y 102 de la Ley;
c) Notifíquese,
d) Publíquese en versión pública en el Portal de Transparencia con base a lo establecido en los Arts. 30 LAIP y 6 del RLAIP.
e) Archívese.

Licda. Isis Acosta Flores
**OFICIAL DE INFORMACIÓN**

IA/ce

CRONOGRAMA DE ACTIVIDADES

| ACTIVIDADES | MESES | FEBRERO | | | | MARZO | | | | ABRIL | | | | MAYO | | | | JUNIO | | | | JULIO | | | | AGOSTO | | | | SEPTIEMBRE | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | SEMANAS | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| Planteamiento de posibles áreas de Derecho, a investigar. | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Planteamiento de posibles temas a investigar. | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Selección del tema. | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Estructuración de las variables del tema. | | | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Planteamiento concreto del tema. | | | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Planteamiento de las directrices del tema. | | | | | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Inscripción del tema. | | | | | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Elaboración del planteamiento del problema. | | | | | | x | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Revisión del planteamiento del problema. | | | | | | | x | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Revisión del planteamiento del problema y de la estructura del enunciado del problema. | | | | | | | | x | | | | | | | | | | | | | | | | | | | | | | | | | |
| Revisión del planteamiento del problema y de la estructura del enunciado del problema. | | | | | | | | | | x | | | | | | | | | | | | | | | | | | | | | | | |
| Justificación de la investigación y delimitación delimitación de los objetivos generales. | | | | | | | | | | x | | | | | | | | | | | | | | | | | | | | | | | |
| Revisión de objetivos generales y redacción de objetivos específicos. | | | | | | | | | | | x | | | | | | | | | | | | | | | | | | | | | | |
| Replanteamiento de los objetivos generales y específicos. | | | | | | | | | | | x | | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Revisión de objetivos generales y específicos. | | | | | | | | | | | x | | | | | | | | | | | | | | | | | | | | | | |
| Redacción de preguntas de investigación. | | | | | | | | | | | x | | | | | | | | | | | | | | | | | | | | | | |
| Revisión de las preguntas de investigación y elaboración de consideraciones éticas. | | | | | | | | | | | | x | | | | | | | | | | | | | | | | | | | | | |
| Elaboración del marco histórico. | | | | | | | | | | | | | x | | | | | | | | | | | | | | | | | | | | |
| Presentación del marco histórico terminado y elaboración del esquema tentativo de marco teórico. | | | | | | | | | | | | | x | | | | | | | | | | | | | | | | | | | | |
| Revisión del esquema tentativo de marco teórico, propuestas de puntos a plantear en el esquema e inclusión de éstos. | | | | | | | | | | | | | x | | | | | | | | | | | | | | | | | | | | |
| Presentación final del esquema con los puntos a desarrollar y desarrollamos el primer tema. | | | | | | | | | | | | | | x | | | | | | | | | | | | | | | | | | | |
| Revisión y corrección del primer punto e inicio de desarrollo del segundo punto del esquema. | | | | | | | | | | | | | | x | | | | | | | | | | | | | | | | | | | |
| Revisión del punto dos del esquema y se dio inicio al desarrollo del tercer tema. | | | | | | | | | | | | | | | x | | | | | | | | | | | | | | | | | | |
| Correcciones del segundo punto, revisión del punto tres y se inició el desarrollo del cuarto punto. | | | | | | | | | | | | | | | | x | | | | | | | | | | | | | | | | | |
| Presentación del cuarto punto, observaciones y correcciones del mismo. | | | | | | | | | | | | | | | | | x | | | | | | | | | | | | | | | | |
| Presentación del punto cinco y seis, el docente sugirió correcciones. | | | | | | | | | | | | | | | | | | x | | | | | | | | | | | | | | | |
| Corrección de observaciones del punto cinco y seis. | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | | | | | |
| Desarrollo del punto séptimo, se nos observó y se corrigió, iniciamos el desarrollo del punto octavo y noveno. | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | | | | |
| Presentación del punto octavo y noveno y planteamos términos que serán desarrollados en el marco conceptual. | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Presentación del marco conceptual. | | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | | |
| Establecimiento de los lineamientos para la elaboración del marco metodológico | | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | | |
| Elaboración de marco metodológico. | | | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | |
| Revisión de observaciones del marco metodológico. | | | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | |
| Subsanación de observaciones | | | | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | |
| Revisión del diseño de instrumentos para recabar información y subsanación de errores. | | | | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | |
| Revisión y subsanación de marco metodológico. | | | | | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | |
| Revisión y subsanación del vaciado de información. | | | | | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | |
| Revisión de la triangulación de la información. | | | | | | | | | | | | | | | | | | | | | | | | | | x | | | | | | | |
| Revisión de la triangulación de la información. | | | | | | | | | | | | | | | | | | | | | | | | | | | x | | | | | | |
| Revisión e interpretación de datos, supuestos y riesgos de la investigación. | | | | | | | | | | | | | | | | | | | | | | | | | | | | x | | | | | |
| Revisión de matriz de respuestas de las entrevistas y subsanación de errores. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | x | | | | |
| Revisión de instrumentos de encuesta y señalamiento de observaciones a subsanar. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | x | | | |
| Subsanación de observaciones, unificación de instrumentos y redacción de carta de presentación de trabajo de grado ante el Departamento de Ciencias Jurídicas. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | x | | |
| Revisión general del anteproyecto de tesis. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | x |