UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

DEPARTAMENTO DE CIENCIAS JURIDICAS

TEMA:

"LA IMPUNIDAD DE LAS CONDUCTAS LESIVAS A LAS PERSONAS HUMANAS COMETIDAS A TRAVÉS DE LAS REDES SOCIALES EN EL DEPARTAMENTO DE SANTA ANA"

PARA OPTAR AL GRADO DE:
LICENCIATURA EN CIENCIAS JURIDICAS.

PRESENTADO POR:

ESTRADA SEVILLANO, CLAUDIA MICHELLE

MENJIVAR MENDOZA, ELMERSON EVARISTO

REYES ZELAYA, MANRIQUE ALEXANDER

DOCENTE DIRECTOR:

LICDO. Y MASTER NAPOLEÓN HUMBERTO ZAMBRANO

MARZO 2016

SANTA ANA, EL SALVADOR, CENTROAMÉRICA.

UNIVERSIDAD DE EL SALVADOR.

AUTORIDADES CENTRALES.

RECTOR INTERINO.

LICDO. JOSE LUIS ARGUETA ANTILLON.

VICE-RECTOR ADMINISTRATIVO INTERINO.

ING. CARLOS ARMANDO VILLALTA.

SECRETARIO GENERAL

DRA. ANA LETICIA ZAVALETA DE AMAYA.

DEFENSORA DE LOS DERECHOS UNIVERSITARIOS.

LICDA. CLAUDIA MARIA MELGAR DE ZAMBRANA.

FISCAL GENERAL.

LICDA. NORA BEATRIZ MELENDEZ.

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE.

AUTORIDADES.

DECANO INTERINO.

ING. JORGE WILLIAM ORTIZ SANCHEZ.

SECRETARIO INTERINO DE LA FACULTAD.

LICDO. DAVID ALFONSO MATA ALDANA.

JEFA INTERINA DEL DEPARTAMENTO DE CIENCIAS JURÍDICAS.

LICDA. Y MASTER MIRNA ELIZABETH CHIGÜILA DE MACALL ZOMETA.

DEDICATORIA

A DIOS: por haberme permitido culminar mi carrera universitaria, por tomar el control de mi vida y rodearme de personas tan maravillosas; y por qué sin su sabiduría y favor no habría podido alcanzar esta meta.

A MI ANGEL: mi mama Claudia María Sevillano que sé que aunque no físicamente estuvo en el camino recorrido lo largo de estos años, Gracias por la inspiración, por tu amor, educación, principios son lo mejor que me pudiste dar, Gracias totales.

A MI PAPA: Miguel Estrada Palacios Gracias por tu apoyo incondicional y esfuerzo en los momentos más difíciles de la carrera, gracias por transmitirme la confianza necesaria y tener las palabras de aliento en el momento indicado, con tu ejemplo me inspiras a ser un profesional que día a día lucha por alcanzar lo que se propone.

A MIS CUATRO FANTASTICOS: mis abuelos gracias por sus oraciones, por su amor y apoyo incondicional gracias por tener el abrazo necesario, las palabras de aliento y tener fe en que Dios nuestro padre me ayudaría a terminar mi carrera son cada uno de ustedes extraordinarios

A MIS HERMANOS: Miguel Estrada gracias por tu amor, apoyo y por enseñarme a ver la vida desde otra perspectiva, me haces crecer con tus experiencias, siempre vas a ser una de mis razones de salir adelante; André Estrada gracias por alegrar mi vida por ser la alegría en momentos de tristeza.

A MIS QUERIDOS TIOS: Gracias por su apoyo, amor, comprensión ,por su ayuda en cada una de las etapas de mi carrera, Gracias por estar y por animarme a nunca darme por vencida y sobre todo por darme a mis mejores amigos de la vida, mis primos.

A MIS PRIMOS: Gracias por ser parte de mi vida, gracias por estar, por apoyarme y con su ejemplo animarme a salir adelante, son por mucho mis mejores amigos de la vida.

A MIS AMIGOS: sin duda son fundamentales en mi vida, agradezco infinitamente a Dios por permitirme conocer personas tan especiales en los momentos necesarios, han sido una pieza fundamental en este logro ; a los que han estado siempre gracias por apoyarme, creer en mi capacidad y animarme a escalar cada peldaño para poder alcanzar este logro, gracias por marcar mi vida con su amistad especialmente Marcos Valle, Kathy Estrada, Mercedes Castillo; son sin duda alguna de las más grandes bendiciones que puedo tener en mi vida, Gracias por su apoyo incondicional, por su amistad y por estar en todos los momentos durante mi carrera, son otro nivel de personas.

A MIS COMPAÑEROS DE TESIS: Elmerson Menjivar y Manrique Reyes gracias por su esfuerzo y empeño para que este trabajo de grado se realizara con excelencia, y por ser parte de esta experiencia, con su ejemplo me han ayudado a crecer, éxitos en su vida profesional.

A MI ASESOR DE TRABAJO DE GRADO: Licenciado Napoleón Humberto Zambrano, que con su conocimiento, experiencia y apoyo logístico, permanente e incondicional me estímulo para seguir creciendo intelectualmente y para realizar un trabajo de excelente calidad para la Universidad de El Salvador.

A LICENCIADO ALIRIO CARBALLO: por facilitarnos las herramientas necesarias para poder realizar el presente trabajo de grado.

CLAUDIA MICHELLE ESTRADA SEVILLANO

DEDICATORIA

A DIOS: por haberme guiado en los momentos difíciles de mi vida y de mis estudios, por ser el encargado de tener a mi lado a mi familia y mis seres queridos al igual por darme salud y sabiduría durante la realización de mi carrera y así poder alcanzar esta valiosa meta. Gracias por bendecirme en todo momento.

A MIS PADRES: Sonia Elizabeth Mendoza de Menjívar y Luis Alonso Menjívar Rivera por apoyarme en todas las etapas de mi vida como estudiante, gracias por enseñarme valores fundamentales que me hacen ser cada día una mejor persona; también les doy las gracias por amarme y cuidarme siempre, así como también por esforzarse en darme lo mejor, por orientarme en todo momento y enseñarme el camino del bien, para ellos es este logro tan importante en mi vida, los amo a los dos.

A MI HERMANO: Luis Alonso Menjívar Mendoza le doy las gracias por demostrarme su apoyo incondicional durante mis estudios, al igual por ser un ejemplo a seguir para poder triunfar en la vida, por enseñarme que no existen obstáculos para poder alcanzar nuestros sueños, sin la ayuda de él nada de esto hubiese sido posible, te quiero hermano.

A MI NOVIA: Licda. Milena Corina Hernández Sandoval gracias por todo lo demostrado durante mis estudios universitarios, por tu comprensión, apoyo y sobre todo tu amor; también agradecerte por los consejos que me dabas para poder ser una mejor persona y por guiarme siempre en el camino de Dios, eres una persona muy importante y especial en mi vida que amo mucho.

A MI FAMILIA: les doy las gracias por haber confiado en mis capacidades como estudiante y por estar al pendiente de mi desarrollo en la universidad. Son parte importante en mi vida que aprecio mucho.

A MIS COMPAÑEROS DE TESIS: Michelle Estrada y Manrique Reyes gracias por haber realizado esta importante investigación que demuestra nuestras

capacidades como estudiantes, así como también por vivir experiencias únicas dentro de la investigación, gracias por compartir este último esfuerzo al lado de ustedes fue algo muy valioso para mi vida. ¡En hora buena ya somos Licenciados!..

A NUESTRO DOCENTE ASESOR: Lic. Napoleón Zambrano gracias por disponer de su tiempo para las reuniones como grupo de tesis, también por orientarnos durante la investigación realizada y enseñarnos la dedicación y responsabilidad que este trabajo de grado conlleva.

A MIS AMIGOS: por estar en las buenas y en las malas, le doy las gracias por demostrarme su amistad y por haber compartido dentro de la universidad un trayecto de vivencias que nunca olvidare.

AL LIC. RAYMUNDO ALIRIO CARBALLO: gracias por habernos facilitado el material bibliográfico para realizar nuestra tesis, así como también por orientarnos dentro de la investigación.

ELMERSON EVARISTO MENJIVAR MENDOZA.

DEDICATORIA

A DIOS TODO PODEROSO: Por darme vida, fuerza, salud y la sabiduría así como también proveerme de los medios necesarios para alcanzar mis metas. Gracias padre todo poderoso por darme la oportunidad de culminar mis estudios, por tu grande amor y misericordia a ti y solo a ti la honra por reste logro.

A MIS PADRES LUIS ANTONIO REYES Y BERTILA ZELAYA DE REYES: les doy las gracias por su apoyo incondicional, en todo momento desde el inicio hasta el final de mi carrera, por ser un ejemplo de responsabilidad y sobre todo a mi madre por creer en mí y mi capacidad a Dios y a ella le dedico este logro.

A MIS HERMANOS LUIS ANTONIO Y JUAN CARLOS REYES ZELAYA: por ser un ejemplo de perseverancia, superación y su apoyo en todo momento y sobre todo por creer en mí.

A MI HIJA GABRIELA ARLETTE REYES ZELAYA Y SU MADRE: por ser un aliciente para poder salir adelante con mis estudios sin ellas nada de esto fuera posible.

A LA LICENCIADA ÁNGELA ESTER PEÑA Y SU FAMILIA: por ser un apoyo, por su ayuda incondicional, además de estar ahí cuando la necesite.

A NUESTRO DOCENTE ASESOR LICENCIADO NAPOLEÓN HUMBERTO ZAMBRANO: por su comprensión y apoyo a nuestro trabajo. Por acompañar nuestras decisiones y la confianza que nos brindó desde el inicio hasta el final.

AL LICENCIADO RAYMUNDO ALIRIO CARBALLO: por su valiosa aportación y orientación en la elaboración de este trabajo de investigación, y por compartir todo su conocimiento sobre la temática.

A MI TÍA: Rita de Jesús Reyes, por su apoyo incondicional y ayuda brindada en los momentos más difíciles de mi carrera, por incentivarme a luchar y no desmayar.

A MI DEMÁS FAMILIA: A mis cuñadas y sobrinos por su apoyo y darme ánimos cuando los necesite para ellos también este logro.

A MI JEFA ANA MIRIAM MARTÍNEZ: Por darme su apoyo y comprensión en el transcurso de estos 5 años de carrera.

A MIS VECINAS Y DEMÁS AMIGOS EN GENERAL: Por creer en mí y su apoyo incondicional en todo momento, así como también por su comprensión y por compartir este último pasó en la culminación de mi carrera.

A MIS COMPAÑEROS DE GRUPO: Por su compañerismo comprensión por compartir este último paso en la culminación de nuestra carrera.

Así como también a todas las personas que han intervenido durante el proceso de preparación académica y en la elaboración de este trabajo de grado.

MANRIQUE ALEXANDER REYES ZELAYA

INDICE

INTRODUCCION.

La presente investigación sobre la impunidad de las conductas lesivas a la persona humana cometidas a través de las redes sociales en el departamento de Santa Ana, es motivada por la trascendencia propia del tema, ya que es una realidad social que estamos viviendo, debido a que las conductas son realizadas a través de un medio difuso como lo es el internet específicamente por las redes sociales, que si bien es cierto existen requisitos que debe de llenarse para poder ser un usuario de las mismas, estos requisitos están al alcance de cualquier persona que posea un servicio de internet, es ahí donde radica la peculiaridad de la investigación que vamos a realizar debido a que si el medio es difuso, identificar a la persona que reúna las características necesarias para poder denominarlo sujeto activo se vuelve un problema cuando estamos frente a casos que describen este tipo de conductas, es ahí donde el Estado juega un papel muy importante y trascendental por que deberá garantizar la protección de la intimidad de todas las personas y debería ser este mismo el que regule el proceder de cada una de las instituciones que proveen el servicio de internet residencial como empresarial en todo el país especialmente en el departamento de Santa Ana; y prohibiendo comportamientos que vulneren derechos protegidos en la ley primaria de nuestra legislación, siendo principalmente en materia de los delitos relacionados al Honor y la intimidad, que en los diversos Códigos Penales existentes en la historia del Estado Salvadoreño han requerido cambios de forma y fondo de acuerdo a las cambiantes necesidades de la sociedad contemporánea salvadoreña.

El Código Penal vigente regula un capitulo en materia de los delitos relativos a la intimidad, específicamente en el artículo 190, que prohíbe la utilización por cualquier medio de la imagen o nombre de otra persona, sin su consentimiento, con fines periodísticos, artísticos, comerciales o publicitario, constituyendo estas conductas adecuadas al tipo de utilización de la imagen o nombre de otro; así mismo tenemos descrito en el artículo 55 de la Ley especial para una Vida Libre de Violencia para las Mujeres que prohíbe la elaboración, difusión o transmisión por

cualquier medio, imágenes o mensajes visuales, audiovisuales, multimedia o plataformas informáticas con contenido de odio o menosprecio hacia las mujeres; por tanto, con la regulación de esta conducta se pretende contribuir a una cibersociedad libre de violencia y discriminación en los contenidos que se vierten en internet especialmente en las redes sociales; siendo por ello, el tema objeto de estudio.

En el capítulo primero se presenta el Planteamiento del Problema donde se incluye la situación problemática de la investigación de la conducta, el problema fundamental y específicos consecuentes, la justificación, los objetivos generales y específicos, además de los alcances del tema de estudio objeto de investigación.

El segundo capítulo se integra por el Marco Teórico conformado por los antecedentes históricos desde la edad de piedra, el descubrimiento de la red de comunicación más grande a nivel mundial como lo es el internet, realizando un análisis de la forma en que el internet se introdujo en nuestro país primeramente como una herramienta de comunicación para las instituciones gubernamentales hasta ser una herramienta de comunicación común para cualquier ciudadano, asimismo de analizar la evolución que las conductas objeto de estudio ha experimentado en los diversos cuerpos legales como lo son el Código Penal, así como la Ley especial para una Vida Libre de Violencia contra las Mujeres; se desarrollan temas especiales como: La función del Estado Salvadoreño en función a los Delitos Informáticos, la situación actual del ambiente informático en El Salvador, las formas de tipificación de los Delitos informáticos, sus criterios determinantes, las leyes secundarias relevantes que integran el estudio de las conductas cometidas utilizando el internet específicamente las redes sociales, el análisis de Noticias Nacionales acerca de la judicialización de casos cometidos en El Salvador, legislación internacional que regula y tutela estas conductas, y construcción de semejanzas y diferencias entre legislaciones extranjeras y la salvadoreña, así como la existencia de tratados internacionales que nuestro país podría ratificar para una mejor tutela de las conductas lesivas a las personas humanas cometidas a través del internet.

El capítulo tercero, denominado Metodología de la Investigación, presenta la población que está conformada por profesionales de las Ciencias Jurídicas que laboran en los Juzgados de Sentencia de Santa Ana, Fiscalía General de la República Regional Santa Ana y Procuraduría General de la República Auxiliar Santa Ana; así también por personas con conocimientos especializados en la materia de informática las cuales basados en el marco teórico de nuestra investigación son de gran importancia para poder determinar el objetivo de la misma; es así que la población muestreada es aquella de la que a partir se extrajo la muestra y sobre la cual estableceremos como grupo de investigación nuestras conclusiones, siendo el método de la evaluación estadística el que nos permitirá sacar las conclusiones sobre la población muestreada bajo el precepto que esta es adecuada en calidad y en cantidad determinando que esta es representativa de la muestra extraída de una fuente especial y de informantes con especialidad sobre el objeto de estudio en referencia, la recopilación de la información se hará por medio de la entrevista estructurada a profundidad, se recibirá información de una manera estructurada pero metodológicamente se hace necesario procesarla bajo la metodología llamada "Metodología de Triangulación" la cual consiste en una técnica para poder analizar los datos que se recabaron en la investigación cualitativa por medio del instrumento a utilizar.

En el cuarto capítulo, titulado análisis e interpretación de la investigación, se incluye la recopilación, el procesamiento, el análisis tanto el inductivo como el comparativo para posteriormente realizar el análisis de triangulación de los datos obtenidos en la investigación, a través de las entrevistas estructuradas a profundidad dirigidas a especialistas en el tema, que son los sujetos intervinientes en la Judicialización de un caso penal como lo son : los agentes auxiliares de la Fiscalía General de la República, Defensor Auxiliar de la Procuraduría General de la República y Juez de Sentencia del Departamento de Santa Ana, con el propósito de analizar y construir conocimiento sobre las conductas para lo cual fue necesario crear categorías para poder realizar el análisis comparativo de la información y poder crear con esto las conclusiones y recomendaciones de nuestra investigación.

Así mismo se incluye en los anexos de la investigación un marco conceptual con el objetivo de facilitar terminología utilizada a lo largo de nuestra investigación, legislación comparada de los Países Centroamericanos acerca de las conductas lesivas cometidas utilizando como medio el internet, así como noticias de casos que se han conocido en nuestro país para poder determinar el tratamiento que a estos se les ha dado al momento de judicializarlos.

CAPITULO I: ANTEPROYECTO DE LA INVESTIGACION.

1.1 PLANTEAMIENTO DEL PROBLEMA.

Para comprender el desarrollo de nuestra investigación se deberá conocer el origen del internet el cual remonta sus orígenes a los años sesenta. En plena guerra fría Estados Unidos de América crea una red exclusivamente militar, cuyo objeto fue el que se pudiera tener acceso a la información militar en caso de un ataque ruso con el pasar del tiempo esta red que empezó con cuatro ordenadores ya contaba con alrededor de cuarenta ordenadores conectados a través de satélites y ubicados en lugares estratégicos alrededor del mundo tanto fue el crecimiento de la red que su sistema de comunicación se quedó obsoleto viéndose en la necesidad de crear una nueva forma de comunicación que es la que usamos en la actualidad. Las funciones militares se desligaron creando los Estados Unidos de América una red exclusiva para funciones militares. Es así que la NSF (La Fundación Nacional para la Ciencia es una agencia del gobierno estadounidense independiente, que impulsa investigación y educación fundamental en todos los campos no médicos de la Ciencia y la Ingeniería) crea su propia red informática llamada ARPANET (fue una red de computadoras creada por encargo del Departamento de Defensa de los Estados Unidos para utilizarla como medio de comunicación entre las diferentes instituciones académicas y estatales) creando así una red con propósitos científicos y académicos. El desarrollo en las redes fue abismal, y se crean nuevas redes de libre acceso que más tarde se unen a NSFNET, siendo este el origen de lo que posteriormente se conocería como Internet. En nuestro país, surgió en el año de 1996 cuando ANTEL (Asociación Nacional de Telecomunicaciones) se convierte en el único proveedor de acceso conmutado al internet a ese momento, en términos comercialmente factibles, siendo de esta manera la empresa estatal la proveedora principal a las instituciones de gobierno y a las empresas privadas más privilegiadas por tal motivo los medios informáticos eran utilizados como herramientas de desarrollo tecnológico que tuvieron que adecuarse a la necesidad de la evolución de

la sociedad y por consiguiente al uso de la tecnología por un gran sector de la población, en los inicios del año antes mencionado el Internet aún no era tecnología para las mayorías, su fin era más que todo científico con el propósito de conectar a las instituciones en el país como la Universidad de El Salvador, Universidad Centro Americana, Conacyt (El Consejo Nacional de Ciencia y Tecnología) y la Universidad Don Bosco que fueron las primeras en tener enlaces dedicados a Internet en la segunda fase que surgió a mediados del año 1996 y principios de 1997 se conectaron más instituciones de gobierno de cada país cuya finalidad era transmitir información de carácter esencial de la organización interna para integrar una red electrónica en todo el mundo para el intercambio de información científica y tecnológica entre sus pocos usuarios. Para finales del año de 1998 el crecimiento del internet en El Salvador fue notorio debido a que ANTEL (Asociación Nacional de Telecomunicaciones) instala un nuevo servidor para acceso al internet colocando así a la población salvadoreña a la vanguardia de este nuevo sistema, como en todo el mundo es innegable que el avance del internet es acelerado por ello es que el uso del Internet se ha vuelto una práctica cotidiana en el país, en estos últimos años ha crecido enormemente debido a que seis de cada diez personas poseen un sistema de internet en sus hogares lo que nos lleva a la conclusión que más del 60% de la población salvadoreña utiliza el internet especialmente las nuevas generaciones, que desde sus inicios convivieron con la tecnología del internet, por lo que dentro de un tiempo ya el internet será algo intrínseco en nuestras vidas, y su expansión y evolución no la podremos detener. Ahora bien, el internet ha hecho que muchas cosas se mejoren, haciendo procesos más eficientes cuando se hace un buen uso de estos, como ejemplo podemos mencionar que se utiliza para obtener una mejor comunicación entre personas de distintos lugares reduciendo el costo que esto implica, búsqueda de información más accesible por la influencia de países de bagaje cultural mucho más amplio, por ello el internet llega a ser una parte importante para el desarrollo cultural y en cualquiera de los ámbitos para toda persona ya que ofrece ventajas de comunicación; por parte de la gran mayoría de personas que suele utilizar principalmente en establecer contactos y vinculaciones a nivel mundial con familiares, amigos o personas de su círculo social que se

encuentran en todo el mundo superando de esta manera la distancia física, comunicación, educación. Por medio del Internet es posible expresarse y hablar de determinados temas que podrían resultarles difíciles tratar en relaciones directas, lo más importante para la cultura de los pueblos es investigar y conocer debido a que esto les permite encontrar información sobre temas que impliquen avances científicos mundiales que les resulten interesantes y que mediante la utilización del internet se tiene el acceso para cualquier persona con una cultura diferente y esto trae como consecuencia para la mayoría de los pueblos sub-desarrollados una sociedad que depende de los medios informáticos para la realización de sus actividades creando con esto una Ciber-Sociedad que etimológicamente se deriva del prefijo cotidiano Ciber, del cual emana la palabra cibernética entendida esta como el arte de dirigir y manejar sistemas tecnológicos complejos, y de Sociedad que describe a un grupo de individuos marcados por una cultura en común, costumbres y estilo de vida que se relacionan entre sí en el marco de una comunidad. La ciber-sociedad la cual se define como el espacio en donde existen las comunicaciones electrónicas como lo demostraremos en el desarrollo de nuestra investigación y además podemos definirla como un espacio social estructurado a partir de la información virtual, invisible pero absorbente y finalmente es una necesidad humana ya sea por el trabajo, la educación, la cultura llegándose con esto a convertir en una actividad económica, comercial y cotidiana al igual que la participación en el ciber-espacio que permite aumentar considerablemente y tener facilidad de acceso a diferentes tipos de información utilizando este sistema. Sin embargo, no se deben ignorar la necesaria intervención estatal en relación con la diversidad de hechos que pueden ocurrir a través de este medio es obligación de los sujetos que se relacionan con estos sistemas puedan prever y no puede dejar de analizar los peligros y riesgos que puede conllevar el hacer un mal uso del internet ante la diversidad de factores positivos que este posee, porque la información privada puede ser mal utilizada por otras personas para vulnerar derechos fundamentales en relación a la libertad sexual y así actuar con poca educación, cultura y una adecuación a la sociedad moderna con fines delictivos y además ser utilizado para suplantación de identidades, aunque en el internet existan muchas fuentes confiables debemos de

tener cuidado con los propósitos delincuenciales de robo, hurto, estafa, los cuales se podrían realizar utilizando como medio las redes sociales como el Facebook y twitter porque podemos encontrar todo tipo de páginas, que no brinden información correcta. Sobre todo en sectores de la población especialmente influenciables o vulnerables como pueden ser los niños, los adolescentes o las personas con determinados problemas psicológicos, ya que a diario personas sin escrúpulos sacan provecho del anonimato que ofrece el Internet y las redes sociales para realizar conductas antijurídicas en el marco de un orden jurídico y como consecuencia lesivas a otras personas que muchas veces no poseen la madurez suficiente para defenderse de los ataques recibidos o al menos tener la oportunidad de que le sea aclarado la opinión u ofensa vertida en su contra. Por lo dicho anteriormente, en nuestro país la normativa constitucional dispone que El Salvador reconoce a la persona humana como el origen y el fin de su actividad como Estado el cual está organizado con tres pilares jurídicos esenciales los cuales son la justicia, la seguridad jurídica y del bien común definido como Valores jurídicos fundamentales, podemos afirmar que nuestra Constitución busca proteger y garantizar el principio de la Dignidad Humana de las personas pues como ley fundamental según la normativa constitucional este hace referencia a que es un valor inherente al ser humano en cuanto a ser racional y libre, pues las personas mejoran sus vidas mediante la toma de decisiones y el ejercicio de su libertad, siempre y cuando al ejercer sus derechos de los cuales esta envestido, no se vulnere los derechos de otras personas usando como medio el internet es decir en la ciber-sociedad. En este mismo orden de ideas protectoras nuestra Constitución regula que "Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa de los mismos. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen". Protegiendo la carta magna a la imagen, el derecho al honor y a la intimidad de la persona humana pero si bien es cierto nuestra Constitución consagra estos derechos inherentes a la persona humana; en nuestro país no se regulan las conductas lesivas que son relativas a la libertad sexual que se reproducen por los usuarios de los medios informáticos por lo que existen muchas víctimas con tales acciones cuyas

conductas lesivas terminan en hechos delictivos y quedan en su mayoría impunes utilizando el termino anterior como la falta de castigo, ya que nuestro derecho penal salvadoreño no está preparado para sancionar debidamente los delitos que se den en la ciber sociedad debido a la inexistencia de una ley especial que determine las conductas antijurídicas y a la vez establezca una sanción para dichas conductas descritas; actualmente muchos usuarios se aprovechan y utilizan el internet para desprestigiar a personas, como ejemplo de esto tenemos las calumnias que se dan desde el anonimato porque las personas pueden dar su opinión personal sin tener una amonestación por hacerlo, conductas que terminan configurando un delito que la mayoría de veces quedan impunes debido a la falta de individualización del sujeto activo. Se nos hace imprescindible dar a conocer conductas que pueden ser observadas en redes sociales que según nuestra legislación penal las describe como conductas lesivas, las cuales tienen una penalidad al configurar los elementos del tipo. En la actualidad a través de nuestra búsqueda como equipo investigador determinaremos y realizaremos la investigación por medio de un análisis comparado de las conductas lesivas realizadas a través de las redes informáticas, que en su mayoría son conductas lesivas a la libertad sexual reguladas en el Titulo IV Capítulo I Código Penal Salvadoreño regulados bajo el acápite "Delitos contra la Libertad Sexual", conductas que si bien es cierto no siempre encajan en su realización con los medios informáticos de nuestra sociedad, pero que se está volviendo una necesidad dejar de verlos como conductas separadas de estos medios, debido a que la relación social cada vez es más estrecha y estas conductas anteriormente descritas están siendo realizadas a través de la utilización antijurídica irresponsable de los medios informáticos. Por ello se le debe dar un antídoto legal al mal uso del Internet que debe considerarse como un peligro que los salvadoreños hacen debido a la desinformación existente y a la accesibilidad que los medios electrónicos nos han proporcionado, teniendo acceso a internet sin control, sin restricción algún y que el hecho de poder pagar un contrato de servicio de internet, sin incurrir en ninguna responsabilidad y sin tener que dar una explicación del uso de este recurso, ni muchos menos responder legalmente a la acción del caso a través de las redes sociales, sitios web u otros recursos que el medio nos pone a nuestro alcance,

podemos observar a diario conductas lesivas a las personas, cuando comentarios vertidos en redes slas cuales son "comunidades virtuales" es decir, plataformas de internet que agrupan a personas que se relacionan entre si y comparten información e intereses comunes. El cual podemos decir que es el objetivo principal ya sea para reencontrarse con antiguos vínculos o para generar nuevas amistades las cuales tuvieron su origen en el año 1995 en la cual un ex estudiante Universitario de Estados Unidos de America creo una red social en internet a al cual el llamo classmate.com (compañeros de clase.com) justamente para él poder mantener contacto con sus antiguos compañeros de clase dos años más tarde aparecería redes como sexdegrees.com (seisgrados.com) considerándose el primer sitio de redes sociales el cual permitía la creación de perfiles de usuarios y listas de amigos. Del año 2000 al 2002 aparecen los primeros sitios web que promueven el armado de redes basado en círculos de amigos en línea apareciendo más adelante en el año 2004 unas de las redes más conocidas y usadas en la actualidad como lo es Facebook creada por estudiantes Universitarios de Estados Unidos de América cuya función principal es la de hacer nuevos amigos o reencontrarse con antiguos interactuando entres estos por medio de mensajes, publicación de fotos, videos entre otras funciones posteriormente en el año 2006 nace la red social de twitter que aun que no es la más utilizada ha tenido un enorme crecimiento en los últimos años cuya característica principal es él envió de "tweets" o "mini-textos" (Un *tweet* o tuit es el significado que se le da a una publicación o actualización de estado realizada en la plataforma de microblogging conocida como **Twitter**. Como tal, un tuit es un mensaje cuyo límite de extensión son ciento cuarenta caracteres. Puede contener letras, números, signos y enlaces los cuales según las estadísticas son más de 3 millones de tweet lo que circulan por día. Es así que por este tipo de medios es que pueden darse todo tipo de agresiones como acoso, extorción, delitos contra el honor y la intimidad y caer con ello en una conducta descrita y tipificada en nuestra legislación penal lo cual puede verificarse a través de la observación y verificación ingresando a algunas cuentas de redes sociales como lo son Facebook, Twitter, Instagram por mencionar algunas en las cuales se comenten este tipo de conductas y que a pesar de ser redes sociales a las cuales tienen acceso la mayoría de la población no existe

requisitos intrínsecos que deban cumplirse para poder tener acceso a una cuenta. Cabe destacar que las redes sociales no son un requisito básico para una persona, en nuestra generación altamente influenciada por la informática se ha convertido más que en un medio de comunicación, en un medio de socialización y esparcimiento, que en realidad lo que hace es crear una dependencia y con esto aumentar el riesgo de ser víctima de una conducta que vulnere nuestra integridad. Se nos hace importante aclarar que los medios informáticos en el departamento de Santa Ana, el acceso a ellos no es algo que afecte en sentido negativo al país, el problema es el mal uso o el uso discriminativo que hacen algunas personas, al contrario la buena utilización de estos, es lo que podría marcar la diferencia en el desarrollo no solo del país, si no en el desarrollo mundial, es decir la mala utilización de recursos tecnológicos pueda en el caso de la sociedad provocar un estancamiento en ella y dicho factor se convierta en la necesidad de modificar y crear legislación severa en cuanto a medios tecnológicos e informáticos provocando un uso adecuado y responsable de los mismos. En base a lo analizado nuestro problema de investigación es **"QUE ANTE EL CRECIENTE USO QUE LA SOCIEDAD SALVADOREÑA Y ESPECIFICAMENTE, LA SOCIEDAD SANTANECA HACE DE LOS MEDIOS INFORMATICOS, LOS CUALES SE CARACTERIZAN POR CARECER DE MEDIOS DE CONTROL QUE LIMITEN SU USO NEGATIVO Y SEAN UNA HERRAMIENTA PARA EL DESARROLLO CULTURAL DE LOS PUEBLOS, EL USUARIO POR EL CONTRARIO ESTA REALIZANDO CONDUCTAS LESIVAS, A BIENES JURIDICOS TUTELADOS INSUFICIENTEMENTE POR LA LEGISLACION PENAL SALVADOREÑA, PERO LAS CUALES ANTE LA FALTA DE UNA LEGISLACION ESPECIAL ESTAS CONDUCTAS NO SON CASTIGADAS"**

1.2 JUSTIFICACION DE LA INVESTIGACION.

En una sociedad jurídicamente organizada existen derechos los cuales son fundamentales y los cuales están consagrados y tutelados en la constitución por lo tanto como equipo investigador realizaremos un **ESTUDIO DE LA IMPUNIDAD DE**

LAS CONDUCTAS LESIVAS A LAS PERSONAS HUMANAS COMETIDAS A TRAVES DE LAS REDES SOCIALES EN EL DEPARTAMENTO DE SANTA ANA, ya que en la actualidad dichas conductas cada vez son más frecuentes siendo un medio para cometer estos actos que son lesivos por medio del uso del internet y que se cometen a través de las redes sociales y también por medio del uso de dispositivos móviles así como también por computadoras, la problemática anteriormente mencionada debería estar regulada por el Estado o por las entidades competentes más cabe mencionar que existe una total ausencia de Legislación Especial la cual proteja derechos como lo son la intimidad y la moral las cuales son violentados a través de las redes sociales y como grupo vemos la necesidad de hacer la propuesta de investigación para tratar de resolver este problema para que estas acciones por medio de nuestra investigación quedan reflejadas como un problema socio-jurídico y no queden impunes es por esto que la investigación a llevar acabo pretende ser un medio de ayuda alterno para facilitar a todas aquellas personas que quieren saber del tema ya que existe una creciente demanda del mismo, puesto que dichas conductas lesivas se realizan día con día en nuestra sociedad las cuales afectan a todo un colectivo social, debido a que el uso de las mismas cada vez es mayor por lo tanto como grupo de investigación queremos indagar el por qué; es decir las causas fundamentales por lo que las conductas lesivas que daña derechos fundamentales de las personas que se encuentran consagrados en la Constitución quedan impunes y que en la mayoría de los casos se trata de "CONDUCTAS LESIVAS A LAS PERSONAS RELATIVAS A LA LIBERTAD SEXUAL DEL DEPARTAMENTO DE SANTA ANA" utilizando como medio de cometimiento el internet por lo tanto pretendemos aportar a la sociedad santaneca con nuestra investigación una alternativa de solución factible y un conocimiento general el cual será tener la certeza que cuando le sea violentado sus derechos constitucionales a través de estos medios cibernéticos la sociedad sepa a qué instituciones puede recurrir para que se le dé una solución a su problemática teniendo este el conocimiento al menos teórico por medio del presente trabajo de investigación de que le han sido violentado/s ya sea uno o más derechos y que se espera que ya exista una legislación la cual le proteja, en consecuencia nos interesa

de igual manera conocer el funcionamiento que tienen las entidades encargadas de defender los derechos de las personas en el país como lo son la Fiscalía General de la Republica y la Procuraduría para la Defensa de los Derechos Humanos; también conocer la actuación del aparato judicial; así como también el criterio de los jueces de Santa Ana al momento de resolver un proceso en donde se ha vulnerado Derechos Fundamentales relativos a la Libertad Sexual de las personas de Santa Ana, ya que estos derechos están tutelados por nuestra Constitución , pero no existe una tutela de aquellos que su medio de cometimiento sea a través de internet o a través de dispositivos electrónicos como lo son celulares, Tablet o computadoras, esto servirá para discernir y dar respuesta a la interrogante ¿Por qué en el ámbito tecnológico es difícil resolver este tipo de ilícitos? Si el desarrollo y progreso es algo inevitable el medio a través del cual se cometen los delitos también va evolucionando, por ende es necesario la actualización y reforma de los tipos penales, de igual manera como grupo investigador estudiaremos en el transcurso de nuestro trabajo si existe en nuestra legislación la tipificación de dicha conducta la cual es lesiva a la dignidad humana de todo un colectivo social, si esta se encuentra sancionada y descrita en nuestro Código Penal y otra ley especial y que si está a su vez vulnera el derecho relativo a la libertad sexual usando como medio el internet, también llevaremos a cabo un análisis exhaustivo de todos aquellos casos y denuncias los cuales hasta la fecha ha sido presentados por la Fiscalía General de la Republica ante los tribunales, hasta su posible resolución judicial no existiendo un tipo penal de las conducta antes mencionadas la cual viene a representar una de las grandes causas que a nuestro criterio como grupo de investigación hace posible que en la mayoría de las casos sea difícil su comprobación como delito y es posible que no lleguen inclusive a judicializarse.

1.3 OBJETIVOS DE LA INVESTIGACION.

1.3.1 Objetivo General.

- ✓ Realizar un estudio sobre las conductas lesivas a las personas en la ciber sociedad relativas a la libertad sexual en el departamento de Santa Ana con el

fin de lograr determinar cuáles son las dificultades en el proceder de estos ilícitos.

1.3.2 Objetivos Específicos.

- ✓ Examinar la legislación penal salvadoreña a fin de determinar si existe tipificado como delito las conductas lesivas a las personas en lo relativo a la libertad sexual cometidos a través del internet por medio de dispositivos como teléfonos móviles o computadoras.

- ✓ Determinar cuál es el tratamiento que las instituciones pertinentes dan a este tipo de casos que violentan derechos fundamentales y si estas tienen el conocimiento necesario ante este tipo de delitos que tiene una grabe repercusión en la sociedad.

- ✓ Saber cuál es el criterio utilizado por los jueces del municipio de Santa Ana al momento de resolver un proceso en el cual se han vulnerado derechos fundamentales otorgados por la constitución cometidos a través del internet y por medio de dispositivos como celulares o computadoras.

1.4 PREGUNTAS GUIAS DE LA INVESTIGACION.

1.4.1 Pregunta General.

- ✓ ¿Por qué las malas conductas que dañan derechos fundamentales de las personas y que son cometidas a través de las redes sociales quedan impunes en nuestro país?

1.4.2 Preguntas Específicas.

- ✓ ¿Por qué en El Salvador las personas hacen mal uso del internet a tal grado de dañar a otras personas?

- ✓ ¿Cuál es el daño que causan las conductas lesivas a las personas humanas que son cometidas a través de las redes sociales?

- ✓ ¿Qué tipo de legislación en el país es la que se aplica para estas conductas que dañan derechos tutelados por la Constitución?

- ✓ ¿Cómo es el actuar de las instituciones de gobierno que entran en el proceso judicial?

- ✓ ¿Qué debería hacer el Estado salvadoreño para prevenir este tipo conductas no convencionales?

CAPITULO II: MARCO TEORICO DE LA INVESTIGACION.

2.1 ANTECEDENTES HISTORICOS DE LA INVESTIGACION.

La tecnología tuvo su aparición en la edad de piedra con la invención del fuego, las herramientas de piedra, las armas, el atuendo y la música que fueron desarrollos tecnológicos de gran importancia de este periodo; el desarrollo de la tecnología también tuvo su recorrido por las diferentes épocas históricas como edad de cobre y bronce, de hierro, edades media y moderna, etc.; cada una con sus diferentes innovaciones brindando su aporte tecnológico en la época en la que se encontraba, es así como la tecnología ha tenido su avance significativo, es decir que ahora en día la tecnología ha aportado diversos cambios a la humanidad brindando resultados muy buenos para el desarrollo tecnológico de los países. Por lo tanto podemos relacionar con los medios tecnológicos de la actualidad como son la computadora, laptop, celulares inteligentes, Tablet entre otros dispositivos que se van actualizando con el transcurrir del tiempo, en este contexto el primer medio tecnológico de gran valor para el desarrollo de las sociedades es la computadora que data desde el año de 1977 en donde surge ya la computadora personal que llegaron a ser más económicas y se popularizaron a nivel mundial teniendo un auge de gran relevancia debido a que era una innovación tecnológica muy importante para el aporte a las instituciones de gobierno de ese tiempo, porque su aporte de una computadora personal o de escritorio era de un "sistema digital con tecnología microelectrónica capaz de procesar datos a partir de un grupo de instrucciones denominado programa", posteriormente como una evolución se presentó una innovación muy significativa basándose siempre en la computadora personal que fue la denominada "laptop o notebook" que se denomina como una computadora portátil (mac o pc) pensada para usarse de forma móvil. Esta computadora portátil como se le denomina aparece en el año de 1982 pero con el pasar de los años el modelo se fue modernizando lo cual en el año de 1991 aparece la primer laptop que marco tendencia hasta nuestros días y su línea de diseño es la que vemos en la actualidad. Luego con las comunicaciones telefónicas aparece el teléfono inteligente que

en inglés es denominado como *Smartphone* su aparición fue en el año de 1993 pero que en esa época solo estaban disponibles para altos ejecutivos, ya que su precio resultaba prohibitivo para la mayoría de las personas; pero en el año del 2007 aparece al mercado los teléfonos inteligentes con precios que estaban al alcance de las personas que lo quisieran adquirir, su masificación comenzó en nuestro país brindándolos las compañías que prestan los servicios telefónicos de tal manera que a la fecha los Smartphone han causado un impacto en la tecnología de nuestro país.

Con el desarrollo del mercado de estos productos, posteriormente aparecen las Tablet o iPad que su comercialización en los países fue en el año 2010 que mejora las funciones de una computadora portátil y que su tamaño es más grande que un Smartphone aunque con similares características de funcionamiento como la pantalla táctil, con el avance tecnológico de estos medios de comunicación traen como consecuencia la creación del **internet** que ha revolucionado la informática y las comunicaciones como ningún otro medio lo ha hecho. La invención del telégrafo, el teléfono, la radio y el ordenador sentó las bases para esta integración de funcionalidades sin precedentes. "Internet es a la vez una herramienta de emisión mundial, un mecanismo para diseminar información y un medio para la colaboración y la interacción entre personas y sus ordenadores, sin tener en cuenta su ubicación geográfica", los orígenes de Internet a nivel mundial se remontan a más de veinticinco años atrás, como un proyecto de investigación en redes de conmutación de paquetes, dentro de un ámbito militar. A finales de los años sesenta (1969), en plena guerra fría, el Departamento de Defensa Americano (DoD) llegó a la conclusión de que su sistema de comunicaciones era demasiado vulnerable. Estaba basado en la comunicación telefónica (Red Telefónica Conmutada, RTC), y por tanto, en una tecnología denominada de conmutación de circuitos, (un circuito es una conexión entre llamante y llamado), que establece enlaces únicos y en número limitado entre importantes nodos o centrales, con el consiguiente riesgo de quedar aislado parte del país en caso de un ataque militar sobre esas arterias de comunicación.

Este novedoso medio de comunicación aparece en El Salvador en el año de 1990, la Administración Nacional de Telecomunicaciones, ANTEL, era la única institución que ofrecía servicios de telefonía y telecomunicaciones a los

salvadoreños. Sin embargo, comenzaban los proyectos, pruebas y ajustes para permitir que El Salvador pudiese conectarse también a Internet, y de esta manera El Salvador queda conectado satisfactoriamente a internet. En septiembre de 1994 se gestionó, ante el IANA (Internet Assigned Numbers Authority) y el InterNIC (Internet Network Information Center), respectivamente, un conjunto de direcciones IP, equivalentes a una clase B, y la administración del dominio de Nivel Superior correspondiente a El Salvador, SV. Ese mismo mes y año, el grupo SVNet13 , fue constituido por la Universidad Centroamericana UCA, el CONACYT (Consejo Nacional de Ciencia y Tecnología), la Universidad de El Salvador, la Universidad Don Bosco, ANTEL y FUSADES, con el fin de administrar ambos recursos.

2.2 LAS REDES SOCIALES EN EL SALVADOR.

Hoy en día, las redes sociales han logrado gran popularidad a nivel mundial, y es que no solo los países desarrollados gozan de ellas, tanto así que también están presentes en nuestro país. Una red social es una estructura social compuesta de personas (u organizaciones u otras entidades) las cuales están conectadas por uno o varios tipos de relaciones, tales como amistad, parentesco, intereses comunes, intercambios económicos, relaciones sexuales o que comparen creencias, conocimiento o prestigio. De esta manera es como surgen en El Salvador las diferentes redes que se utilizan para socializar por algún medio informático las cuales han evolucionado con el transcurrir de los años, las cuales podemos clasificarlas según el tiempo en el que aparecieron en la cibersociedad; el Messenger fue creado en el año de 1999 pero se innovo en el año 2002 que fue donde ya los usuarios interactuaban utilizando el chat, que facilitaba una conversación a largas distancias por medio de los mensajes en tiempo real.

Posteriormente se crea en el año 2003 la primera red social a nivel mundial que es denominado como el Hi5 pero que en el año 2007 ya era un medio usado por 70 millones de usuarios registrados lo que nos indica que la mayoría de los que hacían uso de esta red social eran de América Latina y era uno de los sitios web más visitados, su funcionamiento se basaba en crear un perfil con datos personales los

cuales se utilizaban para tenerlos en el muro, también tiene la opción de publicar fotos en la red social, además de poderlas comentar entre amigos o seguidores. Seguidamente aparece la red social más popular en la actualidad innovando y tomando como base las funciones que tiene el Hi5, se crea el Facebook y este novedoso ingenio se hizo el 4 de febrero de 2004, originalmente era un sitio para estudiantes de la universidad de Harvard su propósito era diseñar un espacio para que los alumnos de dicha universidad pudieran intercambiar una comunicación fluida y compartir de forma sencilla a través de internet; en el año 2008 Facebook causa una gran revolución al colocarse como la red social más popular a nivel mundial convirtiéndose en parte importante de nuestra vida tanto profesional como personal; por lo que revisar el Facebook diariamente en términos de comunicación social se ha vuelto tan obligatorio, tanto así que nuestro Estado de El Salvador es a nivel Centroamericano el tercer país que tiene más usuarios con perfiles en Facebook.

Posteriormente aparece Twitter en julio del 2006 que fue creado por una serie de jóvenes que trabajan para una compañía de San Francisco de los Estados Unidos de America y se vieron inmersos en un día completo de ideas; twitter estallo a nivel mundial en 2009 masificando sus servicios a los usuarios. Y consta de ser una web gratuita de microblogging que reúne las ventajas de los blogs, las redes sociales y la mensajería instantánea. "Esta nueva forma de comunicación, permite a sus usuarios estar en contacto en tiempo real con personas de su interés a través de mensajes breves de texto a los que se denominan *Updates* (actualizaciones) o *Tweets"*. Luego aparece el WhatsApp como una aplicación de mensajería instantánea de pago para teléfonos inteligentes, para enviar y recibir mensajes mediante Internet, complementando servicios de correo electrónico, mensajería instantánea, servicio de mensajes cortos o sistema de mensajería multimedia; su año de creación fue en el 2009, siendo una aplicación que se desarrolla de manera directa por el Smartphone; posteriormente aparece el Instagram en el año del 2010 brindando el funcionamiento de compartir fotos y videos al perfil, también se pueden compartir a las distintas redes sociales como el Facebook, Twitter y se creó para los sistemas de IPhone, IPod, IPad y sistema Android (Smartphone), el Instagram ganó rápidamente popularidad debido a las características que presenta. La evolución de todos estos

medios tecnológicos en comunicación crea la necesidad de construir La Cibersociedad es decir una fusión entre medios y usuarios que etimológicamente se deriva del prefijo CIBER del cual se forma la cibernética entendida como el arte de dirigir y manejar sistemas tecnológicos complejos y de sociedad que es un grupo de personas que se comunican entre sí buscando el bien común. La cibersociedad es el espacio en donde existen comunicaciones electrónicas, es un espacio social estructurado a partir de la información virtual, es un espacio invisible pero absorbente y finalmente es una necesidad humana ya sea por el trabajo, la educación, el ocio, las actividades económicas, comerciales y las actividades de la vida cotidiana.

2.3 LA REGULACION DE LA CIBERSOCIEDAD.

Poco se ha dicho con relación al medio tecnológico utilizado para la comisión de los hechos (internet) y el medio donde aquel funciona. Internet es el medio de intercomunicación global es la tecnología que permite vincular millones de computadoras y así, acceder desde cualquier sitio del planeta a la información o servicios que se ofrezcan en ella desde cualquier lugar; es un medio en el que no existen las distancias, no existen obstáculos lingüísticos, en definitiva la información crea una nueva estructura global a nivel mundial. El internet a nivel mundial es un medio tecnológico que ha hecho evolucionar a todos los países, ha creado una unión a diferentes regiones del mundo así como también ha facilitado la información, por lo tanto hacer buen uso del internet es obtener facilidades y beneficiarse de las garantías que este posee pero también hacer mal uso de él, acarrea diferentes problemas que pueden trascender judicialmente.

También la participación en este mundo virtual que existen obligaciones y deberes, tan sociales como para quienes participan en el mundo real. Y lentamente aparecen así reglas que vinculan a internautas entre si y a la sociedad virtual con la internauta individual. Ya es utópico sostener estructuras hiperlibertarias, y se van imponiendo aquellas que tienen la necesidad de una regulación estatal. A medida que el internet crea un nuevo estilo de vida en los países insertándose en la sociedad como un elemento que ya es necesario tenerlo, se debe de crear una ley especial

que regule las malas conductas que se realizan al hacer mal uso del internet en las diferentes redes sociales vulnerando así derechos fundamentales de las personas con actos que dañan la libertad sexual. (Gustavo Eduardo Aboso, Cibercriminalidad y Derecho Penal 2006)

Ello significa que puede observarse internet de la forma que a cualquier pueblo o ciudad, país o región de cualquier comunidad; es un espacio público, aunque sea de acceso restringido por requerimientos técnicos económicos, en el que se insertan ámbitos privados, es así que también cualquiera de nosotros tiene la libertad teórica de ingresar en él y usufructuarlo por ese motivo internet se hace privado en la medida que se contrata a una empresa que brinda el servicio de internet como lo es en nuestro país con las empresas de telefonía como lo es Tigo, Claro, Digicel, Movistar. Ciertamente que el reconocimiento mencionado respecto a la cibersociedad puede considerarse un avance interesante, en poco tiempo nos iremos enfrentando a los desafíos que este espacio informático presenta, de igual manera debemos saber que los actos que se realizan por medios tecnológicos no debe de vulnerar derechos individuales protegidos por la carta magna, la Constitución de la Republica. El espacio informático debería de tener un límite, es decir restringir a aquellas personas que hagan mal uso del internet afectando los derechos individuales y la única manera por la que se puede limitar es creando una ley especial compleja que regule todo tipo de conductas que dañen los derechos de otra persona y que usen como medio de cometimiento el internet por medio de sus diferentes redes sociales existentes.

2.4 SEGURIDAD EN INTERNET.

Para poder realizar un análisis de la seguridad en internet existen una cantidad de factores que deben ser examinados como son la fuente del ataque, calidad de los atacantes y atacados. Factores que no se pueden perder de vista cuando se retoma el nuevo ámbito en el cual se desarrolla el hombre modernamente, posibilitando con la aparición del internet, es fácil pensar que existe un ámbito nuevo donde se necesitaran reglas para evitar caer en conductas antijurídicas, así como los

encontrados dentro del Título VI del Código Penal Salvadoreño delitos relativos al honor y la intimidad previstos y sancionados en el Capítulo I y más específicamente los que se refieren a la Calumnia y la Injuria, Difamación, así mismo los del Capítulo II De los delitos relativos a la intimidad, violación de comunicaciones privadas, utilización de la imagen o nombre de otro, los cuales son cometidos por un medio diferente es decir utilizando el Internet y más específicamente las redes sociales, y en estos casos son víctimas y victimarios las mismas las personas que forman parte de una red social es decir aquellas personas que con el fin de ocupar para comunicación esta herramienta comparten información necesaria que es utilizada por las personas que ven una ventana para el cometimiento de un ciber-delito; es por eso con la existencia de internet viene aparejada la necesidad de proteger los derechos fundamentales de la persona que son vulnerados a través de medios electrónicos como computadoras, Tablet, Ipad, Smartphone; surgiendo así la nueva categoría de ciber delitos, que son aquellas conductas ilícitas que su medio de cometimiento es el internet usando las diferentes redes sociales. (Anibal, 2002, pág. 63)

Es una necesidad que había que prever debido a que el internet entre los miles de usos que posee puede ser utilizado para el cometimiento de conductas lesivas está contemplado, debido a la idoneidad del medio, el cual es fácil de desvincular la responsabilidad así como la difícil tarea de individualizar al sujeto activo, pero en nuestra legislación aún no se ha contemplado reformas para poder adoptar figuras nuevas de realización de los tipos penales, los cuales son clasificados técnicamente como "ciber-delitos" que según el Libro (El Ámbito Electrónico y sus formas de Comunicación en su Pág. 64) establece que los Ciber-delitos son nuevos grupos de ataques contra bienes jurídicos tutelados por la Constitución de la Republica pero que son vulnerados a través de medios electrónicos. Es por esto que se hace necesario establecer diferencia entre un delito analógico que vamos entender por ello una conducta delictiva cometida y que no necesitan que el medio de cometimiento reúna características especiales y un Ciber-delito que es un delito que puede estar descrito en un tipo penal pero cuyo medio de cometimiento va relacionado a la utilización de internet y más específico a las redes sociales (Anibal, 2002, pág. 64)

2.5 FUNCION DEL ESTADO EN RELACION A LOS DELITOS INFORMATICOS.

Para analizar la situación actual del ambiente de la información y en especial, la del tratamiento que se le ha dado a través de los delitos informáticos, se hace necesario partir de un marco teórico y conceptual sobre el actual describir de las acciones dañosas relacionadas con el ambiente informático, y a partir de dicho marco, reflexionar críticamente sobre la respuesta penal del Estado a tales conductas.

En primer lugar, reflexionar en cuanto a la Misión del derecho penal, de si dicha misión es la protección de bienes jurídicos o si tal misión es la protección de funciones, pues aunque no se admita expresamente, las recientes respuestas estatales tienen una propensión fuerte hacia esta última en la construcción de los tipos delictivos, al carecer de contenido el bien jurídico tutelado en dicha construcción. De igual forma, se hace necesaria una reflexión sobre la ya asentada tendencia de un Derecho Penal consecuencialista es decir es una postura mental en los terrenos de la moral una posición que tiene como base las consecuencias de las acciones para juzgar si estas son buenas o malas es así que una conducta es buena si los efectos que produce son buenos y será mala si los efectos y consecuencias que produce son malos esto se considera que esta sobre un Derecho Penal Principialista que no es más que la legitimación del derecho penal a partir de los principios Constitucionales. De ahí que necesariamente también, deban abordarse las diferentes concepciones de la Criminología y la Política Criminal frente a la respuesta estatal ante los novedosos delitos informáticos. La importancia de dicha reflexión es a efecto de analizar las nuevas tendencias de la política criminal en los delitos informáticos y hacer un enfoque crítico a la situación actual de los delitos no convencionales. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 166)

2.5.1 Misión del Derecho Penal en las Legislaciones de los Estados.

La doctrina mayoritaria afirma que la misión del derecho penal es la "protección de bienes jurídicos del ciudadano y de la comunidad" frente a las lesiones o puestas

en peligro de lesión, aunque hay que admitir que tal misión no es de pacifico consenso, existiendo al menos en la actualidad, otras dos tesis discrepantes una de estas es la que formula Welzel que es la de "Proteger Valores de la actitud interna de carácter ético social que existan en la sociedad, y solo en la medida que está incluida en ellos la protección de bienes jurídicos" y la otra es la de Jacobs la cual dice que "La Prevención general que confirma el reconocimiento normativo".

En el caso de otros países, la decisión del consenso democrático manifestado en la Constitución, sea adhiere expresamente a la idea de las protección de los bienes jurídicos, y que en derecho penal es conocido como "Principio de Lesividad, "donde las acciones privadas que no dañen la moral o el orden público, o que no perjudiquen a tercero, están fuera de las acción de la ley", respetándose en consecuencia la esfera individual de las acciones humanas frente a la injerencia estatal, a menos que estas sean lesivas a la moral, al orden público o a terceros, debiendo ser tal intervención estatal, "necesaria", "útil", "razonable" y "oportuna", como lo ha sostenido la jurisprudencia constitucional Costarricense (Sala Constitucional, Voto 6273-96) la cual expresa… De igual forma se ha sostenido que las limitaciones a derechos fundamentales, para que sean legítimas, deben: 1. Estar llamadas a satisfacer un interés público imperativo; 2. Para alcanzar dicho interés, debe escogerse entre varias opciones aquella que restrinja en menos escala el derecho protegido; 3. La restricción debe ser proporcionada al interés que la justifica y ajustarse estrictamente al logro de tal objetivo; 4. La restricción debe ser imperiosa socialmente y por ende excepcional… (Constitución Política de Costa Rica, anotada y acordada con jurisprudencia de la Sala Constitucional. Sin embargo, existe una tendencia actual en la que se adelantan "las barreras protectoras" del derecho penal, a fases previas a las actos de ejecución y ello se ve manifestado en los delitos informáticos, como se demostrara más adelante. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 168)

Es decir que será necesario explicar las definiciones básicas de lo que constituye los delitos informáticos hasta llegar al grado de afectación que estos pueden llegar a producir ya sea desde el punto de vista consecuencialista es decir por el grado de afectación que puede llegar a producirse sobre un determinado bien

y que afecte el grado de satisfacción que este le cauce a la persona, o desde el punto de vista principialista, es decir visto desde el punto de vista de principios enmarcados en la constitución y como estos pueden son cometidos día con día conformado por cualquier particular conociéndole a esto como delitos no convencionales en estas se lesiona el bien jurídico que son protegidos por las leyes pero que no necesitan una protección especial.

Por tal motivo nos hace necesario a realizar un análisis de la misión del derecho penal ya que por lo mencionado anteriormente han surgido diferentes tesis sobre qué es lo que se protege si el bien jurídico o si protege valores haciendo necesario la injerencia del estado a tal grado de proteger ya sea el bien jurídico o los valores haciendo necesario la injerencia del estado a tal grado de proteger ya sea el bien jurídico o los valores en lo referente a los delitos cometidos en la "ciber-sociedad".

2.6 LA INFORMACION COMO NUEVO PARADIGMA DEL DERECHO PENAL.

2.6.1 La autonomía de los llamados Delitos Informáticos y su objeto: la Información.

Por lo general, existe consenso doctrinario judicial extendido en cuanto a aceptar la nueva categoría de delitos informáticos, así pues esta nueva forma de criminalidad se relaciona directamente, con el uso o la intermediación de un elemento o dato informatizado. Más allá de procesos de formalización de categorías jurídicas, el empleo del termino delitos informáticos impone un auténtico desafío para el Estado de El Salvador, en relación con su ordenamiento normativo. Lo cual es el de tratar de definir el objeto propio de esta moderna clasificación y de tipificar estas conductas lesivas a derechos fundamentales de las personas constitucionalmente hablando; es decir en primer lugar interrogamos sobre la base cierta de esta novedosa forma de criminalidad asociada a la tecnología que se está generando en la sociedad salvadoreña.

De esta manera existen áreas jurídicas posibles para recorrer; el primero está constituido por la indagación sobre la existencia o no de un nuevo interés social que demanda de urgente protección jurídica, particularmente la ofrecida por el derecho

penal a través de una sanción con pena de cárcel; el segundo diametralmente opuesto al primero, correr el velo de esta supuesta necesidad normativa de regular el uso abusivo de los elementos y datos informáticos, revelar así que lo que se subyace en el fondo una nueva norma de arista carente de tutela jurídica de bienes jurídicos conocidos por todos. (Gustavo Eduardo Aboso, Cibercriminalidad y Derecho Penal 2006, pág. 17)

Como se desarrollara en la investigación y como equipo investigador, consideramos que la primera opción es la correcta, es decir, el avance tecnológico que representa internet y los problemas que presenta el uso generalizado de los sistemas informáticos generan necesidades propias para el derecho penal, que ahora tiene un nuevo interés social digno de protección; la información y su transmisión a través de los sistemas telemáticos.

Se refiere que la información es confidencial es una necesidad proteger con una ley que regule las conductas que dañen los derechos de las demás personas por lo tanto de acuerdo al avance tecnológico y a lo que ahora en día representa el internet en nuestra sociedad podemos decir que así como trae beneficios también acarrea problemas ya que se ha vuelto un medio por el cual acceder a información es de manera muy fácil y rápida, pero sin ningún límite que regule las acciones negativas del usuario.

Este punto de partida metodológico no implica desconocer la función de vehículo de expresión de pensamientos, posibilidad y ampliada por estos sistemas digitalizados, pero lo cierto es que el dato y su capacidad de almacenamiento, procedimiento, transmisión, empleo, y los mecanismos automatizados que presupone, normalmente, la intermediación de máquinas en la vida moderna en general, y en el tráfico mercantil en particular, importa imponer, de manera concreta una nueva visión de la realidad y la necesidad de regular dichos procedimientos. (Gustavo Eduardo Aboso, Cibercriminalidad y Derecho Penal 2006, pág. 18)

De igual manera se deben de regular todas aquellas expresiones en donde se utiliza el internet y se favorecen de las redes sociales expresando pensamientos en los cuales daña la moral y la imagen de la otra persona debe de tener una consecuencia jurídica ya que nuestra legislación no cuenta con una ley especial que

regule las conductas que vulneren derechos fundamentales cometidos a través de las redes sociales; cuando hablamos de medios cibernéticos, nuestro país no ha avanzado en cubrir esta necesidad de proteger los derechos fundamentales de las personas por esta área tan delicada la cual es el internet y que muchos se favorecen por la falta de una ley especial en nuestra legislación; favoreciéndose de esta manera al delincuente en poner en la red imágenes que son alusivas a la pornografía pero que el sujeto pasivo de esta acción es una persona natural que tal vez haya tenido una relación amorosa con el sujeto activo de esta acción delictiva.

Para poder responder a la pregunta original, será necesario determinar si la información y las imágenes difundidas de carácter sexual en las redes sociales pueden llegar a ser consideradas como un delito, de acuerdo a los artículos 1, 2 y 6 de nuestra Constitución, si deben de ser considerados como actos que recaigan en un hecho punible y que cuya protección de los derechos demanda una respuesta sancionatoria de carácter penal.

2.6.2 Situación Actual del Ambiente de la Información en El Salvador.

El desarrollo de la informática ha incidido en una serie de cambios vertiginosos que no se limitan al ofrecimiento de ordenadores en el mercado internacional, sino en el cambio de actitud de los distintos sectores, en la absorción de tales herramientas informáticas en sus actividades. Lo anterior ha generado una enorme fluidez de información, haciendo que las distancias se acorten exageradamente, haciendo de este mundo lo que ha sido denominado "cibersociedad" donde se mueve una enorme y compleja "cantidad de información".

Ello ha generado nuevos riesgos para el ciudadano salvadoreño, que repercuten en la esfera del desarrollo de su personalidad, pues al obtenerse y cruzarse la distinta información, esta puede utilizarse para limitar su participación diferentes aspectos de la vida cotidiana así como también para elaborar su "perfil de ciudadano" ya que los sitios de redes sociales en internet permiten crear perfiles de usuario, agregar fotografías, compartir información personal lo cual puede dar lugar ser vigilado en sus actividades diarias o personales como la realización de compras

en línea conseguir noticias, alquileres, obtener servicios médicos y hasta posiblemente la información de tipo electoral debido a la participación en encuestas de opinión; por lo que la poca privacidad personal que una vez se tenía, corre el grave riesgo de desaparecer. De igual forma, el empleo de esta novedosa tecnología puede ser utilizada para actividades delictivas, con la diferencia en que a través de la red de internet y el uso de las distinta tecnología como lo es a través del uso de computadoras portátiles las cuales no es necesario que estén fijas en un escritorio para que puedan ser utilizadas mayormente conocidas como laptop, o también el uso Tablet la cual no es más que un nuevo dispositivo el cual tiene funciones similares a las de un ordenador o computadora pero que se presenta en un asola pieza sin teclado físico, con un diseño plano, fino y compacto, o por medio del uso de teléfonos celulares de última generación lo cuales tiene a parte de la función de poderse realizar llamadas funciones similares a las de una computadora con opciones de conectividad a internet objetos mediante los cuales pueden borrarse las huellas con mayor facilidad y mantener hechos delictivos en la impunidad .

Respecto a la seguridad en internet y al manejo de esa información, si bien se han empleado políticas de privacidad por parte las empresas que tienen bancos de datos de las personas que hacen uso de estas redes, estas no son suficientes y no constituyes una garantía para el ciudadano frente a la actitud de los gobiernos de adoptar una posición de no intervención en relación con las políticas de privacidad en internet esto puede deberse al interés de los Estados de no ser juzgado en cuanto a que está realizando una intervención directa hacia las empresas las cuales están obteniendo un beneficio monetario y que por consiguiente tienen un enorme poder el cual les puede permitir que estos influyan en los Estados para que estos no intervengan así también se relaciona con que puede violentarse la libertad de expresión, es debido a esto que se espera que las industrias se regule así mismas como por ejemplo: en varios Estados de los Estados Unidos de Norte América, han decretado ya sus propios estatutos sobre la privacidad personal, por lo que el Congreso está discutiendo actualmente Proyectos de Ley que han sido diseñados para regular el manejo de diferentes tipos de información personal, que van desde registros médicos hasta información financiera y medios de comunicación escritos.

Sin embargo, una cosa es cierta la reunión en línea de los datos personales no desaparecerá. La cuestión verdadera es sobre quien está en control del perfil de las personas en línea, y sobre quien puede tener acceso, así como también quien lo está vendiendo y hasta los vendedores de productos para proteger el anonimato, admiten que no hay solución fácil al problema del comercio en línea y la divulgación de información de tipo personal/privada causando con esto una inseguridad en los usuarios respecto al manejo que se hace de información de tipo personal. Aun frente a programas de seguridad que son capaces de proteger la identidad mientras la persona navega, envía correos electrónicos o asiste a foros de discusión en línea, el problema real es que tan pronto como el usuario decide comprar algo en línea, su identidad queda al descubierto y desprotegida.

Todos estos problemas hacen que el actual ambiente informático este lleno de riesgos para los ciudadanos, que van desde la vulneración de la intimidad de la persona humana, es decir su ámbito recóndito del desarrollo de su personalidad, hasta novedosas formas de delincuencia, frente a una "sociedad de riesgos" terminología dada por Beck Ulrich la cual es la Fase de desarrollo de la sociedad moderna donde los riesgos sociales, políticos, económicos e industriales tienden cada vez más a escapar a las instituciones de control y protección de la sociedad industrial , de diferentes tipos financieros, sociales, laborales, tecnológicos, etc., que hacen que la sociedad este con un "miedo al crimen", y que exija del Estado nuevos políticas para generar un Estado de seguridad a través de la guerra del crimen, leyes simbólicas, especialmente de carácter penal, siendo la respuesta del Estado la que es percibida por la ciudadanía como la más eficiente y eficaz, convirtiéndose con esto al Derecho Penal, que con el afán de materializar dicha tranquilidad ciudadana, se vaya tornando en un Derecho Penal de amplio espectro, adelantando las barreras punitivas y despojándose de fundamentos dogmáticos de un Derecho Penal Democrático. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 163)

Es debido a esto que la situación actual de la información que circula en el internet debe ser regulada por una normativa que no solamente regule y castigue a quien cometa un delito a través de estos medios sino que tenga como uno de sus grandes objetivos actuar de forma preventiva todas aquellas situaciones que puedan

cometerse a través de las redes sociales haciendo uso de dispositivos como tablet, laptop y teléfonos inteligentes ya que como se ha mencionado anteriormente son los medios más usados para el cometimiento de delitos que atentan no solamente contra el honor y la dignidad sino que también contra el Derecho a la Intimidad de las personas el cual se encuentra en la Constitución en su artículo 2 como un derecho fundamental como lo es la Intimidad y que hasta el día de hoy no hay normativa que regule este tipo de situaciones con el fin de proteger este derecho.

2.7 FORMAS TIPICAS ESCOGIDAS DE DESCRIPCION DE DELITOS INFORMATICOS.

Los comportamientos relacionados con medios o procedimientos informáticos que pueden alcanzar relevancia penal son muy variados. Un mismo procedimiento comisivo puede dar lugar, según los casos, a diversos tipos de fraude o manipulación, pudiendo ser analizado desde la perspectivas de varios y distintos delitos, según la ocasión; del mismo modo que, en otras, el uso de la informática no supone más que un modus operando nuevo, que no plantea particularidad alguna respectos de las formas tradicionales de comisión de delitos. El tratamiento penal de estos supuestos delitos depende de la conducta que se realice y del tipo de datos o ficheros que se vean afectados. Las posibilidades que pueden generarse en la práctica son muy variadas, por lo que para abordar el tratamiento penal de los distintos tipos escogidos distinguiremos los siguientes apartados. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV)

2.7.1 Formas Típicas de los Delitos Informáticos.

En el presente trabajo de investigación como equipo investigador enunciaremos las principales formas típicas de la utilización de las herramientas informáticas en la comisión de los delitos, para luego analizar las respuestas del Estado ante estas nuevas formas de criminalidad. Ejemplo de este tipo de delitos son: la Manipulación de los Datos de Entrada (-Input-), Acceso No Autorizado a Servicios y Sistemas Informáticos, Acceso No Autorizado a Servicios **y** Sistemas Informáticos, Espionaje,

Interceptación de E-Mail y Ciberdelito; por lo tanto cada figura se desarrollara a continuación.

2.7.2 La Manipulación de los Datos de Entrada (-Input-).

Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos que ocupa, para que en una fase posterior activar su acción nociva para la que ha sido programado. Los efectos que causan los virus son muy variados algunos se limitan a mostrar un mensaje en la pantalla; otros a producir sonidos extraños; otros a consumir espacio en el disco y a realizar el trabajo del ordenador, y otros causan diversos daños, hasta llegar a la pérdida total o parcial de los datos del ordenador. Por último, atendiendo a las partes del software que modifican, los virus se clasifican en dos grupos, virus del sector arranque, que sustituyen al sector de arranque original del disco y se activan cuando se enciende el sistema, y virus de programas, que se añaden en los ficheros ejecutables, es decir en los ficheros que almacenan los código que se ejecutan directamente en el ordenador, y se activan únicamente cuando se ejecuta el programa cuyo fichero ejecutable está infectado. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 199)

2.7.3 Acceso no autorizado a Servicios y Sistemas Informáticos.

Es el uso ilegitimo de password (contraseña) y la entrada en un sistema informático sin la autorización del propietario, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 203)

2.7.4 Espionaje.

Es el acceso no autorizado a sistemas informáticos gubernamentales e interpretación de correo electrónico del servicio secreto, entre otros actos que podrías ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera, existe el espionaje Industrial que es el acceso no autorizado a sistemas informáticos de grandes compañías, usurpando diseños industriales, formulas, sistemas de fabricación y estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada, en este tipo de actos delincuenciales, ha tomado mucho protagonismo la figura del "insider trading", o empleados de la administración pública o de empresas, que trabajan en un determinado campo o como el personal del proceso de datos, que son quienes normalmente, dentro de la misma administración (bolsa de valores, como por ejemplo) o de las empresas privadas, sirven como espías y venden dicha información privilegiada. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 203)

2.7.5 Interceptación de e-mail.

En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad, (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 204) existe una serie de actos parasitarios realizados por usuarios incapaces de integrarse en grupos de discusión o foros de debate on-line (en línea o conectado), se dedica a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales.

2.7.6 Ciberdelito.

Ciberdelito, conductas lesivas a una persona los cuales presentan cuatro elementos característicos los cuales son: 1.Falta de una debida tipificación, lo cual no

solo se vuelve un problema a la hora de individualizar a los sujetos activos, si no al momento de luchar con la ciberdelincuencia, 2.No se requiere de presencia física para la comisión del hecho, 3.Se requiere poca inversión, comparada con el daño que causa, 4. Su expansión es rápida. (Anibal, 2002, pág. 65)

La mayoría de problemas surgen con los delitos perpetrados a distancia, muy frecuentes en Internet, y en los que la acción y el resultado se producen en diferentes países. La doctrina y la jurisprudencia se han manifestado más favorables a apreciar la teoría de la ubicuidad que tiene en cuenta como lugar de comisión del delito tanto el lugar en el que se ha producido la acción como el resultado dañoso, en muchas ocasiones, la conducta delictiva se puede haber llevado a cabo en un país con una legislación diferente la cual en muchas ocasiones puede ser incompleta o permisiva con respecto a conductas nocivas cometidas a través de la red, o que no poseen medios de detección no han ratificado ningún tratado con el país en el cual tenga repercusiones la acción para poder castigar este tipo de conductas, lo cual dificulta aún mucho más la investigación y enjuiciamiento de estas conductas.

Un ciberdelito tiene una alcance vasto así como la red misma, por lo que aunque en algunos países exista legislación que busque contrarrestar este tipo de conductas, no se ha podido obtener los resultados que se buscan, porque para penalizar este tipo de conductas debe de existir una tipificación de los estándares mínimos delictuales en la red que configuren una conducta exigible, que permita de este modo sancionar, en cualquier lugar y de forma universal este tipo de conductas. En países como España se han realizado intentos por codificar de alguna forma los estándares mínimos delictuales para poder obtener un tipo penal ya que los ciber-delitos son una clara amenaza a la privacidad e integridad de cualquier persona que tenga acceso al mundo del internet. (Anibal, 2002, pág. 66)

2.8 FORMAS DE INICIAR LA INVESTIGACIÓN.

Suele iniciarse con una denuncia realizada por los particulares afectados por la conducta delictiva o por solicitud a instituciones encargadas de garantizar la seguridad de las personas, en nuestros casos estas instituciones pueden ser: La

Fiscalía General de la República, la Procuraduría general de la República, Fiscalía Debido a que la perpetración de delitos tecnológicos o informáticos se está incrementando exponencialmente se han creado unidades especiales de investigación en el Cuerpo de Policía Nacional Civil y de la Fiscalía especializada en delitos informáticos, resulta obvio que en el mundo tan técnico y avanzado de las nuevas comunicaciones se hace necesario recurrir a expertos que asesoren en el modo de desarrollar la investigación es por ello que se hace necesaria la especialización de los peritos para dar respuesta a las soluciones que la sociedad demanda contra la delincuencia informática. Igualmente se hace necesario que las Fuerzas y Cuerpos de Seguridad del Estado dominen herramientas y conocimientos para poder detectar y hacer seguimiento de las conductas delictivas para identificar a su autor, muy especialmente en los delitos informáticos resulta importante destacar que los infractores suelen conocer muy bien el medio empleado para la comisión delictiva por lo que se convierten en especialistas para borrar las huellas o rastros que quedan en la red hasta dejar sin armas a las víctimas para señalarlos como autores. (Eduardo La Valoracion de la Prueba Electronica, 2009, págs. 52-55)

2.8.1 Surgimiento y Evolución de la "Privacy" (privacidad) o Intimidad.

El "privacy" (privacidad) surge en un principio, dentro del marco de los derechos fundamentales de carácter burgués, sobre la idea de la propiedad, extendiéndose posterior mente a la vida privada, o derecho a la intimidad, como lo recogen los textos españoles, configurándose como presupuesto de la libertad individual.

Así, la intimidad o "privacy" "(privacidad), tiene dos manifestaciones: el del secreto de la morada, que implica el derecho a la no intromisión al espacio físico, intimo, privado no público, en el que la persona desarrolla su intimidad; y el secreto de las comunicaciones, por el que se garantiza que el intercambio de ideas, palabras, mensajes, entre dos o más persona (emisor-receptor), no podrá ser interrumpido, divulgado ni interferido por terceras personas ni por el Estado.

De igual forma, la idea de "privacy" o intimidad, se hace extensible para salvaguardar otras órdenes como honor, fama, imagen, pues hay cierta información íntima o privada, que puede resultar lesiva para tales derechos.

Siendo esa la idea en la que ha descansado el contenido del derecho a la "privacy" o intimidad, resulta insuficiente para la protección de la persona, ya que aunque se cree una normativa adecuada ante el cometimiento de este tipo de delitos siempre conllevara la afectación de otros bienes jurídicos esto debido al surgimiento y desarrollo de las nuevas tecnologías. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 193)

2.8.2 Privacy (privacidad), Intimidad y Autodeterminación Informativa.

La sociedad moderna ofrece una serie de ventajas para el individuo, en cuanto a sus expectativas de vida, medios de transporte y comunicación más eficientes, etc. Y dentro de tales ventajas, se destaca el avance tecnológico que ha tenido la informática.

Sin embargo, al mismo tiempo que eleva las condiciones de vida ,mediante la adquisición de dispositivos electrónicos los cuales le permiten tener acceso a una amplia y diversa gama de información y prestación de servicios por parte de muchas empresas, sobre todo en cuanto al manejo de la información ha hecho que se ponga en grave riesgo a la persona, en un aspecto: en el de elaboración de un perfil de su personalidad y consiguiente divulgación de todo tipo de información de tipo personal con la finalidad de causar un daño así como también para fines de control y vigilancia, o para fines de mercado, lo que implica que el inicial concepto de "privacy" (privacidad) como derecho fundamental, de origen anglosajón se ha modificado sustancialmente según Fermín Morales Prats ya que hoy en día se toma como "el derecho a gozar de la vida, o sea el derecho a estar solo". (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 192)

2.8.3 El "Privacy" (privacidad) o intimidad y la Sociedad Informatizada.

A diferencia de lo que se creía a modo de ciencia-ficción, que la persona se vería vigilada por el Estado omnisapiente y omnipresente almacenando información de todos los ciudadanos, en la realidad y actualidad ya no es una simple ficción, porque los "bancos de datos" de esa información está en manos de sujetos privados, de tal suerte que el Estado no tienen necesidad de tener tales bancos de datos, un pilar básico y fundamental de un efectivo sistema de protección de datos personales es la garantía de la seguridad de la información, entendida ésta como la implementación de medidas administrativas, físicas y técnicas eficaces para garantizar y velar por la integridad, confidencialidad y disponibilidad de tus datos personales aunque este deberá ser un pilar básico y fundamental de un efectivo sistema de protección de datos personales en garantía de la seguridad de la información. Contribuyendo con esto a minimizar los riesgos de acciones en contra de la información personal como robo, alteración, modificación o pérdida total o parcial de esta mediante la promulgación de leyes orientadas en este sentido y no conformase con solo tener únicamente acceso a todas esas grandes existencias de datos en manos de particulares.

De ahí que la acumulación, de archivos y divulgación indebida de datos contenidos en sistemas informáticos, puede representar peligros para la persona, como se ha indicado antes, tanto a nivel de su participación democrática ya que mediante el registro de la persona en bases de datos para la obtención de documentos de identificación personal puede existir una estrecha relación entre esta información y la que puede darse al momento que se ejerce el derecho Constitucional como lo es el voto en donde puede ser comparada dicha información con la que el Estado tienen de la persona y la que se encuentra en los organismos encargados de estos procesos, otro peligro es a nivel de intimidad como cuando se elabora un perfil de su personalidad en alguna red social produciéndose una intromisión en la esfera de la intimidad personal, pero que no se encuentra protegida dentro de la clásica concepción del "privacy" o derecho a la intimidad, pues no implica una intromisión física a la morada, ni una interferencia o interrupción de las

comunicaciones, poniéndose en peligro el secreto, el honor, la imagen, intimidad y otras manifestaciones de la personalidad, ante el manejo de dicha información, con la posibilidad que dicha información sea "cruzada" debido a la falta de legislación adecuada que regule el manejo y uso de esta por terceras personas y evitando con esto que sea utilizada para limitar la participación democrática del ciudadano, o ser vigilado en su conducta, sin que él se entere siquiera, ante los nuevos medios de investigación delictiva en esta aérea en cuanto a lo que se le exige a un Derecho penal eficiente (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 193).

2.8.4 La Auto Determinación Informativa.

Ya que el concepto tradicional y su tutela se encuentran imposibilitados de proteger al ciudadano ante los riesgos de la sociedad tecnológica, se ha hecho necesario proteger la dignidad de la persona humana, el libre desarrollo de su personalidad y su afianzamiento de la libertad en la sociedad democrática, frente al control de las informaciones de ahí que se hace necesario garantizar al ciudadano un estatus positivos conocidos por el termino romano como status civitatis y no es más que: la facultad que el hombre libre sea sujeto de derechos y obligaciones. Esto implica la tutela jurídica: Para auto determinarse en una sociedad marcada profundamente por las tecnologías de la información; y para prevenir posibles ataques a la esfera jurídica, que puedan provenir de la utilización de herramientas de comunicación y tratamiento de datos.

De tal forma que en la actualidad, el área de intimidad o "Privacy" ya no es simplemente de tratar de concebir facultades de exclusión de terceros, como sucede con la concepción tradicional de la intimidad aunque pueda considerarse que la persona proporciona voluntariamente la información esta concepción va más allá puesto que aun que efectivamente se proporciona la información y se convierte de índole publica cuando se habla de la intimidad es de la difusión de toda aquella información de índole personal que es transmitida en mensajes privados de tipo personal y que son enviados con consentimiento de la persona pero esto no quiere decir que autoriza al receptor de la información a hacerla pública posterior mente y

mucho menos al ente encargado de almacenarla lo faculta para que pueda hacer un mal uso de esta con esto nos referimos más bien a que se deben de crear "facultades de control" sobre los datos recogidos, almacenados y transmitidos en múltiples formas siendo ese el nuevo contenido del Derecho a la Intimidad. Surge así la noción de la "auto tutela informativa", que fue elevada al rango constitucional por el Tribunal Constitucional Federal Alemán, en su sentencia sobre la ley de Censos de 1983, "como garantía del ciudadano en las modernas sociedades frente al peligro del tratamiento electrónico de sus datos, consignando este derecho como la facultad de un ciudadano a decidir, quien, como, cuando y bajo qué circunstancias toma contacto con sus datos personales". Configurándose como un derecho fundamental de la tercera generación, que tiene un valor de solidaridad para la sociedad Alemana. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 194)

2.9 BIENES JURIDICOS PROTEGIDOS.

En relación con los bienes jurídicos tutelados, los delitos informáticos han sido clasificados tradicionalmente por la doctrina, en dos grandes grupos: los que se comenten contra el Honor, Intimidad como lo son la Violación a las Comunicaciones Privadas, Violación Agravada de Telecomunicaciones entre otros así también los relativos al orden socioeconómico como la Infidelidad Comercial y la Violación de Privilegios de Inversión existentes en el Titulo IX Capítulo I de los delitos relativos a la propiedad industrial en el cual se contempla la protección al software de computadora y otros programas que gozan de patente y privilegios de explotación resguardando una estrecha relación con lo regulado en la Ley de la Propiedad Intelectual. Sin embargo, también la fe pública puede verse afectada por tales acciones ya que por la cantidad de información que se proporciona a diversos sitios es vulnerable a que se den delitos como la falsedad material o la falsedad ideológica. Tal es el caso de la falsificación de los documentos electrónicos (públicos o privados), (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 192) pero sobre todo si se trata de documentos aunque para esto se debe alejar la concepción tradicionalmente unida a un soporte físico, como el papel o el cartón, encuentra

dificultades para ser aplicada a los discos magnéticos y ópticos en los que cada día con mayor intensidad, se almacenan los actos y negocios jurídicos. El documento como objeto corporal que refleja una realidad fáctica con trascendencia jurídica, no puede identificarse ni con el papel, como soporte, ni con la escritura, como unidad de significación es así que nos referimos a documentos en registros públicos de tipo electrónico sobre todo con la modernización de los Registros de la propiedad inmobiliaria, propiedad intelectual, propiedad de vehículos automotores y Registro de Comercio, mediante el acceso a los mismos por medios electrónicos y su alteración y falsificación, lesionando la fe pública. Por todo lo anterior, la acción delictiva cometida por medios informáticos presenta singularidades tan importantes que reclaman una tipificación singular y específica, resaltándose el continuo avance tecnológico que ofrece grandes dificultades para reconducir todas las modalidades comisivas a una formula típica cerrada.

Es necesario hacer referencia dentro de los bienes jurídicos que se deben proteger uno de los más importantes derechos como lo es el Derecho a la privacidad ya mencionado anterior mente como de origen anglosajón pero que su concepción más reciente dentro de la doctrina española en la actualidad puede decirse que no está acorde a las necesidades de un colectivo social Salvadoreño ya que este original mente hace referencia a la injerencia a un espacio físico por parte de un tercero pudiendo ser este inclusive el estado o a la interferencia dentro de las comunicaciones mas es necesario decir que no se está considerando dentro de este la información de tipo cibernética que como es conocido por todos en la actualidad es de gran importancia ya que en la "cibersociedad" en la que vivimos actualmente constantemente es un derecho el cual es violentado y que no existe una regulación que permita frenar estos delitos de tipo no convencionales.

Junto con esto surge la inquietud de considerar si ¿es una obligación pertenecer a una cibersociedad? y se debe analizar que aun que no es precisamente una obligación con los avances tecnológicos es una necesidad creciente en toda sociedad ya que las empresas en cargadas de la información y prestación de servicios están utilizando cada vez más este tipo de medios creando con estos la

necesidad de que la las personas quieran pertenecer estas redes sociales y por consiguiente a la "cibersociedad".

Es por ello que se debe dejar a atrás la concepción que el estado es quien más puede verse beneficiado con la utilización de la información de tipo personal con fines electorales ya que la información a la cual este puede solamente tener acceso es manejada por otras compañías y no por este como se cree, es así que el verdadero enfoque debería estar dirigido a la prevención del cometimiento de delitos por parte de personas inescrupulosas cuyo único fin es causar un daño a la intimidad y al honor de las personas y que no es necesario la intromisión física a un lugar físico determinado donde se puede considerar que deba haber privacidad puesto que como se mencionó anteriormente esto no es necesariamente indispensable ya que puede existir otros tipos de intromisión a la privacidad y que van encaminados a afectar el Honor y la Intimidad de las personas como por ejemplo: la Violación a las Comunicaciones Privadas o la Violación Agravada de las Telecomunicaciones (Anibal, 2002, págs. 79,80)

Por consiguiente se considera que como sociedad empecemos a exigir a nuestros legisladores mayores y rigurosas formas de control referente al mejo de la información proporcionada a redes sociales y al uso que terceras personas puedan darle pudiendo ser incluso el mismo receptor de la información quien con el afán de dañar la intimidad y la privacidad pueda llegar a realizar un mal uso de la misma, es así que es necesario ver ejemplos como la legislación Alemana donde existe por ley una "auto tutela informativa" la cual da todo el derecho a los ciudadanos de como cuando, donde y bajo qué circunstancias la información de estos puede ser divulgada. (Anibal, 2002, págs. 82,83)

2.9.1 Probables delitos contra la Intimidad cometidos mediante Medio Informático.

El derecho a la intimidad, o a la privacidad, está expresamente regulada en nuestra carta magna que es la Constitución de la Republica de El Salvador. En general, puede decirse que la privacidad de una persona se vincula directamente con

una razonable expectativa de intimidad de las proyecciones de nuestra personalidad, y que constituyen el ámbito nuclear donde la persona puede desarrollar su plan de vida. La intimidad así entendida no se limita únicamente a la persona, sino que alcanza muchas veces zonas compartidas como el núcleo familiar y el domicilio donde las personas pueden llevar adelante proyectos comunes.

De esta manera podemos aclarar que la intimidad forma parte de los derechos fundamentales de las personas por lo tanto este derecho se encuentra amparado en la Constitución de la Republica en el artículo 2 en donde expresa de forma clara, que garantiza el derecho a la intimidad personal; es así que ninguna persona puede vulnerar este derecho tan importante pero en la actualidad es decir en el diario vivir se está violentando de la forma menos esperada que es por medios informáticos haciendo uso de las diferentes redes sociales prevaleciéndose de que es una manera fácil de interferir en la intimidad de las personas.

Esta expectativa de privacidad se extiende también hacia ciertas relaciones profesionales como por ejemplo relación médico con paciente o abogado con cliente, etc.; y se conecta, en la actualidad, con el uso seguro de ciertos sistemas o medios de comunicación masivo. De esta manera, la relación de amistad que une a dos personas y que se ejercita tanto en el correo electrónico como en las redes sociales necesita un ámbito de privacidad y de exclusión a las terceras personas ajenas a esta relación. La privacidad, en sentido amplio, incluye no solo el ámbito privado de la persona en sí, sino también todas aquellas proyecciones de su personalidad y de sus relaciones con terceros que permitan realizar el plan de vida fijado por ellos mismos. (Gustavo Eduardo Aboso, Cibercriminalidad y Derecho Penal 2006, pág. 119)

Es decir la privacidad o la intimidad puede generalizarse cuando existe un vínculo de amistad, de amor o de familiaridad, pero esto no quiere decir que será vulnerado al contrario siempre se debe de respetar este derecho; en el caso de cuando la categoría amistad hace su función en las redes sociales podemos aclarar que siempre se respetara a la persona como tal cuidando de igual manera su imagen y la moral.

Nuestra legislación Constitucional ha establecido que los derechos a la privacidad e intimidad se extienden al ámbito de autonomía individual constituida por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física. (Gustavo Eduardo Aboso, Cibercriminalidad y Derecho Penal 2006, pág. 120)

Más allá del elemental espacio privado tutelado por el ordenamiento en general y el derecho penal en particular, cierto es que la nueva dimensión de la intimidad personal abarca un sinnúmero de contactos con terceros que merecen mayor resguardo jurídico, ya que la intimidad no debe ser entendida como una conducta o situación solipsista de la persona es decir que el ser humano piense que solo el existe, ya que desde tiempos inmemorables se subraya la naturaleza social de la persona y la necesidad de relacionarse con terceros. (Gustavo Eduardo Aboso, Cibercriminalidad y Derecho Penal 2006, pág. 124)

Por eso es necesario proteger de diferentes formas el derecho a la intimidad, es así que siempre es necesario que lo regule una legislación especial que proteja este derecho y que no exista ningún vacío de ley que pueda hacer prevalecer las personas que deseen dañar la privacidad o la imagen por medio de las redes sociales publicando ofensas, fotos de carácter sexual o mencionando comentarios alusivos a dañar la imagen de la otra persona es por ello que el derecho debe de estar siempre a la vanguardia de la tecnología para abarcar todos estos ámbitos especiales.

En la diversidad de evoluciones de las personas existe una zona de interacción con otros, en un espacio público en concreto, la cual puede caer dentro del ámbito de la vida privada. De esta manera se echan por tierra los argumentos que pretenden justificar la ausencia de lesión a la intimidad de la persona cuando ella mantiene una relación de amistad, divulgación de situaciones basadas en el afecto o en el sexo que son aptas para lesionar otro tipo de bienes o intereses.

Se mantiene la teoría que las personas que vulneran el derecho a la intimidad son aquellas en las cuales se mantiene una relación afectiva o de amistad por lo tanto existe un límite para no vulnerar este derecho pero por diferentes circunstancias o problemas que pueden surgir en un momento esto puede cambiar y

transformase en malos sentimientos surgiendo el odio, ira, celos, envidias, rencores etc., pueden estas personas dañar la intimidad y estos motivos no justifican la mala actuación que han realizado; actualmente se realizan por los medios informáticos subiendo a la red fotos íntimas, secretos que por su relación y por la confianza mantenían y que de esa manera se han hecho públicas dañando la moral y la imagen de la víctima.

Así por ejemplo, las situaciones de intimidad compartida, relaciones sexuales, no autorizan la revelación de secretos o su divulgación a merced de la experiencia compartida, ya que en estos casos también rige la tutela jurídica de la persona y su intimidad, que se encuentra afectada cuando dichas relaciones son expuestas al público. Con la simple divulgación ya sea por postear una foto de carácter sexual en internet específicamente en las redes sociales se está realizando un acto ilícito, en mucho de los casos se dan por problemas de carácter sentimental y que debido a la situación de intimidad que han compartido se prevalecen de esta situación para dañar la imagen de la persona dejando como consecuencia daños muy graves a la imagen y sobre todo a la moral de la víctima afectando su reputación como ser humano.

En relación con lo anteriormente expuesto se caracteriza por sostener que en los casos de intimidad compartida teniendo una relación amorosa, no existe vulneración del derecho a la intimidad por tanto una de las partes puede disponer libremente de ella y la otra está sujeta a esa decisión en la medida que acepta compartir su intimidad con la primera; es decir cuando existe voluntad de ambas partes de tener una imagen de carácter sexual de su pareja no cae en ningún ilícito. Este argumento puede ser erróneo, como también en casos referidos a la intimidad familiar, por cuanto lo que se comparte es una actividad personal desarrollada reservadamente, pero no propiamente la intimidad de otra; por eso parte del supuesto que esta corresponde exclusivamente a cada uno de los partícipes y no es susceptible de ser comparado porque es un derecho personalísimo. Se puede analizar de ese punto de vista teniendo los dos argumentos que si existe consentimiento se puede hacer sin acarrear un delito pero el otro argumento es que no se puede hacer ni de esa manera porque es un derecho personalísimo.

El avance tecnológico impone gradualmente la necesidad de ampliar la tutela jurídica de la intimidad personal cuando los medios técnicos permiten un mayor grado de vulnerabilidad de dicho ámbito privado. Esto se evidencia no solo uso de los medios telemáticos, sino también con la interceptación de mensajes, llamadas telefónicas, o el intrusismo informático que permite q terceros puedan acceder de manera ilícita a la esfera privada de una persona. (Gustavo Eduardo Aboso, Cibercriminalidad y Derecho Penal 2006, pág. 125)

Se puede analizar que la tecnología en las comunicaciones está avanzando de manera significativa por lo tanto el derecho debe ser cambiante en cuanto a regular conductas que no estén descritas en una ley secundaria es por ello que la posibilidad de vulnerar derechos fundamentales amparados por la Constitución es alto, entonces podemos concluir que debe de existir una ley especial compleja que cuide estos actos realizados por los diferentes medios informáticos. En cuanto a sus efectos, el consentidor debe tener capacidad para consentir; para esto no es menester contar con capacidad civil, sino con la capacidad de juicio y comprensión del hecho por parte del afectado, el autor debe estar en conocimiento del consentimiento y no pueden consentirse injerencias ajenas en el ámbito personal contrarias a las buenas costumbres. (Gustavo Eduardo Aboso, Cibercriminalidad y Derecho Penal 2006, págs. 131-132)

Cuando se refiere a la capacidad civil estamos en presencia de que la persona debe ser mayor de edad así como lo menciona la LEPINA en su artículo 3 en la definición de niño, niña y adolescente; es decir tener cumplidos los 18 años, pero este apartado menciona que solo es necesario tener la capacidad de juicio ósea saber lo que se está haciendo pero en este caso que se trata de actos de carácter sexual que dañan los derechos fundamentales de la persona y se puede consentir solo siendo mayor de edad. Respecto a la privacidad en la actualidad se han elaborado distintas teorías para poder explicar el grado de protección jurídica que se le acuerda al individuo en su esfera de intimidad. Por lo general se reconocen en el ámbito de la privacidad, diversos grados de tutela jurídica frente a las injerencias extrañas.

2.9.2 Delitos contra la Libertad Sexual cometidos mediante Medio Informático.

La concepción de libertad, en este caso la sexual implica necesariamente poseer la capacidad de actuar libremente, es decir, la capacidad de consentir o no intromisiones en el ámbito personal de la libertad sexual.

Excepto cuando por algún motivo la persona actora del ilícito que posee imágenes intimas del sujeto pasivo, quiere prevalecerse e intimidando con que esa imagen la subirá en las redes sociales y es de esta manera que incurre en un acto que daña derechos fundamentales amparados en la constitución de la república.

En la actualidad, los delitos cometidos a través de las redes sociales han cobrado auge de tal manera, que las instituciones tanto nacionales como internacionales deben interesarse, no solo en acaparar lo último en formación e información digital, sino en controlar y reformular legislaciones que combatan el uso abusivo de tales medios cibernéticos, que a la postre, asegurarían su disfrute y racional utilización. En esta vorágine globalizante, El Salvador, como todos los países que se embarcan en esta aventura mundial, no se queda atrás y soporta, con estoicismo, los inconvenientes legales para asimilarlo y regularlo.

En esta tarea, surgen los inconvenientes de adaptar la legislación actual con las distintas manifestaciones de la realidad virtual, que en la mayoría de los casos no es nada fácil, porque siempre la ciencia avanza más rápido que el derecho. (Apuntes de clase., 2013)

2.9.3 ¿Existen los "delitos informáticos" per se?

La naturaleza de los delitos informáticos depende del ambiente desde donde estos se cometen, así como tienen sus repercusiones. Quizás debido a una obsesión periodística en los inicios del boom de internet, existe una tendencia a considerar que los delitos informáticos como un nuevo tipo de delitos; así como se ha evidenciado el que los jueces han tenido el instrumental necesario y suficiente que ha hecho que los flagrantes actos criminales acabaran sin castigo.

La inmensa mayoría de los delitos informáticos que causan alarma social no son más que traslaciones de delitos "normales" o "comunes" a un nuevo medio: Así, existe una legislación clara que evita los actos de estafa, espionaje, violación de privacidad o injurias, ya sea fuera o dentro de la red. Lo cierto es que existían y aún existen vacíos legales por lo que no se haya tenido en cuenta que un determinado delito pueda cometerse también desde Internet, pero las figuras delictivas han existido aunque estén desfasadas o no tomen en cuenta esta nueva forma y objeto de comisión de delitos; por ello existe la necesidad social y jurídica de reformarlos y adecuarlos a las nuevas realidades que el ambiente informático han introducido.

Lo cierto es que no existen "delitos de la red" lo que hay son delitos de toda la vida, que también pueden practicarse desde nuevas tecnologías. Aunque en algunos casos no se trata de una "nueva" criminalidad sino de nuevas manifestaciones, ya que como dice MIDDENDORFF si bien el hombre es siempre el mismo, el desarrollo de la tecnología pone en nuestros días nuevos medios a disposición de la delincuencia con mayor perjuicio de la colectividad. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 211).

2.10 EL ORDENADOR COMO "MEDIO" DEL DELITO.

Al analizar el tema de la eventual introducción de nuevos tipos penales, se advierte que los equipos de proceso electrónicos de datos, son frecuentemente empleados como instrumento para la comisión de hechos punibles. De tal forma, que pueden ser utilizados como "medio" a efecto de lesionar el Derecho a la Intimidad o el patrimonio de otro (estafa, hurto, apropiación indebida, extorción, calumnia, fraudes informáticos), mediante el uso de tales herramientas informáticas, como el caso de los fraudes financieros de tipo informático o el espionaje de datos con la afectación de la propiedad intelectual, industrial o comercial. También como medio para la comisión del delito, a través de la informática puede lesionarse la fé pública, mediante la alteración de datos como la falsedad documental, medio por el cual se utilizaría para ocasionar perjuicios patrimoniales. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 197)

Por lo tanto se puede decir que el ordenador como objeto del delito u objeto material de la acción no debe confundirse con el instrumento del delito que son los objetos con que se cometió el delito, un cuchillo en un homicidio, una palanca en caso de robo de vivienda es así que el ordenador puede llegar convertirse en el medio para el cometimiento de los delitos informáticos y por consiguiente la lesión del Derecho a la Intimidad ya que en muchas ocasiones la exposición por medio de este de información de tipo intima es expuesta en las diferente redes sociales ya sea con la finalidad de exponer o la de realizar una amenaza entre otros.

2.10.1 Intervención de las Comunicaciones Electrónicas.

La entrada en un domicilio electrónico es una de las bases fundamentales para poder detectar un la realización de un Delito Informático, según nuestra fuente de información la Fiscalía General de la República, en la mayoría de los casos se realiza la inspección pericial al domicilio electrónico, se rastrea la Dirección IP (es una etiqueta numérica que identifica, de manera lógica y jerárquica, otorgados por el proveedor de internet a una interfaz (elemento de comunicación o conexión) de un dispositivo (habitualmente una computadora), en las primeras horas de investigación, debido a que es la única forma en la que se podrá obtener la evidencia, sin que esta pueda ser alterada por el Sujeto Activo, esto se realiza sin la necesidad de que exista una orden Judicial, pero si es necesario realizar la pericia de los archivo de un aparato electrónico especifico en el proceso se requiere de autorización Judicial, la cual debe ser solicitada por la Fiscalía General de la República ante el Juez de Paz que haya conocido del caso en primera instancia, mediante la acreditación de un perito idóneo para la realización de la misma. Dicho criterio va requerir una valoración desde el punto de vista constitucional sin que esto implique un entorpecimiento en cuanto a la integridad del material incautado o detectado.

Una forma muy práctica para mantener la integridad del material es bloquear cualquier puerto USB, disquetera en la que se pudiera dar la alteración de la información, la cual a su vez deberá ser dotada de fe judicial en cuanto al manejo y extracción de los datos, lo cual se puede realizar mediante la obtención de una copia

exacta del contenido del disco duro o cualquier otro dispositivo informático. (Eduardo La Valoracion de la Prueba Electronica, 2009, págs. 68,69)

2.10.2 Problemas respecto a la Tipicidad de tales Conductas ante el vacío Normativo.

Las relaciones entre la informática y delito, en la distintas formas lesivas como ha sido planteadas anteriormente, nos obliga a reflexionar si al acción delictiva cometida por medios informáticos presenta singularidades tan importantes que reclaman una tipificación singular y especifica. Por otra parte, el continuo avance tecnológico ofrece grandes dificultades para reconstruir todas las modalidades comisivas a una forma típica cerrada.

Dificulta por un lado, la lentitud de la respuesta estatal al respecto del problema, lo que genera dificultades para los operadores directos de tratar de aplicar los tipos penales tradicionales y verse con supuestos de atipicidad, obligando en muchos casos a utilizar la "analogía in malampartem", prohibida como consecuencia del principio de legalidad; pero por otro lado, una respuesta estatal que pretenda abarcar la mayor posibilidad de punibilidad de estas conductas, expandiendo el derecho penal aun a situaciones en que no se genera ningún resultado lesivo, convirtiéndose en delitos de mera actividad o delitos de peligro abstracto, adelantando las barreras de la punibilidad mediante la creación artificiosa de bienes jurídicos que carecen de contenido material y personal, así no la tipificación de conductas que o constituyen meros actos preparatorios o son simples resoluciones manifestadas, lesionando los principios de ese Derecho Penal mínimo que debe regir en un Estado constitucional y democrático de derecho.

Así que el primer punto a analizar ante esta problemática será la de analizar la situación de la política criminal actual, es decir, que medidas tomara el Estado o más bien, que medidas ha tomado y están tomando los Estados en lo que es ya la "cibersociedad". Respecto a la "autopista informática" y sobre las distintas posiciones que proponen su autoregulación de los cibernautas, así como sus incidencias en el plano de las relaciones de las personas con la democracia; pero sobre todo, con el

tratamiento que se ha dado a las figuras delictivas. Para ello se ha de analizar, a manera de derecho comparado, las figuras delictivas que han adoptado España y El Salvador, así como las que contienen los proyectos del Código Penal de Nicaragua y Costa Rica. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 206)

En nuestro país se ha tratado de encuadrar los delitos cibernéticos en figuras típicas como lo son la extorción, calumnia, robo o hurto fraudes sin embargo es necesario analizar en qué medida los medios informáticos van avanzado, así también si ha avanzado el uso que se hace de las computadoras, tablet o celulares de última generación donde cabe destacar que estos solamente son un medio para el cometimiento de delitos llevado a un uso indebido de estos dándose la necesidad de que estas sean reguladas por parte del derecho.

A pesar que muchos doctrinarios coinciden en una definición de lo que es el delito cibernético u informático en países como España (donde la definición está dada desde el punto de vista de un criminólogo y serían aquellas conductas que lesionan un bien jurídico protegido de nuestro ordenamiento, mediante el uso de un medio telemático para delinquir.), México (se entiende que "delitos informáticos" son todos aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático), Costa Rica (según Acurrio del Pino "delincuencia informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera") como se puede apreciar se han formulado conceptos funcionales con la finalidad de atender a realidades nacionales concretas. Es así que es necesario en nuestro país la creación de una definición de los que es el delito cibernético u informático para luego poder definirlo dentro de una norma como el acto mediante el cual ya sea una o varias personas comenten acciones ilícitas por medio del uso de computadoras personales, tablet o celulares así como cualquier otro dispositivo mediante el cual se pueda realizar la acción delictiva. En este orden de ideas es necesario dejar a un lado la creencia que se estaría violentado el derecho a la información, propiedad intelectual o derechos de autor debiendo prevalecer el

precepto Constitucional como lo es el Derecho a la Intimidad y la necesidad que existe que el Estado regule todo este tipo de situaciones ya sea cuando estas ya se hayan cometido o anticipándose ya que como se ha mencionado con anterioridad la complejidad de este tipo de conductas está dada por el constante avance tecnológico que existe día con día.

2.11 ARGUMENTOS A FAVOR DE LA REGULACIÓN.

Los partidarios de la regulación se apoyan en la tesis de que las redes de telecomunicaciones como Internet han generado un submundo en el que los delitos son difíciles de perseguir debido a la propia naturaleza del entorno y a la falta de tipificación de las modalidades de comisión y de los medios empleados. Ya desde el Seminario realizado por la Organización de Cooperación y Desarrollo Económico (OCDE), en junio de 1974, se proponía entre otras medidas, la "Creación de códigos de deontología profesional para el personal informático en los que se concreten deberes de discreción. Diligencia y fidelidad en ese sector. Junto a ellos es preciso dotar a los sistemas informáticos de medidas técnicas de seguridad adecuadas"; de igual forma, en el Octavo Congreso de las Naciones Unidas sobre la prevención del delito y tratamiento del delincuente, celebrado en la Habana, del 27 de agosto al 7 de septiembre de 1990, en la Resolución 9. Delitos relacionados con la informática, como Medida 2.e de dicha resolución, se propone: "La elaboración, en colaboración con las organizaciones interesadas, de un reglamento deontológico (manual que recopila las obligaciones morales que tiene que respetar aquellos que ejercen un trabajo, es decir: hacer o evitar según lo que le dicte su conciencia) sobre el empleo de la informática y la inclusión de este reglamento en el programa de estudio de información en la esfera informática". (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 208)

2.11.1 Argumentos en contra de la Regulación.

Frente a la corriente reguladora se levantan los partidarios de que ciertas áreas queden libres del intervencionismo o proteccionismo estatal. Entre los argumentos

más solicitados figuran el derecho a la intimidad, la libertad de expresión y la libertad de acceso a la información. (Muñoz Campos, Diciembre 2002 / Año V-VOL. IV, pág. 209).

La verdad referente al tema es que constantemente nos damos cuenta de la gran necesidad que existe de regular este tipo de conductas lesivas puesto que es a diario que se realizan actos que son directamente atentatorios contra el Derecho a la Intimidad que tienen las personas y en lugar de enfrascarse si la posibilidad de la aprobación de una futura ley la cual regule todo este tipo de acciones es atentatoria o mordaza como se le pretende denominar es necesario debatir sobre los alcances de la misma en aspectos como el alcance del denominado sujeto activo ¿Que sucede si el que comete dicha conducta es un funcionario público o una persona con conocimiento técnico o especializado en el área de la computación? y consecuente uso de estos dispositivos o si el computador o dispositivo electrónico sea de cualquier tipo es un medio o un objeto para el cometimiento del mismo. Cabe señalar que, a nivel mundial, muchos países cuentan con legislación en materia de delitos informáticos, algunos incluso desde hace ya más de una década. A título ejemplificativo podemos mencionar los siguientes: Alemania (1986), USA (1986 y 1994), Austria (1987), Francia (1988), Inglaterra (1990), Italia (1993), Holanda (1993), España (1995) y el Consejo de Europa (Convención sobre el Cybercrimen de 2001).

También en Latinoamérica varios países han legislado este tipo de delitos, entre otros: Chile (Ley 19.223 de 1993), Bolivia (Ley 1.768 de 1997), Paraguay (reforma al CP en 1997), Perú (reforma al CP en 2000), Colombia (Ley 679 de 2001 sobre pornografía infantil en redes globales), Costa Rica (Leyes 8.131 y 8.148 de 2001), Venezuela (Ley Especial de 2001) y México (Código Penal Federal). Nuestro país no debe ser la excepción en este tema y hacer a un lado discusiones de quienes están a favor y quienes en contra puesto que a todas luces la regulación es necesaria.

2.12 MARCO JURIDICO.

2.12.1 Leyes Nacionales.

2.12.1.1 La Constitución de la Republica de El Salvador.

Nuestro trabajo de investigación se desarrollara amparándose en los derechos fundamentales que protege nuestra carta magna, debido a que es nuestra Ley Primaria que data del 16 de Diciembre de 1983, con la Reforma 24, Decreto Legislativo No. 36 de fecha 27 de mayo de 2009, publicado en el Diario Oficial No. 102, Tomo 383 de fecha 04 de junio de 2009, se desarrollara el estudio de las conductas lesivas a las personas que dañan derechos humanos fundamentales que están regulados y contenidos en la normativa constitucional.

En su Artículo 1 que se expresa de manera clara y precisa los derechos que se les atribuyen a las personas siendo esos inalienables e inherentes a cada ser humano expresándose así, "El Salvador reconoce a la persona humana como el origen y el fin de la actividad del Estado, que está organizado para la consecución de la justicia, de la seguridad jurídica y del bien común." Lo importante a destacar del inciso anterior es que menciona lo valores jurídicos fundamentales los cuales son la justicia entendida como una regla de igualdad proporcional entre personas así como también de armonía entre individuos; el segundo valor jurídico es seguridad jurídica lo cual es un criterio que se relaciona con un aspecto sociológico, entendida como la realización plena del orden jurídico positivo apropiado para la estructura de la comunidad que rige y su aplicabilidad debe de basarse en los ordenamientos jurídicos que exija el sistema es decir que el Derecho debe de actualizarse para normar las formas innovadoras que vulneren derechos fundamentales. El bien común es una de las finalidades a las cuales tiene el Derecho, entendiendo el objeto del derecho como la regulación de la actividad individual que permite la vida en sociedad, es decir que el hombre actúa en su ámbito de colectividad tomando en cuenta factores que determinan el campo ilícito de la acción personal lo cual no puede haber sistema jurídico que su objeto quiera alcanzar un fin individual.

Dejando claro que el deber del Estado es de garantizar cada uno de los derechos fundamentales expresándose a través de su carta magna de la siguiente manera; "En consecuencia, es obligación del Estado asegurar a los habitantes de la República, el goce de la libertad, la salud, la cultura, el bienestar económico y la justicia social." Siendo los anteriores derechos los que el estado debe de proteger y garantizarlos a cada persona para una vida digna entre habitantes por eso es obligación del estado actualizar los mecanismos de control social, la legislación secundaria, las instituciones que aplican el derecho y toda actividad que resguarde los derechos fundamentales de la persona humana debido a que han aparecido delitos no convencionales cometidos por medio de redes sociales.

De manera que bajo el fundamento constitucional que menciona en su Artículo 2 "Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y hacer protegida en la conservación y defensa de los mismos. Se garantiza el derecho al honor, a la intimidad personal y familiar, a la propia imagen. Se establece la indemnización, conforme a la ley, por daños de carácter moral", es así como basamos nuestro trabajo de investigación en estos últimos derechos, por ende será nuestro enfoque a investigar debido a que es el derecho a la intimidad en el que podemos referirnos que está siendo vulnerado de formas no convencionales, debido a la evolución que la tecnología va desarrollando en El Salvador por eso es importante citar el articulado en donde prevalecen las garantías que toda persona posee.

En consecuencia refiriéndonos a la vulneración del derecho al honor que afecta también de manera directa la dignidad de la persona, la propia imagen, la reputación; se tratan de derechos vinculados a la propia personalidad por estar relacionado con la dignidad e intimidad y estos derechos deben ser considerados de manera irrenunciable y esto implica la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás; es decir se tratan de derechos que pertenecen al ámbito de la vida privada.

De esta forma el Articulo 6 "Toda persona puede expresar y difundir libremente sus pensamientos siempre que no subvierta el orden público, ni lesione la moral, el honor, ni la vida privada de los demás. El ejercicio de este derecho no estará sujeto a

previo examen, censura ni caución; pero los que haciendo uso de él infrinjan las leyes, responderán por el delito que cometan". En el inciso primero se refiere a que las personas tienen el derecho de expresar sus pensamientos pero no tiene que dañar la moral ni la intimidad de otras personas, en relación a nuestro tema de investigación este artículo de la Constitución es una de las bases fundamentales para que el Estado pueda ampararse en desarrollar una Ley Especial que regule los actos que dañen o vulneren los derechos que están amparados en nuestra Ley Primaria, debido a eso es necesario proteger los derechos de las personas ante estos delitos no convencionales que se están desarrollando por las diferentes redes sociales y que por no tener una normativa que regule directamente las conductas que se manifiestan por el facebook, twitter; que su objetivo es de dañar la moral, la dignidad de la persona, la propia imagen y la intimidad.

Por lo tanto nuestro trabajo como equipo de investigación se basara en desarrollar la problemática que aqueja nuestro país específicamente en el departamento de Santa Ana tomando como base los artículos antes mencionados que son los que contienen los derechos fundamentales protegidos que más se vulneran por los delitos no convencionales es decir por aquellas conductas lesivas a las personas humanas que se cometen por medio de las redes sociales.

2.12.2 Leyes Secundarias.

2.12.2.1 Código Penal.

Dentro del Título VI del Código Penal Salvadoreño nos encontramos con los DELITOS RELATIVOS AL HONOR Y LA INTIMIDAD previstos y sancionados en el Capítulo I y más específicamente los que se refieren a la Calumnia y La Injuria ya que en la actualidad en lo delitos referentes al honor y la intimidad nos encontramos ante nuevos escenarios para que puedan cometerse este tipo de delitos siendo estas las Redes Sociales es de mencionar la enorme capacidad de estas de causar un mayor daño a la persona ya que el efecto es instantáneo, viral y con mucha más capacidad de causar daño que otros medios, es así que debemos hacer un análisis de estos delitos cometidos a través de estos medios.

CALUMNIA

Art. 177 C. Pn.- El que atribuyere falsamente a una persona la comisión de un delito o participación en el mismo, será sancionado con prisión de uno a tres años. La calumnia realizada con publicidad será sancionada con prisión de dos a cuatro años. Las calumnias reiteradas contra una misma persona serán sancionadas con prisión de dos a cuatro años y multa de cincuenta a cien días multa. Si las calumnias reiteradas se realizaren con publicidad, la sanción será de dos a cuatro años y multa de cien a doscientos días multa. Si las calumnias reiteradas se realizaren con publicidad, la sanción será de dos a cuatro años y multa de cien a doscientos días multa.

La creciente demanda que tienen estos medios en la actualidad hace cada vez más necesario la necesidad que se promulgue una ley de carácter especial donde se contemple este tipo de delitos cometidos por medio de dispositivos electrónicos y a través de las Redes Sociales y más en concreto en lo que se refiere a la Calumnia puesto que la mayor parte de personas que comete en la actualidad este tipo de delitos en nuestro país realizan esta acción sin que pueda hacerse algo al respecto debido a la falta de una adecuada legislación en lo relativo al problema investigado ya que aunque el delito está tipificado en el artículo 177 del Código Penal Salvadoreño este no hace alusión a cuando la acción de imputar Delitos no cometidos a una persona a través de las Redes Sociales tiene una clara finalidad la cual es dañar intencionalmente la imagen de otros hace que cada vez este tipo de situaciones se dé con mayor regularidad sin que se pueda hacer algo al respecto.

DIFAMACIÓN

Art. 178 C. Pn.- El que atribuyere a una persona que no esté presente una conducta o calidad capaz de dañar su dignidad, menoscabando su fama o atentando contra su propia estimación, será sancionado con prisión de seis meses a dos años. La difamación realizada con publicidad será sancionada con prisión de uno a tres años. La difamación reiterada contra una misma persona será sancionada con prisión de uno a tres años y multa de cincuenta a cien días multa.

Por su parte la Difamación es otro de los delitos que día con día en la actualidad se da a través de las Redes Sociales según la Real Academia de la Lengua Española Difamar es: desacreditar a alguien, de palabra o por escrito publicando algo contra su buena opinión y fama. Siendo así que la difamación es un delito que debe ser perseguido sea dentro o fuera de la red la única diferencia entre estos dos aspectos es la capacidad de difusión que tiene las Redes Sociales mientras que fuera de la red la repercusión de una demanda por difamación por un tema determinado suele tenerse un recorrido limitado es debido a esto que es necesario para proteger a las personas que se ven afectadas por este tipo de situaciones se cree la normativa indicada para que cuando se den casos grabes poder actuar e identificar al autor que, aun que pudiera llegar a ser complejo no debería ser imposible con la ayuda de la normativa indicada.

INJURIA

Art. 179 C. Pn.- El que ofendiese de palabra o mediante acción la dignidad o el decoro de una persona presente, será sancionado con prisión de seis meses a dos años. La injuria realizada con publicidad será sancionada con prisión de uno a tres años y multa de cincuenta a cien días multa. Las injurias reiteradas contra una misma persona serán sancionadas con prisión de uno a tres años y multa de cincuenta a cien días multa. Si las injurias reiteradas se realizaren con publicidad, la sanción será de uno a tres años de prisión y multa de cien a doscientos días multa.

Cuando el artículo hace alusión a ofender ya sea de palabra o acción indican una relación de acciones dirigidas a lesionar el honor de una persona entendiéndose por esto que el Honor no es más que el derecho que toda persona natural tiene a que se le respete según las cualidades propias de esta, y supone una lesión que se realiza a través de una expresión o acción y que lo que pretende es dañar la dignidad de una persona perjudicando su reputación por medio de la imputación de un hecho o una cualidad en menoscabo de su fama y de su auto estima es así que a través de las Redes Sociales puede llegar a cometerse este tipo de delitos y es a través de los dispositivos electrónicos y por medio de las denominadas "redes" es que hoy en día se está dando este tipo de delitos sin que exista si quiera la forma de sancionar esta

actividad haciendo necesario ya sea la promulgación o la modificación de las leyes existentes donde se controle y sancione el cometimiento de estos delitos cometidos a través de las Redes Sociales.

En El Salvador el Código Penal en su libro II se regulan algunas figuras delictivas de las cuales se han utilizado en relación con los delitos informáticos las cuales como se puede apreciar ya no son las mejores figuras puesto que no se hace referencia concreta a las muchas formas que puede existir del sujeto activo, debido a el anonimato que ofrece Internet y la posibilidad de ejecución de conductas dañosas a distancia dificultan la detección de los posibles delitos. Tampoco es fácil delimitar quien es el autor de dichas conductas. Por eso para investigar una comunicación delictiva realizada a través de Internet lo que hay que determinar principalmente son los datos de tráfico y los rastros de navegación, ya que aportan información fundamental sobre el origen de una comunicación y las idas y venidas de la misma entre los distintos dispositivos a través de la red. La mayoría de veces se vuelve todo un dolor de cabeza la localización de los datos de tráfico y si son encontrados el descifrar estos datos es casi imposible, ya que las aplicaciones o dispositivos utilizados tienen una programación en un lenguaje de programación que solo el fabricante y algunos especialistas pueden entender, así como también consideramos la falta de capacidad en el poder punitivo de estas normas puesto que las sanciones van desde multas hasta días cárcel. A continuación se presenta el articulado el cual hace referencia no solo a los delitos informáticos sino que también a los Delitos Relativos al Honor y la Intimidad.

DE LOS DELITOS RELATIVOS A LA INTIMIDAD.

VIOLACIÓN DE COMUNICACIONES PRIVADAS.

Art. 184 C. Pn.- El que con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido o se apodere de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivo o registro público o privado,

será sancionado con multa de cincuenta a cien días multa. Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de cien a doscientos días multa. El tercero a quien se revelare el secreto y lo divulgare a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa.

Existen elementos necesarios para poder identificar la comisión de un hecho delictivo a través de Internet los cuales son: **Conocer la dirección IP, identificar el ordenador y su ubicación y el contrato de acceso.** Cabe aclarar que conocer estos elementos por sí solo y sin la ayuda de una investigación minuciosa por parte de las autoridades puede que no se ayuden a esclarecer los delitos cometidos a través de internet.

VIOLACIÓN AGRAVADA DE COMUNICACIONES.

Art. 185 C. Pn.- Si los hechos descritos en el artículo anterior se realizaren por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros, se impondrá, además de la pena de multa, inhabilitación del respectivo cargo o empleo público de seis meses a dos años.

Como se puede apreciar en el inciso primero del artículo se habla de apoderamiento de soportes informáticos con la finalidad de vulnerar la intimidad de una o varias personas la finalidad del apoderamiento es causar daño todo esto a través de una forma ilegal teniendo el sujeto activo todo el conocimiento de causar ese daño y por consiguiente dicha conducta se pueda tachar de reprochable con lo cual se debería agravar su situación jurídica así también en el art.185 nos hace ver que se hace una referencia clara al sujeto activo el cual puede ser cualquier persona lo cual puede decirse que a nuestro criterio se debería ser más específico ya que si bien puede ser cometido por cualquier persona sabemos que hay individuos cuya calidad en el cometimiento de un delito es de carácter "especial" por el cargo el cual se desempeña pudiendo ser funcionario público a parte de una persona con una conocimiento especializado en la materia informática y que con mayor razón a esto es que se debería hacer referencia en una ley especial y por consiguiente tener una

sanción acorde a las necesidades actuales profundizando más allá de la inhabilitación del ejercicio o cargo que se ostente. Por consiguiente en el inciso segundo del art.184 hace una clara referencia a la difusión de datos mas no hace mención a los medios por lo que ahora se puede difundirse la información como lo son redes sociales las cuales en el presente trabajo se han mencionado con anterioridad y que como es conocido por todos con el avance de la tecnología estos medios pueden ser muy variados siendo necesario por consiguiente que de una buena medida se trate de llenar este posible vacío legal así como también un cambio en la sanción por la realización de estas conductas ya que como se es conocido se puede llegar a causar una grave afectación a la persona no siendo considerada a nuestro criterio una sanción acorde al grado de afectación que es producida por la acción y se puede establecer que el medio de cometimiento fue internet debido a la tecnología y a la prueba electrónica.

Es necesario establecer lo que de aquí en adelante consideraremos bajo el concepto de Prueba Electrónica es la que nos permite acreditar hechos a través de los medios tecnológicos de reproducción de las palabras, de sonidos e imágenes así como también aquellos instrumentos que nos permiten archivar o reproducir datos relevantes en un determinado proceso, esta prueba tiene la característica peculiar que debe de ser expresada a través de un instrumento tecnológico, es decir que cualquier tipo de prueba electrónica tiene una parte material que será identificada como un "Hardware" (Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático) y una parte que será su mecanismo de existencia llamado "Software" (Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas), la naturaleza de esta prueba si es una prueba documental, de documentos especiales o es una prueba de reconocimiento Judicial. Existe doctrinas como lo es la Alemana sustentan sus teorías en base al libro La Valoración de la Prueba Electrónica de Eduardo de Urbano Castillo este establece que la prueba electrónica solo puede ser admitida como objeto del reconocimiento judicial, y por su parte los países de origen Latino Americanos creen que es mejor aplicarle un método análogo de valoración, la discrepancia radica en la presentación y la valoración de la prueba, debido a que este tipo de prueba tan

peculiar debe ser presentada a través de medios electrónicos, pero a la hora de realizarle su examen debe realizarse a través de papel, la imagen o algún medio de almacenamiento podemos entonces distinguir en relación con los medios de prueba que: la prueba configurada sobre un documento electrónico no es una excepción al sistema general valorativo y probatorio, es decir se mantiene taxativo el hecho que debe existir una conexión lógica entre la prueba y el hecho probablemente, concluyendo con esto que es necesario que se dé el vínculo entre racionalidad y sentido común.

CAPTACIÓN DE COMUNICACIONES.

Art. 186 C. Pn.- El que con el fin de vulnerar la intimidad de otro, interceptare, impidiere o interrumpiere una comunicación telegráfica o telefónica o utilizare instrumentos o artificios técnicos de escucha, transmisión o grabación del sonido, la imagen o de cualquier otra señal de comunicación, será sancionado con prisión de seis meses a un año y multa de cincuenta a cien días multa.

Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de prisión de seis meses a un año y multa de cien a ciento cincuenta días multa.

El tercero a quien se revelare el secreto y lo divulgare, a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa. El que realizare los actos señalados en el primer inciso del presente artículo para preparar la comisión de un delito grave será sancionado con la pena de dos a seis años.

Por lo que se puede apreciar en el artículo en su inciso primero en los verbos interceptar, impedir o interrumpir estos son en referencia de comunicaciones telegráficas o telefónicas dejando muy por fuera los medios informáticos dándose un vacío legal habiendo la necesidad de estar estos incluidos en una ley especial que abarque tanto las comunicaciones telegrafías y telefónicas pero como un complemento de los medios informáticos. Es así que en los dos incisos siguientes se hace mención a la divulgación o revelación de los datos a los cuales se hace referencia en el inciso primero más es necesario mencionar que la sanción tanto de

días multas como la pena de prisión la cual puede ser sustituida por medidas cautelares tales como trabajos de utilidad pública parecen ser inadecuados y como ya se mencionó con anterioridad insuficientes ante el grabe nivel de afectación el cual se puede llegar a causar el sujeto que cometa las conductas anteriormente mencionadas. Y aunque en el inciso cuarto del mismo se hace mención a la pena que va desde los dos a los seis años de prisión esta solamente se considerara en los casos en los cuales las conductas descritas en el inciso primero sean con el fin de preparar el cometimiento un delito del cual no se hace ninguna especificación y pareciera que se deja a criterio y valoración del juez dándose con esto a nuestra consideración como grupo de investigación un vacío legal el cual pudiera suplirse con la creación de una ley especial.

UTILIZACIÓN DE LA IMAGEN O NOMBRE DE OTRO.

Art. 190 C. Pn.- El que utilizare por cualquier medio la imagen o nombre de otra persona, sin su consentimiento, con fines periodísticos, artísticos, comerciales o publicitarios, será sancionado con multa de treinta a cien días multa.

En este artículo se hace mención a la imagen o nombre de la persona sin su consentimiento más se hace mención al bien jurídico el cual es el derecho a la propia imagen que tiene cada persona pero orientado el articulado a fines meramente periodísticos aunque no hay duda que hay una violación al derecho a la intimidad y al honor es necesario decir que se deja por fuera la difusión de la imágenes u otro tipo de datos por medio de las redes sociales y aunque en la redes existen medios de información como periódicos digitales nuestra critica va encaminada a la difusión de imágenes pornográficas que atenten contra la intimidad de la persona a la cual sin su posible consentimiento han sido sustraídas y posteriormente difundidas en estos medios. Una vez más es necesario hacer mención a la sanción de días multas las cuales debería ser cambiadas a penas de prisión que vayan desde los tres años en adelante.

Es necesario hacer un apartado especial para una serie de delitos que también pueden llevarse a cabo por medio del internet y a través de las redes sociales como

lo son Delitos relativos a la Autonomía Personal como lo es las Amenazas del artículo 154, de los Relativos al Patrimonio como lo es la Extorción del articulo 214 derogado por D.L.Nº 954 dando paso con esto a la Ley Especial contra el Delito de Extorción y Delitos Relativos al Orden Socioeconómico en lo referente a la Violación de Privilegios de Invención del articulo 228 y por consiguiente atentado contra la Ley de la Propiedad Intelectual.

2.12.2.2 Ley Especial Nacional.

2.12.2.3 Ley Especial Integral para una Vida Libre de Violencia para las Mujeres. (LEIV)

Legislación basada en materia de familia y que surge por la necesidad de proteger la integridad física, mental y moral de las mujeres, siendo el objetivo primordial de existencia de la misma la vulneración constante y la falta de tutela de los bienes jurídicos constitucionales protegidos por las leyes ya existentes en materia de violencia contra la mujer.

Como equipo de investigación utilizamos este cuerpo normativo debido a que encontramos regulada la protección de los derechos de las mujeres buscando como objetivo principal garantizarles una vida libre de violencia. En nuestra investigación nos centraremos en analizar aquel articulado que describa tutele e imponga sanciones a las conductas que atenten contra la integridad de las mujeres y cuyo medio de cometimiento y difusión sean los medios electrónicos debido a que es esta la legislación utilizada por la Fiscalía General de la República en la actualidad por la inexistencia de una legislación que regule conductas lesivas cometidas utilizando como medio de cometimiento el internet buscando con esto estudiar si dicha legislación cumple con las necesidades de regular las conductas lesivas cometidas utilizando un medio tecnológico o las redes sociales.

Artículo 1 LEIV.- "La presente ley tiene por objeto establecer, reconocer y garantizar el derecho de las mujeres a una vida libre de violencia, por medio de Políticas Públicas orientadas a la detección, prevención, atención, protección,

reparación y sanción de la violencia contra las mujeres; a fin de proteger su derecho a la vida, la integridad física y moral, la libertad, la no discriminación, la dignidad, la tutela efectiva, la seguridad personal, la igualdad real y la equidad".

La presente Ley tiene la característica de ser un cuerpo normativo Especial el cual busca tutelar todas aquellas conductas que atenten contra la seguridad Jurídica de las mujeres; si nos basamos en el Art. 1 de nuestra constitución se establece que el Estado estará organizado para la consecución de tres valores intrínsecos en cada ser humano los cuales son: Justicia, Seguridad Jurídica y Bien Común, valores que son tutelados mediante la imposición de sanciones por acciones que estén previamente descritas en los tipos penales que la presente ley desarrolla, actos que sean antijurídicos culpables ,este cuerpo normativo cuenta con la característica especial de cumplir una función en la protección únicamente de la mujer.

Es importante resaltar que en nuestra investigación las mujeres juegan un papel fundamental como sujetos pasivos de todas las conductas lesivas realizadas a través de las redes sociales, ya que según datos estadísticos de la Fiscalía General de la República el 95 % de los casos judicializados en nuestro país la víctimas han resultado ser mujeres, es de aquí de donde surge la necesidad de la creación de un cuerpo normativo especial que vayan en función de proteger y garantizar los Derechos de las mujeres.

Artículo 3 LEIV.- Ámbito de Aplicación. "La presente ley se aplicará en beneficio de las mujeres que se encuentren en el territorio nacional, sean éstas nacionales o no, o que teniendo la calidad de salvadoreñas, estén fuera del territorio nacional, siempre que las acciones u omisiones de que trata la presente ley puedan ser perseguidas con base en parámetros de extraterritorialidad".

Este articulo va en caminado a la tutela de los Derechos establecido en la presente ley, como característica principal del principio de impenetrabilidad del Territorio en relación a la aplicabilidad de su propio ordenamiento jurídico, es decir que la aplicación de la presente ley será para todas la mujeres que estén en el territorio nacional, no importando su nacionalidad ya que obedeciendo al Art. 96 De nuestra constitución en el cual se establece que "… Los extranjeros desde el

instante en que llegara al territorio de la República estarán estrictamente obligados a respetar a las autoridades y a obedecer las leyes y adquirirán derecho a ser protegidos por ellas" el ámbito de aplicación es todo el territorio Nacional, así mismo el articulo hace la salvedad que puede ser aplicado a mujeres que este fuera del territorio pero que tengan la calidad de Salvadoreñas y según el Art 90 de La Constitución de la República esta calidad la ostenta "… Los Nacidos en el territorio de El Salvador, los hijos de madre o padre Salvadoreños nacidos en el extranjero", tomando en cuenta los parámetros te extraterritorialidad en el momento de ocurrida la conducta que ponga en peligro la integridad y seguridad de las mujeres.

Artículo 6 LEIV.- Sujetos Obligados. "Son sujetos obligados para efectos de esta ley, toda persona natural o jurídica, que se encuentre o actúe en territorio salvadoreño, quienes deberán cumplir y hacer cumplir las disposiciones de esta ley, cualquiera que fuese su nacionalidad, domicilio o residencia".

Así mismo este artículo va en caminado a establecer los límites para la aplicación de esta ley para garantizar la libertad física y moral, la seguridad, el trabajo, la posesión, y la protección de los mismo de todas las mujeres que se encuentren en el territorio Nacional a la hora de que exista una conducta que pueda ser típica y antijurídica por la cual se pueda otorgar una sanción a quien realice este tipo de conductas.

Artículo 50 LEIV.- Difusión Ilegal de Información. "Quien publicare, compartiere, enviare o distribuyere información personal que dañe el honor, la intimidad personal y familiar, y la propia imagen de la mujer sin su consentimiento, será sancionado con pena de uno a tres años de prisión".

Este tipo penal describe cuatro acciones que pueden ser cometidas por las personas y menoscabar la integridad, la intimidad y la seguridad de una mujer; al observar nuestro objeto de estudio la aplicación de este tipo penal sería importante debido a que las acciones descritas son exactamente las que se están realizando ahora en día mediante la utilización de las redes sociales, medio que facilita el acceso la información personal nivel mundial de los usuarios de la misma, ahí es

donde radica la problemática que estudiamos, debido a que el medio es difuso porque ahora en día las redes sociales están al alcance de la mayoría de las personas y con el hecho de compartir un contenido puede ser conocido a nivel mundial. Observamos que la penalidad para las conductas arriba descritas es con prisión de uno a tres años, al realizar una comparación de este tipo penal en relación al Capítulo II "de los delitos relativos a la intimidad" del código penal, observamos la diferencia que existe en las penalidades ya que el Código Penal establece días multa, y la presente Ley la penalidad es con prisión; lo que observamos que la tutela de los Derechos establecida en el Código Penal no evita que estos derechos sigan siendo vulnerados y de esa necesidad de castigar las conductas lesivas de una forma más severa es que surge esta ley especial integral para una vida libre de violencia para las mujeres, la cual al observar lo establecido en el código penal evidenciando la necesidad de que exista un cuerpo Normativo que tutele de forma diferente el cometimiento de las mismas conductas, pero que cuyo medio no es el mismo, es ahí donde radica la diferencia de la pena, ya que es en esta ley hablamos del medio de cometimiento a través de aparatos electrónicos como lo son Computadoras, Smartphone, Ipad en alianza con el internet especialmente las redes sociales como el Facebook, el Twitter e Instagram, es por eso que si el medio no es el mismo, la penalidad no puede ser la misma; aunque como grupo de trabajo de investigación observamos que es necesario que exista la aprobación de una Ley Especial que tutele exclusivamente los delitos cometidos a través de medios electrónicos y mediante la utilización de las redes Sociales, ya que en nuestro país solamente existe el "anteproyecto de ley especial contra delitos informáticos y conexos" pero que aún no ha sido aprobado.

Artículo 55 LEIV.- Expresiones de violencia contra las mujeres. "Quien realizare cualquiera de las siguientes conductas, será sancionado con multa de dos a veinticinco salarios mínimos del comercio y servicio: Elaborar, publicar, difundir o transmitir por cualquier medio, imágenes o mensajes visuales, audiovisuales, multimedia o plataformas informáticas con contenido de odio o menosprecio hacia las mujeres".

Este articulo al igual que los Arts. 50 y 55 los hemos relacionados con nuestro objeto de estudio por que si bien es cierto este cuerpo normativo especial es aplicable únicamente al sexo femenino describe conductas que atentan contra la integridad e intimidad y cuyo medio de cometimiento son los medio tecnológicos informáticos, y según las fuentes consultadas con anticipación a nuestra investigación el 90% de las víctimas de este tipo de delitos que se cometen a través de la cibersociedad son mujeres.

Después de analizar el articulado es necesario no dejar de lado que el elemento más importante en cuanto a los tipos penales descritos en la Legislación radica en un solo hecho del que puede emanar la tipificación del mismo y es la actividad probatoria el mayor problema al puntualizar la valoración de la prueba a nivel electrónico radica en la inexistencia de una Normativa Universal de control que obligue a la obtención de ciertos criterios generales en los diversos Ordenamientos Jurídicos, partiendo así que existen mecanismos Analógicos sobre la prueba y otros países que han desarrollado el sistema de presentación y evaluación de la prueba volviéndolo así un sistema subjetivo sin perder en ningún momento de vista que es el Juez el que en estos sistemas el que debe adaptarse a la innovaciones tecnológicas respetando siempre las garantías constitucionales del debido proceso.

Los titulares de los Órganos Judiciales toman un rol importante en cuanto al conocimiento y la valoración de la prueba cuando se plantean tipos penales que pueden ser cometidos a través de un medio diferente como lo es el internet y las redes sociales como facebook, twitter, se vuelve necesario que las autoridades encargadas de aplicar la justicia en nuestro Estado estén capacitadas para la valoración de este elemento tan trascendental como lo es la prueba; si hablamos de Ciberdelitos. tendríamos que hablar de un medio probatorio diferente y no tan convencional ya que según nuestra fuente de información, como lo es la Fiscalía General de la República, el perito que se debe de encargar de la obtención de la prueba en estos casos debe llenar ciertos requisitos y recoger características especiales como ser un especialista en informática forense, debido a que la extracción de datos, no la puede realizar cualquier persona, sino únicamente un Perito Informático con amplio conocimiento en Pericia Informática es fundamental

porque de ahí depende la actividad probatoria del proceso estaríamos refiriendo a una prueba electrónica un medio idóneo de probar el cometimiento de una acción que ponga en peligros o vulnere la integridad de una persona es por esto que la prueba electrónica resulta difícil tener un conocimiento amplio en cuanto a la obtención, transformación de la información digital y convertirla a un medio donde pueda ser percibida y entendida sin ningún grado de dificultad, es por ello que se convierte en algo casi obligatorio el auxiliarse de una persona tenga un grado de conocimiento superior en cuanto a la pericia informática resulta indispensable es aquí donde surge la idoneidad en el sujeto que realiza la extracción y presentación de la prueba.

2.12.2.4 Países Centroamericanos que cuentan con Leyes contra la Ciberdelincuencia.

Hay que mencionar que a nivel Centroamericano hay países que cuentan con regulación ya sea especial contra la ciberdelincuencia como es conocida es así que nuestro país tiene un claro ejemplo en otras naciones del istmo centroamericano para dar el siguiente paso en lo referente a este tipo de delitos a continuación se presenta un los países centroamericanos que cuentan con legislación ya sea especial o inmersa en sus respectivos códigos penales:

Panamá: Código Penal y sus reformas; Ley 51 (2008) No se ha encontrado legislación especial en la materia. No obstante, posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos pueden citarse los artículos 162 a 165, 180, 184, 185, 220, 237, 260, 283 a 286 y 421. Adicionalmente posee la Ley 51/2008 de Firma Electrónica, en la cual se regula penalmente sobre la falsificación de documentos.

Costa Rica: Ley 9.048 (2012) La Ley 9048 es una modificación importante del Código Penal de este país. Inicialmente reforma los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley Nº 4573. Por otro lado adiciona el inciso 6) al artículo 229 y un artículo 229 ter. Finalmente modifica la sección VIII del título VII del Código Penal, titulándolo "Delitos informáticos y conexos", donde regula desde el art. 230

hasta el art. 236. En esta modificación bastante integral, agrega una importante cantidad de delitos informáticos al Código Penal, desde los más tradicionales hasta algunos más modernos como la Suplantación de Identidad (art. 230) o el espionaje cibernético (art. 231).

Guatemala: Dentro del Código Penal, posee el Capítulo VII, titulado "De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos". Allí incorpora distintos artículos penales para las figuras de los delitos informáticos, en especial desde el artículo 274 inc. A hasta el inciso G.

Honduras: Dentro del Código Penal Decreto 144/83 Si bien no se ha encontrado legislación especial en la materia, si posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos podremos encontrar los artículos 214, 215, 223 y 254. Por otro lado, el Decreto 144/83 incorpora algunos delitos para tipificar la pornografía infantil a través del art. 149 y sus incisos al Código Penal.

Nicaragua: No se ha encontrado legislación sobre la materia. Existe un anteproyecto de ley. Como se puede observar los países que cuentan con una adecuada legislación son Costa Rica, Panamá y Guatemala que cabe hacer mención que estos se encuentran suscritos al también conocido como Convenio de Budapest, el cual se abrió a la firma en 2001, tiene como objetivo principal alcanzar una política penal común destinada a proteger a la sociedad contra el Cybercrimen, a través de la adopción de una legislación apropiada y la estimulación de la cooperación internacional por su parte en países como Honduras, Nicaragua y más específicamente en lo que nos concierne como equipo de investigación a El Salvador no existe una regulación especial cuenta solamente con el anteproyecto de ley y unos artículos existentes en la Ley Especial Integral para una Vida Libre de Violencia para las Mujeres los cuales a consideración de este equipo de investigación resultan insuficientes para el aumento de este tipo de delitos a medida se van dando avances tecnológicos por su parte el anteproyecto de ley sobre delitos informáticos, que había obtenido el consenso en la comisión de seguridad de la Asamblea Legislativa, fue atacado y prácticamente detenido por los medios de comunicación, al hacerlo lucir como una "ley mordaza", que intentaría controlar y regular el acceso y la libre expresión a través de las redes sociales, Internet y los medios tecnológicos. Razón

por la cual fue regresada a la Comisión de Seguridad para llevar a cabo un estudio más profundo.

2.12.3 TRATADOS INTERNACIONALES.

En la sección tercera del Título VI de nuestra Constitución específicamente en el artículo 144 se hace referencia a los Tratados Internacionales los cuales estén suscritos por nuestro país y que desde el momento de su ratificación pasan a ser leyes de la Republica así como también a ser una herramienta para que posteriormente puedan ser aplicados en relación con otras leyes las cuales tengan la finalidad de robustecer o suplir los vacíos que los tratados pudiesen tener.

Art. 144 Cn.- "Los tratados internacionales celebrados por El Salvador con otros estados o con organismos internacionales, constituyen leyes de la República al entrar en vigencia, conforme a las disposiciones del mismo tratado y de esta Constitución. La ley no podrá modificar o derogar lo acordado en un tratado vigente para El Salvador. En caso de conflicto entre el tratado y la ley, prevalecerá el tratado".

Es en este mismo orden de ideas y en lo concerniente a los denominados delitos cibernéticos nuestro país hasta el día de hoy no se encuentra suscrito a ningún tratado internacional referente a este tema sobre el cual debe hacerse referencia la existencia del Convenio sobre la Ciberdelincuencia de Budapest (23-11-2001) suscrito por los Estados miembros del Consejo de Europa. De este tratado se deslinda posteriormente la Conferencia de Ministros de Justicia de los países Iberoamericano (COMJIB) en España donde los países como Nicaragua, Guatemala, Perú entre otros firmaron el "Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de la Prueba en Materia de Ciberdelincuencia" así como también la "Recomendación de COMJIB relativa a la Tipificación y Sanción de la Ciberdelincuencia" con esto se pretende tener un fuerte impacto en las diferentes legislaciones donde El Salvador por su parte tuvo representación diplomática mas es de mencionar que en calidad de observadores

donde tomaron la palabra anunciando que un futuro próximo se estaría adhiriendo a ambos instrumentos.

Tal decisión conlleva cierto grado de afectación puesto que en dado caso el Estado Salvadoreño se hubiese suscrito al Tratado y posteriormente con su ratificación fuese una herramienta de gran utilidad para los jueces de la Republica ya que estos debido a la ausencia de una ley especial en la cual este tipificados este tipo de delitos podrían hacer uso del Tratado tomado como base lo dispuesto en el artículo 144 de la Cn. en el cual cita que los tratados celebrados y ratificados por El Salvador constituyen leyes de la republica al entrar en vigencia.

CAPITULO III: METODOLOGIA DE LA INVESTIGACION.

El método en el que nos basaremos como grupo de investigación es el **Método Cualitativo,** debido a que este método se basa en profundizar y enfocar desde la perspectiva de los participantes en el contexto para relacionar los acontecimientos que se dan en el diario vivir con el tema a investigar; una de las características básicas en el método a utilizar es su expreso planteamiento de poder ver los acontecimientos, legislación, acciones, valores; desde la circunstancia que la gente está siendo estudiada y así poder analizar el comportamiento de la sociedad en el ámbito del ambiente en que se desenvuelve el problema a investigar.

La importancia del método cualitativo en los procesos de investigación es la que constituye el análisis que se desarrolla, partiendo así de lo general a lo especifico, permitiendo una investigación eficaz en cuanto a la problemática a tratar, puesto que permite al investigador comprender y profundizar los fenómenos explorándolos desde la perspectiva de los participantes, por lo tanto la finalidad de utilizar este tipo de metodología cualitativa es para presentar la realidad sin alterar su naturaleza es decir mostrar su contenido mediante lo que se observó por los diferentes actores claves que son fundamentales para nuestra investigación.

3.1 TECNICAS DE INVESTIGACION.

Las técnicas que utilizaremos en nuestra investigación se desarrollaran de la siguiente manera:

3.1.1 La Entrevista Estructurada a Profundidad.

Esta se define como una forma estructurada de obtener información mediante una serie de preguntas abiertas realizadas al entrevistado, que es el informante clave de nuestra investigación el cual proporcionara los datos fehacientes y necesarios dando con esto información verídica a nuestro trabajo de investigación los cuales son el Juez del Tribunal Primero de Sentencia de Santa Ana, un Defensor Público

(procurador) y un Fiscal Auxiliar, este tipo de entrevistas tienen la característica especial que solo son realizadas a una sola persona.

El propósito de las entrevistas es obtener respuestas sobre el tema, problema o tópico de interés en los términos, el lenguaje y la perspectiva del entrevistado con sus propias palabras; es la técnica más recomendada por los expertos para obtener una información específica sobre el objeto de estudio mediante una conversación profesional con una o varias personas para un estudio analítico de investigación o para contribuir en los diagnósticos o tratamientos sociales, de la variedad de problemas que se pueden generar en el contexto de la sociedad.

3.1.2 Ficha Bibliográfica.

Es en la que se permite anotar todos los datos y referencias bibliográficas de los libros, noticias, artículos, tesis, leyes de la Republica de El Salvador, páginas web, etc; que se consultaron para poder recabar los datos teóricos que son necesarios y esenciales para la realización de nuestro trabajo de investigación, como parte de la metodología en lo referente a la investigación.

3.2 OBJETO DE ESTUDIO.

Para realizar un estudio exhaustivo sobre la Impunidad de las Conductas Lesivas a la persona humana, cometidas a través de las redes sociales en el Departamento de Santa Ana es necesario realizar un análisis que conlleve ambas variables es decir el fundamento teórico-práctico es así que es necesario separar todos aquellos conceptos básicos que nos han sido proporcionados con anterioridad y poder determinar que sin estos conceptos no es posible determinar nuestro objeto de estudio o investigación.

En razón de lo cual es necesario determinar ¿Qué es el objeto de estudio y de dónde surge? El objeto de estudio no es más que lo que queremos saber sobre la situación o como es citado por Hernández Sampieri "fenómeno de Interés" que se esté dando siendo así que consideramos como grupo de investigación realizar una investigación exhaustiva sobre él porque al cometerse estas conductas lesivas por

medio de las redes sociales por los usuarios en el departamento de Santa Ana quedan en la impunidad. Después de establecido el objeto de estudio es lo que queremos saber con respecto al tema deberemos determinar ciertos aspectos importantes para su determinación como lo son a través de la delimitación, conceptualización, considerar aspectos empíricos y finalmente interpretar el objeto de estudio para lo cual será necesario la utilización de técnicas de investigación científica como lo es la entrevista estructurada a profundidad con la finalidad de poder sustraer de los informantes claves todos los insumos necesarios que poseen como parte de su experiencia que han logrado recopilar en su relación con el objeto de estudio por el trabajo que desempeñan, que nos servirán para lograr los objetivos propuestos en la investigación y poder determinar de una forma clara y veraz nuestro objeto de estudio como lo es poder precisar sobre la Impunidad de las Conductas Lesivas a la persona humana, cometidas a través de las redes sociales en el Departamento de Santa Ana.

3.3 POBLACION Y MUESTRA.

3.3.1 Población.

Para poder determinar lo que es la población y la muestra de nuestra investigación es necesario hacer una distinción entre estos conceptos población por su parte es cualquier colección finita o infinita de elementos o sujetos aun que es necesario hacer referencia a la diferencias existentes entre universo y población ya que algunos autores establecen diferencias entre estos indicando por el primero un conjunto de personas, seres u objetos y con el segundo, un conjunto de números obtenidos midiendo o contando cierta característica de los mismos de ahí que un universo puede contener varias poblaciones. Es así que para esta investigación se hará uso del término Población como sinónimo de Universo ya que no existe la posibilidad de confusión siendo ese el criterio que se usara en esta lectura.

Por consiguiente los sujetos de estudio para la presente investigación no está referido a cualquier universo de personas sino que están conformados en una parte por profesionales de las Ciencias Jurídicas que laboran en los Juzgados de

Sentencia de Santa Ana, Fiscalía General de la Republica Regional Santa Ana y Procuraduría General de la Republica Auxiliar Santa Ana; así también por personas con conocimientos especializados en la materia de informática las cuales basados en el marco teórico de nuestra investigación son de gran importancia para poder determinar el objetivo de la misma.

3.3.2 Muestra.

Es un conjunto de la población, que se obtiene para averiguar las propiedades o características de esta, por lo que interesa que sea un reflejo de la población, que sea representativa de ella, es así que la muestra se toma en base a sujetos que puede proporcionar la información necesaria a cerca del presente investigación, de tal manera que esta no excede ni el cinco por ciento de la población esto con la finalidad de descansar bajo el principio de que las partes representan el todo, y por tal, refleja las características que definen a la población del cual fue extraída lo cual indica que es representativa como para poder validar la información en relación con la investigación.

Es así que la población muestreada es aquella de la que a partir se extrajo la muestra y sobre la cual estableceremos como grupo de investigación nuestra conclusión. Los métodos de la evaluación estadística nos permitirán sacar las conclusiones sobre la población muestreada bajo el precepto que esta es adecuada en calidad y en cantidad determinando que esta es representativa de la muestra extraída de una fuente especial y de informantes con especialidad sobre el objeto de estudio en referencia. Se dice que una muestra es representativa de la población cuando es un reflejo de ella, es decir cuando reúne las características principales de la población en relación con la variable de estudio. Y para nuestra investigación los elementos tomados en cuanta para la realización de la entrevista de investigación consideramos que cumple con la característica de ser representativa de la población.

Consideramos necesario y oportuno hacer mención del tipo de muestreo del cual se hará uso como lo es el Muestreo no aleatorio ya que consideramos que es el más indicado para nuestra investigación ya que en este la muestra se escoge según

el juicio y la conveniencia del equipo investigador pero si considerando la idoneidad y especialidad del informante clave.

3.4 PLAN DE ANALISIS.

Podemos mencionar que en la indagación cualitativa se tiene mejor amplitud y riqueza de los datos recabados en la investigación, debido a que los datos van a provenir de diferentes actores del proceso a investigar, de igual manera de diferentes fuentes que nos brindaran la información necesaria para este tipo de investigación cualitativa, y lo cual permite la interrelación y la triangulación de la experiencia de los informantes claves.

La recopilación de la información se hará por medio de la entrevista estructurada a profundidad, se recibirá información de una manera estructurada pero metodológicamente se hace necesario procesarla bajo la metodología llamada **"Metodología de Triangulación"** la cual consiste en una técnica para poder analizar los datos que se recabaron en la investigación cualitativa por medio del instrumento que se va a utilizar que es la entrevista estructurada a profundidad, brindando así la opción de ver la situación de diversos ángulos, por eso se procederá a agrupar los resultados obtenidos por cada entrevista que se realizara individualmente a los informantes claves, que estos son las personas que por su cargo o función ejercida sostienen una relación directa con el conjunto de elementos que se investiga y que el conocimiento que poseen ha sido logrado por el trabajo que desempeñan por lo que se convierten en piezas claves para el análisis, descubrimiento y así poder aproximarse a la verdad de los hechos.

Luego se elaborara un análisis de las respuestas obtenidas con la finalidad de proporcionar al lector una mejor comprensión en la información que se va a recabar y se va a concluir con vaciar en una matriz dicha información para realizar una síntesis de lo mencionado por cada informante clave de la investigación.

CAPITULO IV: ANALISIS E INTERPRETACIÓN DE LA INVESTIGACION.

La ejecución del plan de análisis se hizo en tres pasos los cuales fueron: Recopilación de la información, Procesamiento y el Análisis e Interpretación de la misma, los cuales como equipo de investigación detallaremos a continuación.

4.1 LA RECOPILACION.

Este paso se llevó a cabo por medio de la entrevista estructurada a profundidad; teniendo un contacto previo con las instituciones que en nuestro trabajo de grado serían las fuentes de donde obtendríamos la información, una vez realizado el primer contacto, se acordó mediante cita el día y hora para la realización de las entrevistas, tomándonos un tiempo de cincuenta y cinco minutos por cada entrevista, debido a la novedad y naturaleza del tema investigado, logrando con esto obtener una calidad en la información obtenida; al momento de realizar las entrevistas cada uno de los integrantes del equipo de investigación desarrollamos un rol importante, dividiéndonos los roles uno de nosotros realizaba la pregunta, otro tomaba nota y el tercer integrante graba la entrevista, sin que esto obstaculizara que los integrantes que tomaba nota y el que grababa pudieran intervenir en caso de duda de la respuesta obtenida, con esta forma de realizar la entrevista estructurada a profundidad se logró posteriormente a la realización de la misma transcribir de manera íntegra el testimonio obtenido.

4.2 El PROCESAMIENTO.

Este paso se llevó a cabo haciendo uso del software llamado "WEFT QDA" es el cual es un programa de uso informático que permite realizar la transcripción de la información obtenida a través de las entrevista estructuradas a profundidad y posteriormente se codifica permite establecer categorías y poder filtrar la información y procesar los datos por genero de categoría de análisis, este software es de uso libre, no hay un propietario que pueda reclamar los derechos de autor.

4.3 EL ANALISIS.

Este paso se llevó a cabo después de obtenida la información mediante las entrevistas estructuradas a profundidad, posteriormente se realizó el filtrado de datos mediante el uso del software "WEFT QDA" que permitió el uso de categorías, de ahí se obtienen tres tipos de análisis: análisis inductivo, análisis comparativo y análisis de triangulación; a partir del criterio obtenido por parte de los informantes claves que desempeñan los siguientes cargos, Jefa Fiscal de la Unidad del Menor y la Mujer Regional Santa Ana, Procurador Auxiliar de la Procuraduría General de la Republica Regional Santa Ana y el Juez del Tribunal Primero de Sentencia del departamento de Santa Ana.

4.3.1 ANALISIS INDUCTIVO.

La inducción es un proceso mental el cual consiste en la observación de los hechos particulares obtenido proposiciones generales, es decir obtener un principio general, posterior haber realizado el estudio, análisis de hecho y fenómenos en particular.

La información obtenida del instrumento utilizado; el cual fue la entrevista estructurada a profundidad, arrojo una serie de datos que se ordenaron en categorías, las cuales se fueron descubriendo conforme se procesó la información y se partió de elementos particulares que se encontraron en las codificaciones de elementos generales establecidos y se hizo una vinculación entre ellas con la finalidad de obtener la conexión existente entre estas.

4.3.2 ANALISIS COMPARATIVO.

El análisis comparativo es un procedimiento sistemático y ordenado utilizado para examinar relaciones de semejanzas y diferencias entre dos o más objetos, con el propósito de extraer conclusiones.

A partir de las condiciones que anteceden se hizo una comparación de las diferentes categorías con el fin de establecer las similitudes, relación que existe entre

las mismas y todo elemento necesario en la investigación, con la comparación se pretendía discutir los elementos previos, es decir la teoría formal con los nuevos hallazgos que fue la teoría sustantiva a fin de generar nuevas perspectivas e interpretaciones del problema.

4.3.3. ANALISIS DE TRIANGULACION.

Este análisis se realiza mediante la confrontación de diferentes fuentes de datos, en los estudios, con lo que se realiza una comparación de datos de diversos ángulos para comparar y contrastar entre sí.

En nuestra investigación el análisis de triangulación se hizo comparando cada uno de los instrumentos que se diseñaron con los resultados obtenidos, con la finalidad de establecer si se alcanzaron los objetivos que como equipo de investigación nos planteamos; para lo cual partimos de elementos teóricos y empíricos que se consideraron en el estudio y en la elaboración del marco teórico.

4.4 DATOS GENERALES.

Se entrevistaron a tres personas que son los informantes claves de nuestra investigación con conocimiento especial y una gran experiencia lo cual los convierte en especialistas en el área Penal, son representantes de instituciones del Estado que conforman el Órgano Judicial y el Ministerio Publico, pudiéndolos denominar informantes claves de la investigación, siendo estos: Jefa Fiscal de la Unidad del Menor y la Mujer Regional Santa Ana quien está encargada de dirigir la investigación de agresiones y violencia en contra de la mujer y posee una experiencia laboral de dieciocho años; Procurador Auxiliar de la Procuraduría General de la República Regional Santa Ana que su función es la defensa técnica a las personas que se les acusa de un delito de cualquier clase y su experiencia laboral es de once años y el Juez Primero de Sentencia de la Ciudad de Santa Ana quien labora para el Órgano Judicial que desempeña las funciones de dirigir las audiencias de vista pública y dictar sentencia que posee una experiencia de dieciocho años de laborar en su cargo.

4.4.1 ANALISIS E INTERPRETACION DE LA INVESTIGACION.

Se realizara de forma detallada las categorías y sus respectivas codificaciones, las cuales surgieron de las entrevistas realizadas como equipo de investigación, así mismo se realizara su respectiva interpretación, análisis y triangulación de los criterios obtenidos con respecto a la temática de nuestra investigación.

1. Institución para la que laboran los informantes claves de la investigación: El objetivo que como grupo de investigación realizáramos esta categoría, tiene como propósito reflejar que los informantes claves son funcionarios que se desenvuelven profesionalmente en instituciones del ministerio público y del órgano judicial, lo que los coloca en una posición idónea de poder brindar su criterio acerca de la temática investigada y el auge que esta presenta en la sociedad actual.

La primera funcionaria entrevistada al realizarle la interrogante que desde hace cuánto tiempo labora para la Fiscalía General de la República, manifestó "tengo dieciocho años de laborar para la Fiscalía específicamente en esta oficina que es la oficina Regional de Santa Ana"; por su parte al realizar la misma pregunta el segundo funcionario entrevistado respondió "laboro para la Procuraduría General de la República a partir del año 2004, tengo once años de Laborar para esta institución"; al preguntarle al tercer funcionario que cuál es el nombre de la institución para la que labora el manifestó "laboro para el Órgano Judicial me desempeño como Juez en el Tribunal Primero de Sentencia de Santa Ana.

Como equipo de investigación podemos concluir en base a la información proporcionada por los informantes claves que las instituciones para las que ellos laboran son de suma importancia, debido a que en nuestro país todo proceso penal inicia con una denuncia en la sede de la Policía Nacional Civil o en la sede de la Fiscalía General de la República siendo estos dos organismos los encargado de actuar conjuntamente para el esclarecimiento del hecho investigado para su posterior judicialización; la base legal para su fundamento es el Articulo 193 de la Constitución de la República, donde se establece las atribuciones de la Fiscalía General de la República, entre las cuales podemos destacar, promover de oficio o a petición de

parte la acción de la justicia en defensa de la legalidad y así mismo dirigir la investigación del delito con la colaboración de la Policía Nacional Civil; el Decreto 733 del Código Procesal Penal establece que poseemos un sistema procesal mixto de tendencia acusatoria, por lo que debe sistematizarse de mejor manera el ejercicio del poder punitivo del Estado, reafirmando el carácter de órgano persecutor del delito a la Fiscalía General de la República; es por esto que surge la necesidad de realizar la investigación en otra institución fundamental en el Proceso Penal como lo es la Procuraduría General de la República debido a la importancia que esta institución representa en cuanto a garantizar los derechos que toda persona a la que se le acuse tiene, por lo que al realizar una conducta lesiva según el Artículo 81 del Código Procesal Penal es el que establece que el imputado tendrá derecho a intervenir personalmente y por medio de su defensor en todos los actos procesales y audiencias que impliquen la producción e incorporación de elementos de prueba y a formular él o por medio de su defensor, las peticiones que se consideren pertinentes; es decir la Procuraduría General de la Republica es el ente garante de los derechos de la persona a quien se imputa un delito, y en tercer lugar para completar la relación jurídico-procesal necesitábamos conocer el criterio de un representante del Órgano Judicial en este caso se le realizo la entrevista al Juez Primero de Sentencia de Santa Ana; quien según el Artículo 1 del Código Procesal Penal establece quienes conforman el órgano judicial y que corresponde exclusivamente a este Órgano la potestad de juzgar y hacer ejecutar lo juzgado en materias constitucional, civil, penal, mercantil, laboral, agraria, de tránsito, de inquilinato, y de lo contencioso-administrativo, es por esto que las tres instituciones entrevistadas serán de vital ayuda en nuestra investigación ya que son las que llevan a cabo la investigación y judicialización de todo caso penal en nuestro país.

2. Cargo o funciones que desempeñan los entrevistados: En esta categoría se especificara el cargo o la función que desempeñan cada uno de los informantes claves, lo cual es de suma importancia para el desarrollo de esta investigación con el fin de evaluar si existe una forma de proceder a partir de tener el conocimiento de

una conducta lesiva cometida utilizando como medio para su cometimiento el Internet por medio de las redes sociales.

Al preguntarle a la Fiscal de Santa Ana que si podría describirnos el cargo que realiza para la institución, la funcionaria entrevistada nos manifestó "actualmente tengo cinco años de desempeñarme como jefa de la Unidad de delitos relativos a la niñez, adolescencia y la mujer en su relación familiar y a partir de mayo de este año también me desempeño alternativamente como jefa de la nueva "Unidad de atención especializada para la mujer"; por su parte el Procurador Auxiliar de Santa Ana ante la misma interrogante respondió "el cargo es brindar asesoría y conceder asistencia legal preventiva, servicios de mediación y conciliación así mismo ejercer la defensa técnica de las personas a las que se les imputa un delito de cualquier naturaleza ya que en la institución para la que laboro no cuenta con unidades específicas, si no que conocemos de todos los delitos en el caso de que a la persona se le impute un delito no contraten un abogado particular", nuestro tercer funcionario que labora para el Juzgado Primero de Sentencia de Santa Ana al realizarle la pregunta que si podría describir la función que desempeña la institución en la que usted labora, nos manifestó "conocer de hechos delictivos suscitados específicamente dentro del área penal, podría decir se me ha sido delegado por parte del Órgano Judicial de acuerdo a los requisitos exigidos por la ley orgánica judicial, es decir conocimiento y experiencia, la resolución de los conflictos de grado penal en etapa de vista pública".

En razón de lo expuesto y manifestado por los entrevistados como grupo de investigación podemos concluir en esta categoría, la relevancia de cada uno de los entrevistados en base al cargo que cada uno desempeña para la institución que estos laboran como funcionarios, así como la claridad en el cargo que desempeñan la primera funcionaria se desenvuelve como Jefa de la Unidad del Menor y la Mujer y según la Ley Orgánica de la Fiscalía General de La República, en su Artículo 19 establece que las facultades conferidas por la Constitución, los Tratados Internacionales y las leyes de la República, al Fiscal General de la República serán desempeñadas por éste y por los funcionarios que laboren para dicha institución, esto lo realizara a través de la estructura interna y jerárquica; en el Articulo 37 del mismo cuerpo normativo encontramos la calificación de agentes auxiliares donde se

establece que todas las personas delegadas por el Fiscal General para desempeñar sus atribuciones, actuando en su nombre y en el de la Fiscalía General, tienen la categoría de empleados de confianza y de dependencia directa, funcional y jerárquica del Fiscal General; los requisitos para desempeñar dicho cargo son ser salvadoreño, mayor de edad, Abogado de la República, de moralidad y competencia notorias; así mismo observamos la importancia de las funciones del Procurador Auxiliar de la República Regional Santa Ana, y el cargo que desempeña , según la Ley Orgánica Judicial de la Procuraduría General de la República en su Artículo 13 y 14, el Procurador General podrá facultar su representación, la cual se ejercerá en los servidores públicos de la Procuraduría, es decir su función está íntimamente relacionada al nivel de dirección de la Procuraduría, ya que esta función será ejercido por el Procurador General, con el apoyo inmediato del Procurador General Adjunto, los Procuradores Adjuntos de Áreas Especializadas, el Secretario General y el Coordinador de Calidad Institucional; por su parte el tercer entrevistado desempeña el cargo de Juez en el Juzgado Primero de Sentencia de Santa Ana es por la idoneidad con los requisitos establecidos en la Ley Orgánica Judicial con el cargo que desempeñan como lo son: ser Salvadoreño, mayor de dieciocho años de edad, tener aptitud y capacidad intelectual para desempeñar el cargo respectivo, ser de conducta y condición moral satisfactoria, llenar los requisitos particulares que para cada cargo señalen otras leyes y el Manual de Clasificación de Cargos así como Aprobar en la escuela judicial los cursos que fije el reglamento, el proceso se realiza sometiéndose a los procedimientos de selección señalados en el reglamento respectivo; según el artículo 17 de la Ley Orgánica Judicial: los magistrados, jueces y los servidores judiciales, ingresarán a la carrera por nombramiento, cumpliendo con lo dispuesto en esta ley, sus reglamentos y manuales, se puede observar que los funcionarios entrevistados poseen el conocimiento y cumplen con los requisitos necesarios estipulados en la ley para el cargo que desarrollan.

3. Funciones y atribuciones específicas que desempeñan los informantes claves: Esta categoría es de mucha relevancia en el desarrollo de la investigación, debido a que se va establecer las funciones que cada informante clave desempeña y

aquí radica el motivo de por qué ellos fueron elegidos como informantes claves en nuestra investigación, es por esto que en la categorías anteriores se determinaron las instituciones paras las que laboran y el cargo que desempeñan.

En el caso de la funcionaria que se desempeña como Jefa Fiscal de la Unidad del Menor y la Mujer de la Fiscalía General de la Republica regional Santa Ana al realizarle la pregunta que cuál es el área donde se desenvuelve en la institución nos respondió "me estoy desempeñando como jefa de las dos unidades, las dos áreas son conexas se trabaja con victimas especiales, en la unidad de delitos relativos a la niñez, adolescencia y la mujer en su relación familiar se trabaja con niños adolescentes y mujeres agredidas por conductas de tipo sexual, familiar y en la Unidad de atención especializada para la Mujer se trabaja con mujeres adultas agredidas sexualmente y que son víctimas de los once delitos contemplados en la LEIV, dirigimos la investigación del delito con la colaboración de la Policía Nacional Civil y de los organismos especializados en la investigación, con el propósito de recabar la mayor cantidad de prueba y posteriormente se fundamenta el caso y se realiza el requerimiento fiscal para promover el enjuiciamiento de los sujetos activos de estas conductas"; por su parte el Procurador Auxiliar de Santa Ana al realizarle la interrogante si podría decirnos cuál es el área específica donde labora en la institución en referencia, nos manifestó "soy defensor Penal, es el área específica donde me desempeño pero nosotros tenemos que brindar así como anteriormente mencione asistencia legal, servicios de mediación, conciliación, representar judicialmente y extrajudicialmente a las personas que se aboquen a la institución en pro de la defensa de las libertades individuales esa la función que se realiza en el área Penal"; el Juez del Tribunal Primero de Sentencia de Santa Ana que es nuestro tercer informante clave al formularle la pregunta que describiera de manera específica cuales son las funciones que realiza dentro de la institución que representa, manifestó "la función que cumplo es la verificación de las audiencias de juicio en la etapa de Vista Publica, además de dictar Sentencia."

Analizando la información obtenida de las entrevistas estructuradas a profundidad realizada a cada uno de los informantes claves, podemos determinar la importancia de las funciones y atribuciones que los informantes como funcionarios

poseen; ya que según lo establecido en el Artículo 5 del Código Procesal Penal encontramos que dentro de las funciones conferidas a la Fiscalía General de la República se encuentra ejercer la acción penal pública, para la persecución de oficio de los delitos en los casos determinados por este Código; es por eso que a las atribuciones que posee dicha institución se ven reflejadas en el trabajo desempeñado por la funcionaria entrevistada en dicha institución debido a que depende de ellos el inicio de la judicialización de una conducta lesiva, porque es precisamente esta institución la que representan los intereses de las víctimas para garantizarles el goce de sus derechos, aquí es donde surge la importancia de la labor desarrollada por el Procurador Auxiliar, ya que es la fiscalía quien garantiza los derechos de la víctima, por lo tanto se necesita de un ente que garantice los derechos y garantías conferidas en la Constitución de la República a toda persona que se le imputa un delito tal y como lo establece el Artículo 12 Cn que reza de la siguiente manera "Toda persona a quien se impute un delito, se presumirá inocente mientras no se pruebe su culpabilidad conforme a la ley y en juicio público, en el que se le aseguren todas las garantías necesarias para su defensa. La persona detenida debe ser informada de manera inmediata y comprensible, de sus derechos y de las razones de su detención, no pudiendo ser obligada a declarar. Se garantiza al detenido la asistencia de defensor en las diligencias de los órganos auxiliares de la administración de justicia y en los procesos judiciales, en los términos que la ley establezca. Las declaraciones que se obtengan sin la voluntad de la persona carecen de valor; quien así las obtuviere y empleare incurrirá en responsabilidad penal.

Es en este artículo donde se garantiza el derecho a un defensor que toda persona posee; en el caso concreto de nuestro tercer informante clave que es el Juez del Tribunal Primero de Sentencia del Juzgado Primero de Sentencia de Santa Ana en el Artículo 53 que reza de la siguiente manera "Los tribunales de sentencia estarán integrados por tres jueces de primera instancia y conocerán de la etapa plenaria de todos los delitos y de la vista pública de las causas excluidas del conocimiento del tribunal del jurado; el tribunal de sentencia en pleno conocerá en los casos siguientes: a) De los delitos de crimen organizado cometidos con anterioridad a la vigencia de la ley especial. b) Delitos de realización o investigación

compleja, no comprendidos en la Ley Especial contra el Crimen Organizado y Delitos de Investigación o Realización Compleja. c) En los delitos conexos con los señalados en los numerales anteriores. Para los efectos de la tramitación, dirección de la vista pública, redacción y ponencia de la sentencia, en los casos de conocimiento colegiado, se hará la distribución de forma equitativa. La fase plenaria corresponderá a uno solo de los jueces en los casos excluidos del conocimiento del jurado y del tribunal en pleno. Es por esto que el equipo investigador llega a la conclusión que los tres entrevistados realizan las atribuciones conferidas en la ley correspondiente al cargo que desempeñan y la importancia que esto implica en la realización de un debido proceso.

4. Experiencia laboral y conocimiento según la especialidad de cada informante clave: El objetivo de esta categoría lleva como propósito reflejar el grado de experiencia que poseen los entrevistados, y cuál es el criterio que ellos como especialista del Derecho poseen acerca del tema de investigación.

La Jefa de la Unidad del Menor y la Mujer de la Fiscalía General de la Republica regional Santa Ana al realizarle la pregunta que con su experiencia y conocimiento, si podría decirnos qué es para ella un ciberdelito, lo cual manifestó "poseo una experiencia de dieciocho años de laborar para la institución y por la experiencia puedo decir son aquellos delitos cometidos por las actualmente y de moda las llamadas redes sociales a través de un medio informático o un medio electrónico una computadora, teléfono, tablet, etc; por todos los medios tecnológicos que la tecnología ahora nos pone a disposición, este conocimiento lo poseo debido a que es necesario en el despeño de mis labores por que la LEIV establece conductas que pueden realizarse a través de medios tecnológicos"; por parte del Procurador Auxiliar de Santa Ana al plantearle la interrogante que debido a su experiencia y conocimiento podría decirnos si se han presentado personas a la institución acusadas de cometer un Ciberdelito, lo que el contesto **"**por ciberdelito entiendo el modo de cometer un delito común, es decir , que es de conocimiento popular que todas las personas tenemos, pero que se realiza a través de medios tecnológicos, haciendo uso de computadoras, celulares inteligentes inclusive utilizando las redes

Sociales, de mi conocimiento no ha habido ningún caso de esos, al menos en los once años que tengo de laborar para la institución no he escuchado que en la institución haya prestado defensa técnica a ninguna persona que sea acusada de un ciberdelito"; y por su parte el Juez del Tribunal Primero de Sentencia del departamento de Santa Ana al realizarle la interrogante que desde hace cuánto tiempo labora para esta institución, él nos manifestó "tengo veintidós años de laborar para el Órgano Judicial, de esos veintidós años, dieciocho los he laborado en el área penal".

Como equipo investigador después de haber realizado las entrevistas estructuradas a profundidad, podemos observar la idoneidad de los informantes claves debido a la experiencia y conocimiento obtenido que los vuelve especialistas penales en el caso del Juez de Sentencia podemos observar que sus veintidós años de experiencia le dan credibilidad y respaldo a su criterio vertido al momento de responder nuestra entrevista; por su parte la funcionaria que labora para la Fiscalía General de la República es vital que combine su experiencia laboral y conocimiento debido a que como anteriormente lo menciono el Articulo 50 y 51 de la LEIV (Ley Especial Integral para una Vida Libre de Violencia contra las Mujeres) establece dos tipos penales que utilizan como medio para cometerse por medio del internet, el primero Difusión ilegal de información y el segundo Difusión de Pornografía, ya que entre los verbos rectores están publicar, compartir o enviar es por esta razón que la funcionaria Jefa Fiscal de la Unidad del Menor y la Mujer de la Fiscalía General de la Republica regional Santa Ana no puede desconocer este tipo de información, así mismo observamos que el Procurador Auxiliar de Santa Ana posee el conocimiento de que podríamos denominar ciberdelito aunque en la institución no se ha presentado un caso de este tipo en este sentido es que como grupo de investigación observamos la importancia que cada uno de los informantes claves posee en nuestra investigación.

5. Conocimiento de delitos cibernéticos según el cargo que desempeñan los informantes claves para nuestra investigación: Dentro de nuestra investigación esta categoría es de gran importancia puesto que se determina el nivel

de conocimiento que puede tener el funcionario de los delitos cibernéticos a razón del cargo que desempeñan en la institución que laboran hay que mencionar que con anterioridad a esta categoría ya se definió tanto el cargo del mismo como los años que este tiene de desempeñar dicha función.

Del tal forma fue necesario conocer la opinión del órgano Institucional encargado de promover la acción penal como lo es la Jefa Fiscal de la Unidad del Menor y la Mujer del departamento de Santa Ana la cual debería conocer de este tipo de delitos siendo así que nos es necesario como grupo de investigación el conocer del criterio de la representante de esta institución en lo referente al conocimiento sobre los delitos cibernéticos ante dicha interrogante nos contestó que "si de hecho si se conocen de muchos casos, se tiene un porcentaje no alto porque la situación es que por desconocimiento no todas las mujeres denuncian sin embargo se tiene un pequeño porcentaje de denuncias de este tipo de delitos e incluso tiene uno últimamente que se dio en flagrancia y hubo detención y es único caso, en los otros casos se inicia la investigación como todos los casos por otros delitos cometidos por otros medios pero se encuentran con muchas limitantes en el proceso de investigación, la policía nacional civil en sus divisiones de investigación que es la que coadyuva con la investigación de estos hechos se encuentra limitada por ejemplo la fiscalía les requiere de que maquina ha salido el mensaje, porque medio si fue por Facebook, WhatsApp, etc; por todas las redes sociales que conocemos y nada más pueden llegar a establecer la procedencia de donde salió el mensaje, la imagen; pero es difícil atribuir la conducta tal como lo establece la normativa penal de atribuir una conducta a una persona determinada por que el hecho que una computadora, celular este a nombre de una persona no significa que ella compartió, difundió que son las conductas rectoras de los verbos rectores que la LEIV castiga pero es difícil investigarlos por ejemplo si la unidad de análisis de la policía dice que salió por Facebook dicen que no pueden determinar porque la casa matriz de Facebook está en Estados Unidos y es una red social abierta y que esa información desde el momento que se sube se hace pública y en segundos se puede cambiar de un destinatario a otro y lo que cuesta es establecer quien lo genero es muy difícil probarlo"; ante tal situación y como es lógico es necesario conocer el criterio del

Procurador Auxiliar de Santa Ana el cual ante la interrogante manifestó que "no he tenido la oportunidad de realizar una defensa técnica, y como anteriormente les decía desconozco que en la institución se haya llevado un caso de esa naturaleza"; por su parte el Juez del Tribunal Primero de Sentencia de Santa Ana nos manifestó que "como juez de sentencia bajo el principio de Legalidad, lex certa, lex estricta, lex específica, debo conocer de todos los delitos tipificados en el Código Penal y Leyes Especiales, no puedo conocer de conductas que no estén reguladas en una ley".

Es por esto que como equipo de investigación podemos concluir que tomando como base lo estipulado en la Constitución de la República en su Artículo 193 en el cual se hace referencia a las funciones de la Fiscalía General de la Republica de las cuales podemos mencionar la siguiente "Promover la Acción Penal de oficio o a petición de parte"… es por esto que la Jefa Fiscal de la Unidad del Menor y al Mujer del Departamento de Santa Ana debe conocer por mandato legal de este tipo de casos y que aun que dice que por el cargo que ostenta que si conoce de algunos casos pero que hay un porcentaje alto de mujeres que no denuncian, el Procurador Auxiliar de Santa Ana manifestó que desconoce que se haya realizado la defensa técnica de este tipo de delitos no convencionales debido a que es posible que busquen un defensor privado o porque no denuncian este tipo de ilícitos, por lo tanto esto nos lleva a concluir que no existe concordancia entre las tres principales instituciones encargadas tanto de iniciar la acción penal, la defensa la cual por su parte se nos hace evidente el desconocimiento que esta tipo de delito y por su parte la Institución encargada del juzgamiento la cual manifiesta desconocer de este tipo de casos basado en el Principio de Legalidad y aun que nos manifestó que si conoce de algunos casos esto ha sido a través del estudio académico que ha realizado de forma personal y que no ha sido por medio de la judicialización de ningún caso presentado en el tribunal para el que labora y es que nos lleva a concluir que no hay concordancia entre estas tres Instituciones por la razón que no existe una ley especifica que describa el tipo penal bajo la cual se pueda fundamentar la existencia de un ciberdelito para su posterior judicialización.

6. Ley a utilizar hacia aquellas conductas que lesionan el honor y la intimidad y que según la experiencia en el cargo utilizan los entrevistados de las instituciones correspondientes: Como se puede apreciar y siguiendo un orden lógico de ideas analizaremos la legislación que pueda ser aplicada desde la perspectiva del cargo que desempeñan cada uno de los informantes claves de nuestra investigación.

Por su parte la Jefa de la Unidad del Menor y la Mujer del departamento de Santa Ana nos respondió a tal interrogante que "se aplica la LEIV y es de acción pública y se puede iniciar sin el consentimiento de la víctima y contempla la prohibición de cualquier salida alterna no hay conciliación, no hay procedimiento abreviado"; es debido a la respuesta de la representante de la Fiscalía que consideramos necesario conocer la legislación a aplicar para la regulación de los ciberdelitos utilizada por el Procurador Auxiliar del departamento de Santa Ana ante lo cual manifestó "en mi conocimiento por la inexistencia de una ley vigente que regule específicamente este tipo de conductas cometidas a través de un medio como lo es el internet, específicamente las redes sociales, las leyes idóneas que tengan validez utilizaría primeramente la Constitución de la Republica, en segundo lugar el Código Penal y claro para un procedimiento de legal forma el Código Procesal Penal"; por su parte el Juez del Tribunal Primero de Sentencia de Santa Ana nos respondió que "según la Ley Sustantiva Penal conocido también como Derecho Penal Material y es el que se encuentra consagrado en el Código Penal, cabe mencionar que el derecho penal sustantivo es la parte estática o imagen sin movimiento es decir donde solo hay modalidades como Estafa, Hurto, (es decir solo formas de comisión). Con esto es necesario decir que no hay ley especial".

Ante tal situación como grupo de investigación determinamos lo siguiente: que la Misión de La Fiscalía General de la Republica representada en este caso por medio de la Jefa de la Unidad del Menor y la Mujer, entendiéndose que para iniciar la Acción Penal solamente es necesario que se configure la figura delictiva tipificada en la Ley Integral para una Vida Libre de Violencia para las Mujeres para que la Fiscalía de oficio pueda iniciar el proceso pero que se desvirtúa por lo expuesto por esta Institución encargada de ejercer la defensa técnica la cual nos deja en evidencia por

su respuesta que no existe una legislación específica que regule estas conductas bajo la tipificación de ciberdelitos y por otra parte el criterio dado por el Señor Juez de Sentencia de Santa Ana y bajo el aforismo iura novit curia es que el juez debe conocer el derecho que interpreta o aplica bajo este precepto se piensa que este debe conocer toda normativa aplicable afirmación que como grupo de investigación nos parece demasiado amplia ya que implicaría que los jueces tienen el conocimiento de todas las leyes existentes, aunque en este caso no existe una ley que regule específicamente este tipo de conductas es por esto que ante tal situación como grupo de investigación determinamos que existe una clara discrepancia entre los tres organismos a los cuales se les realizo la entrevista estructurada a profundidad debido a que la Fiscalía de Santa Ana toma como base la LEIV para regular las conductas cometidas a través de internet y se establecen en la ley especial un catálogo de conductas que pueden ser cometidos por medio de internet; por lo cual difiere de la opinión del juez como del procurador auxiliar en el sentido que para ellos no existe una legislación que regule específicamente conductas que puedan tipificarse como ciberdelitos.

7. Procedimiento, medidas a implementar y criterio profesional a utilizar por los informantes claves ante este tipo de conductas: Como grupo de investigación consideramos que en esta categoría es necesario conocer el criterio, ya que por medio de las respuestas a esta interrogante es que trataremos como grupo de investigación darle solución a la problemática planteada sobre las conductas lesivas que utilizan como medio el internet.

Ante tal problemática hemos tomado a bien consultar a la Jefa de la Unidad del Menor y la Mujer de Santa Ana y debido al cargo que esta ostenta es que consideramos necesario conocer sobre el procedimiento que la fiscalía tiene para indagar es este tipo de delitos la cual bajo su criterio profesional manifiesta que "después de la denuncia de la víctima se tiene por ejemplo imágenes, mensajes de texto que se imprimen dentro del Messenger de Facebook se imprimen los diálogos, las imágenes, se brinda el número de teléfono para indagar las bitácoras de llamadas para hacer la interrelación entre la víctima y el supuesto agresor y es lo más que

pueden hacer porque no han recibido ni capacitaciones de eso porque es una deuda del Estado porque solo les dieron la Ley que se fuese efectiva pero no les dieron las herramientas necesarias para investigar este tipo de delitos entonces en ese sentido la jefa ha recibido algunas capacitaciones que ahora lo que tratan de hacer es adecuar las figuras porque prácticamente son las mismas figuras penales solo que en otra dimensión utilizando otros medios entonces eso es lo que están tratando de explotar actualmente por ejemplo el acoso sexual porque ya está establecido.

Realmente se quedan cortos en la investigación en los delitos así como se ven cibernéticos que realmente no tienen las herramientas legales para la investigación"; siendo esto el procedimiento utilizado por la Fiscalía de Santa Ana para la investigación de este tipo de delitos por su parte consideramos a bien y debido al cargo el cual desempeña el Procurador Auxiliar de Santa Ana es que se reformula la pregunta para conocer de este las medidas que implementara a futuro la institución para la cual ejerce funciones a lo cual nos respondió que "debido a la importancia que este tema está tomando en nuestra realidad social, es palpable la necesidad de que exista una mayor divulgación, concientización de lo que en sí son las redes sociales y de la manera idónea de utilizarlas y no solo las redes sociales sino todo lo que se refiere a una cibersociedad actual"; de tal forma y ante a esta respuesta es que el Juez del Tribunal Primero de Sentencia de Santa Ana se le cuestiona sobre el criterio profesional que usa ante este tipo de conductas a lo cual nos respondió que "se pueden cometer este tipo de delitos a través de estos medios pero; no es el criterio que se utiliza, es la prueba esta determinan la presunción de inocencia.

Esta debe ser introducida en el Código Procesal Penal en lo referente a este tipo de delitos. Además los organismos encargados de aportar la prueba como la PNC aportan muy poca información en cuanto a este tipo de conductas, razón por la cual deber haber una mejor preparación de todos las partes intervinientes en el proceso de esta ya que los casos en nuestra sociedad existen, pero muchos no llegan a ser ventilados al Órgano Judicial por falta de prueba para sustentarlo.

Como equipo de investigación podemos concluir que tanto la Jefa Fiscal de la Unidad del Menor y la Mujer y el Juez Primero de Sentencia de Santa Ana establecen la importancia de la prueba en la indagación de un ciberdelito ya que es

por medio de estas medidas que la institución hace una interrelación entre el sujeto activo y la víctima, es por esto que la prueba es trascendental a la hora de iniciar el procedimiento de investigación que se pueda llegar a judicializar el caso; con respecto a las medidas a implementar el Procurador Auxiliar del departamento de Santa Ana manifestó la necesidad de divulgar el buen uso de las redes sociales con la finalidad de prevenir conductas lesivas que dañen el honor y la intimidad, mas no hace alusión a la creación de normas que sirvan al combate de los casos que se presentan y que como grupo de investigación consideramos que es de vital importancia.

8. Medidas a implementar por parte de las instituciones correspondientes en este tema y función del Estado Salvadoreño ante los delitos ciberneticos: En esta categoría se pretende conocer cuál es la función del Estado salvadoreño ante el aumento de este tipo de delitos y que son reportados por Órganos como la PNC o Ciudad Mujer, así como también cuales son las medidas a implementar por parte de los informantes claves entrevistados ante el aumento de este tipo de delitos cometidos mediante el internet.

La postura de la Jefa Fiscal de la Unidad del Menor y la Mujer de Santa Ana nos manifestó en su momento que a su criterio "cada caso es en particular, quizás implementar no en la institución sino más bien crear dentro de la sociedad y luego ir en una escala uno la ciudadanía a que denuncie y dos seria el hecho de poner a la disposición de las instituciones dotar de herramientas de todo tipo se refiere a los insumos que van a tener para terminar la investigación de todo tipo porque de nada sirve iniciar el caso si van a saber que nunca van a poder establecer algunas conductas entonces lo que genera esa impunidad en el pensamiento de la ciudadanía en el pensamiento de la mujer genera ese sentido equivocado de impunidad que no se hace nada lo que favorecería a la institución es capacitar al personal en esa área pero tanto al personal fiscal como al policial"; es debido a esta respuesta que se consideró preguntarle al Procurador Auxiliar del Departamento de Santa Ana sobre los medios idóneos para desvirtuar la realización de conductas cometidas a través de internet a lo que manifestó "en pro de la defensa del imputado,

y de acuerdo a la naturaleza del delito podría desvirtuarse, demostrando la inexistencia del dolo de realizar el daño, que el imputado no es quien vertió el contenido en las red, tomando desde el punto de vista que las herramientas que la institución como la fiscalía y la Policía Nacional Civil poseen no es la idónea para probar los hechos controvertidos, y que el imputado sea el autor directo, determinar ¿cuándo? ¿cómo? y ¿dónde?, él imputado fue el autor intelectual, el tipo de prueba en estos casos es el que es trascendental en estos casos"; de aquí nos nace la necesidad como equipo de investigación de conocer por medio del Juez del Tribunal Primero de Sentencia de Santa Ana sobre cuál es el papel que debería de desempeñar el Estado respecto a las conductas lesivas cometidas a través de la Internet manifestó que el Estado como garante de fomentar el resguardo de las garantías de la población debería regular todas aquellas conductas al honor de las personas sin importar, que existen personas que se opone a que sean tuteladas dichas conductas lesivas un ejemplo de ello son los medios periodísticos resguardándose bajo el secreto periodístico encubren en esto las conductas lesivas realizadas.

Se necesita de una Ley Especial donde se enmarquen más conductas que procedimientos a manera de ejemplo se puede mencionar la venta de información privada de las personas ya que como es conocido hay dos tipos de información, la pública como lo es el nombre de la persona y la Privada como lo son las preferencias políticas o enfermedades de la persona y es a estas a las cuales nos referimos que no tiene razón de ser el hecho que se divulguen es por esto que debe estar regulado en una ley. El Instituto de Acceso de la Información Publica separa los datos privados como programas o secretos profesionales, institucionales de los Públicos, razón por la cual delitos como el Espionaje, Trafico de Información, debe incluirse delitos sobre la regulación del internet y debe haber una aplicación transparente e igualitaria sin haber privilegios sin distinción alguna".

Es por esto que llegamos a la conclusión a través de esta serie de preguntas realizadas a los informantes claves de nuestra investigación y en lo que se refiere a esta categoría de preguntas que se deja en evidencia que siendo el estado el garante de la seguridad y la justicia debería actuar con la debida diligencia y

prevenir este tipo de hechos tendría que implementar las medidas de capacitación para cada una de las instituciones que intervienen en el proceso de judicialización del mismo modo que debe ser fortalecido el rol prioritario y fundamental de la familia, al ser concebida por nuestra legislación como la base fundamental de la sociedad de tal forma que, el Estado tiene la obligación positiva de activar y apoyar tanto a padres como a instituciones del Estado para que estos respondan a sus deberes y prevengan cualquier amenaza o violación de los derechos de la sociedad así también consideramos que deberá dotar de las herramientas necesarias para evitar la impunidad de conductas lesivas al honor y la intimidad por medio de políticas de seguridad teniendo en cuenta que la efectividad de estas depende de la coherencia con las políticas sociales las cuales no se dan por la falta de recursos.

9. Factores que inciden en la impunidad de los delitos relativos a la libertad sexual cometidos por medio de las redes sociales: En esta categoría se busca determinar qué factores son los que afectan el procedimiento que se da cuando se comete una conducta lesiva a la persona cometida a través del internet, al igual que si la legislación salvadoreña cuenta con las disposiciones legales necesarias para regular lo referente a las redes sociales.

La Jefa Fiscal de la Unidad del Menor y la Mujer de la Fiscalía General de la Republica regional Santa Ana, respecto a que si la institución cuenta con los medios idóneos para probar la realización de una conducta lesiva a través de internet, manifestó que "el medio idóneo para establecer que fue cometido a través de internet es un aparato, el decomiso de un aparato pero no se puede privar del uso del aparato porque se estaría violentando su derecho a la intimidad, es algo tan complejo por eso lo que se les piden es que impriman nada mas de sus usuarios sea de WhatsApp, Facebook, Instagran las imágenes, los diálogos, que correspondan al hecho que se está denunciando, generalmente es un ex novio, ex esposo"; al respecto con el Procurador Auxiliar de la Procuraduría General de la Republica regional Santa Ana en referencia a que si la institución cuenta con los recursos y medios técnicos necesarios para investigar y conocer este tipo de conductas lesivas manifestó que "no, la realidad es que la institución no los posee, si es difícil,

investigar un delito común, debido a los pocos recursos limitados que la institución posee, ya que en las defensas que ejerce la institución el mejor recurso que poseemos es el ingenio y astucia del defensor que está a cargo del caso"; el Juez del Tribunal Primero de Sentencia de Santa Ana con respecto a las reformas que se podrían hacer a la legislación penal vigente para poder sancionar las conductas lesivas utilizando como medio para la realización el internet específicamente las redes sociales, expreso "el uso de las redes sociales no está regulado en el Código Penal, tampoco en el Código Procesal Penal, las regulaciones existentes van más orientadas a los delitos de tipo económico cometidos a través de medios informáticos razón por la cual se debe incluir en la Ley Penal un Capítulo específico sobre los Ciberdelitos o la creación y aprobación de una ley especial y por consiguiente una regulación al Código Procesal Penal para determinar un procedimiento que se deba realizar para estos nuevos tipos de delitos".

Analizando las respuestas de los tres informantes claves entrevistados podemos concluir que para la Jefa de la Unidad del Menor y la Mujer de la Fiscalía de Santa Ana es difícil probar estos actos lesivos que dañan y denigran a la mujer debido a que es una red pública y que no se puede individualizar a la persona que sube a la red imágenes que dañan a la mujer porque es difícil secuestrar el aparato por el que se presume fue usado para el cometimiento de este ilícito, por otra parte de acuerdo a la opinión del Procurador Auxiliar de Santa Ana la institución no cuenta con los recursos y medios técnicos necesarios para resolver un caso relacionado sobre delitos por medios electrónicos que sea de carácter sexual, esto conlleva a que la defensa técnica que ellos podrían ejercer carecería de argumentos legales por lo tanto no están capacitados para realizarse en esta área y que el Juez del Tribunal Primero de Sentencia de Santa Ana manifiesta que no existen disposiciones legales que puedan sancionar estas conductas no convencionales por lo tanto estos ilícitos estarían tomando una ventaja considerable en nuestra sociedad, quedando impunes en la mayoría de los casos y lo cual constituye nuestro problema de investigación.

10. Factores que influyen en la judicialización de los casos relacionados a los ciberdelitos: En esta categoría se incluyen diversos factores que inciden en el

procedimiento de este tipo de ilícitos ya sea al querer aplicar la legislación o si se cuenta con los recursos necesarios para realizar una investigación, es de mencionar que a cada uno de los informantes claves se les hicieron diferentes preguntas pero que llevan la misma formalidad en cuanto a querer indagar como equipo de investigación por qué no se logran judicializar los diversos casos que existen.

A la Jefa Fiscal de la Unidad del Menor y la Mujer de la Fiscalía General de la Republica regional Santa Ana se le pregunto que si cuentan con los recursos y medios técnicos necesarios para conocer de este tipo de conductas lesivas a lo que manifestó que "si se cuenta, la fiscalía tiene una Unidad de Análisis dentro de la fiscalía que es de la que nos auxiliamos conjuntamente con la unidad de análisis de la Policía Nacional Civil pero como les reitero y les dije anteriormente llegan hasta el aparato de donde salió la información hasta ahí establecen ellos"; al interrogar al Procurador Auxiliar de Santa Ana que reformas recomendaría en la legislación Penal vigente, en lo relativo a los Ciberdelitos, dijo "lo idóneo no es la creación de una nueva ley, si no crear dentro del Código Penal un apartado, un capitulo que vaya en función de tipificar conductas de esta índole específicamente, por supuesto esto indicaría que el Código Procesal Penal tiene que incluir el proceso para este nuevo capítulo de Ciberdelitos que existiría en el Código Penal, una ley aparte que no reúna un procedimiento adecuado sería seguir caminando en círculo sin pretender solucionar la problemática actual"; en ese mismo sentido el Juez del Tribunal Primero de Sentencia de Santa Ana se le pregunto si es necesaria la creación de un cuerpo normativo especial que regule las conductas realizadas a través de internet lo cual manifestó "pues hasta donde tengo conocimiento existe un anteproyecto de ley referente a este tipo de delitos pero que en su mayoría van tutelando el patrimonio, razón por la cual a mi criterio de no ponerse de acuerdo en la aprobación de la misma debe realizarse reformas a los artículos así como también una reforma al Código Procesal Penal para incluir los medios de prueba, porque no puede aprobarse una ley sin establecer el procedimiento para judicializarlos, sería como identificar la enfermedad sin tener la cura".

Como equipo de investigación se concluye que la Fiscalía de Santa Ana cuenta con los recursos necesarios para poder realizar una buena investigación a este tipo

de ilícitos y pueden establecer de que maquina se subió a la red la imagen indecorosa que daña la moral de la persona, pero que no es suficiente para poder comprobar un ilícito de esa clase debido a que el problema radica en que no logran individualizar a la persona debido a que esa computadora o aparato electrónico pudo haber sido utilizado por más de una persona lo que conlleva a que es difícil determinar el sujeto activo que realizo esa acción; el Procurador Auxiliar de Santa Ana como el Juez del Tribunal Primero de Sentencia de Santa Ana hacen referencia a que la solución a estos actos de impunidad seria de reformar el Código Penal y el Procesal Penal ya existentes para que de esta manera se pueda adecuar la conducta delictiva, es así que no se puede comprobar un delito si no existe una legislación adecuada en donde se describa el tipo penal, por lo tanto estos son los factores que influyen para poder judicializar los diferentes casos y lo que conlleva a que este tipo de conductas queden sin castigo no obstante lesionan derechos de las personas.

11. La cultura como un obstáculo para conocer de los ciberdelitos por parte de las instituciones competentes: En esta categoría se pretende conocer como incide la cultura en una sociedad y particularmente los habitantes del municipio de Santa Ana para denunciar los casos donde se les vulneran derechos fundamentales relativos a la libertad sexual que se cometen a través de las redes sociales y si esto representa un obstáculo para que se crea una ley especial o se reformen las leyes penales existentes.

La Jefa Fiscal de la Unidad del Menor y la Mujer de Santa Ana según su experiencia en el cargo que desempeña manifestó que "es falta de información y conocimiento, la difusión en la población en general, es importante hay muchas personas que ni siquiera conocen la existencia de la ley, que conductas son las que sancionan creen que eso no es delito entonces es importantísimo la difusión y este tipo de delitos se da en otros niveles porque una persona del campo del área rural por poco conocimiento y poca preparación escolar y con una capacidad social limitada no va a tener a su disposición medios electrónicos, entonces este tipo de delitos son cometidos generalmente por personas de otro nivel llámenle social, educacional, etc; entonces lo que se tiene que hacer es una campaña de difusión de

la normativa y que es lo que la normativa sanciona cuales son las conductas que sanciona la ley especial que protegen a la mujer"; sobre la misma problemática el Procurador Auxiliar de Santa Ana dijo "no es que no existan los casos, no de la forma del funcionamiento, es que las víctimas no lo denuncian por ende, si no hay denuncia, no hay judicialización, no conocemos de este tipo de casos, procuraduría es el último eslabón de la cadena por decirlo de algún modo ya que es la Policía Nacional Civil junto con la Fiscalía General de la República que inician un proceso, si tiene que ver mucho el factor cultura por temor a ser victimizada, a que se sepa, es falta de conocimiento no académico como tal, sino como puede ser ayudada en estos casos"; así mismo el Juez del Tribunal Primero de Sentencia de Santa Ana expreso "todos estamos en las redes pero pocos tienen la conciencia que conlleva el estar en estas, es así que es necesario crear la conciencia del factor cultural del buen uso de las redes sociales por medio de un comportamiento educativo del uso por parte de las personas jóvenes las cuales carecen de conciencia por la falta de factores culturales y educativos, las personas que están a la vanguardia de las redes hay que concientizarlas de la naturaleza de la información que se publica; el órgano judicial así como ha iniciado una campaña para el uso de los Juzgados Ambientales debería llevar a cabo talleres en el cual mediante casos prácticos los cuales le sirvan para hacer conciencia a todas las personas, porque las redes sociales se han convertido en un medio que todos tenemos al alcance de un clic, esto debe realizarse de forma conjunta con la empresa privada, gobierno, instituciones públicas, órgano judicial sobre el buen uso de las redes sociales, es un problema que no logramos medir el alcance que puede llegar a tener, pero es mejor concientizar y de alguna manera prevenir, que curar el mal después".

De las tres respuestas proporcionadas por los informantes claves realizamos como investigadores un análisis e interpretación de las mismas, por lo cual concluimos que el factor cultural ha sido el grave problema para conocer de estos casos de ciberdelitos debido al que los tres informantes claves coincidieron en la misma opinión que el nivel cultural que tienen las personas influyen para conocer de estos casos no convencionales que se están dando en nuestra sociedad por lo tanto se necesita concientizar a las personas en el uso de las redes sociales para que de

este modo se regule la conducta de las personas en la cibersociedad y así prevenir daños a terceros y en lo concerniente a las empresas que prestan el servicio de internet, también es necesario establecer límites de operatividad y no dejar la responsabilidad, únicamente al usuario.

4.4.2 MATRICES DE CATEGORIA.

PREG.	CATEGORIAS	EVIDENCIAS		
		FISCAL DE LA FISCALIA REGIONAL SANTA ANA.	PROCURADOR AUXILIAR REGIONAL SANTA ANA.	JUEZ DEL TRIBUNAL PRIMERO DE SENTENCIA DE SANTA ANA.
1	**Institución para la que laboran los informantes claves de la investigación.**	Jefa de la Unidad del Menor y la Mujer de la Fiscalía General de la Republica Regional Santa Ana: Institución gubernamental encargada del ejercicio democrático de la promoción de la acción penal.	Procurador Auxiliar de la Procuraduría General de la República Regional Santa Ana: Institución gubernamental encargada de resguardar los derechos de las personas que se encuentren acusadas del cometimiento de algún delito.	En el Órgano Judicial Regional Santa Ana: Institución que desarrolla la función de Juzgar y hacer ejecutar lo juzgado en materia Penal entre otras.

PREG.	CATEGORIAS	EVIDENCIAS		
		FISCAL DE LA FISCALIA REGIONAL SANTA ANA.	**PROCURADOR AUXILIAR REGIONAL SANTA ANA.**	**JUEZ DEL TRIBUNAL PRIMERO DE SENTENCIA DE SANTA ANA.**
2	**Cargo o funciones que desempeñan los entrevistados.**	Actualmente tengo 5 años de desempeñarme como jefa de la Unidad de delitos relativos a la niñez, adolescencia y la mujer en su relación familiar y a partir de mayo de este año también me desempeño alternativamente como jefa de la nueva "Unidad de atención especializada para la mujer.	El cargo es brindar asesoría y conceder asistencia legal preventiva, servicios de mediación y conciliación así mismo ejercer la defensa técnica de las personas a las que se les imputa un delito de cualquier naturaleza ya que en la institución para la que laboro no cuenta con unidades específicas, si no que conocemos de todos los delitos en el caso de que a la persona se le impute un delito no contraten un abogado particular.	conocer de hechos delictivos suscitados específicamente dentro del área penal, podría decir se me ha sido delegado por parte del Órgano Judicial de acuerdo a los requisitos exigidos por la ley orgánica judicial, es decir conocimiento y experiencia, la resolución de los conflictos de grado penal en etapa de vista pública.

PREG.	CATEGORIAS	EVIDENCIAS		
		FISCAL DE LA FISCALIA REGIONAL SANTA ANA.	**PROCURADOR AUXILIAR REGIONAL SANTA ANA.**	**JUEZ DEL TRIBUNAL PRIMERO DE SENTENCIA DE SANTA ANA.**
3	**Funciones y atribuciones específicas que desempeñan los informantes claves.**	Me estoy desempeñando como jefa de las dos unidades, las dos áreas son conexas se trabaja con victimas especiales, en la unidad de delitos relativos a la niñez, adolescencia y la mujer en su relación familiar se trabaja con niños adolescentes y mujeres agredidas por conductas de tipo sexual, familiar y en la Unidad de atención especializada para la Mujer se trabaja con mujeres adultas agredidas sexualmente y que son víctimas de los 11 delitos contemplados en la LEIV.	Soy defensor Penal, es el área específica donde me desempeño pero nosotros tenemos que brindar así como anteriormente mencione asistencia legal, servicios de mediación, conciliación, representar judicialmente y extrajudicialmente a las personas que se aboquen a la institución en pro de la defensa de las libertades individuales esa la función que se realiza en el área Penal.	La función que cumplo es la verificación de las audiencias de juicio en la etapa de Vista Publica, además de dictar Sentencia.

PREG.	CATEGORIAS	EVIDENCIAS		
		FISCAL DE LA FISCALIA REGIONAL SANTA ANA.	**PROCURADOR AUXILIAR REGIONAL SANTA ANA.**	**JUEZ DEL TRIBUNAL PRIMERO DE SENTENCIA DE SANTA ANA.**
4	**Experiencia laboral y conocimiento según la especialidad de cada informante clave.**	Poseo una experiencia de 18 años de laborar para la institución y por la experiencia puedo decir son aquellos delitos cometidos por las actualmente y de moda las llamadas redes sociales a través de un medio informático o un medio electrónico una computadora, teléfono, tablet, etc; por todos los medios tecnológicos que la tecnología ahora nos pone a disposición.	Por ciberdelito entiendo el modo de cometer un delito común, es decir , que es de conocimiento popular que todas las personas tenemos, pero que se realiza a través de medios tecnológicos, haciendo uso de computadoras, celulares inteligentes inclusive utilizando las redes Sociales de mi conocimiento no ha habido ningún caso de esos.	Tengo 22 años de laborar para el Órgano Judicial, de esos 22 años 18 los he laborado en el área penal.

PREG.	CATEGORIAS	EVIDENCIAS		
		FISCAL DE LA FISCALIA REGIONAL SANTA ANA.	**PROCURADOR AUXILIAR REGIONAL SANTA ANA.**	**JUEZ DEL TRIBUNAL PRIMERO DE SENTENCIA DE SANTA ANA.**
5	**Conocimiento de delitos cibernéticos según el cargo que desempeñan los informantes claves para nuestra investigación.**	Si de hecho si se conocen de muchos casos, se tiene un porcentaje no alto porque la situación es que por desconocimiento no todas las mujeres denuncian sin embargo se tiene un pequeño porcentaje de denuncias de este tipo de delitos.	No he tenido la oportunidad de realizar una defensa técnica, y como anteriormente les decía desconozco que en la institución se haya llevado un caso de esa naturaleza.	Como juez de sentencia bajo el principio de Legalidad, lex certa, lex estricta, lex específica, debo conocer de todos los delitos tipificados en el Código Penal y Leyes Especiales, no puedo conocer de conductas que no estén reguladas en una ley.

PREG.	CATEGORIAS	EVIDENCIAS		
		FISCAL DE LA FISCALIA REGIONAL SANTA ANA.	**PROCURADOR AUXILIAR REGIONAL SANTA ANA.**	**JUEZ DEL TRIBUNAL PRIMERO DE SENTENCIA DE SANTA ANA.**
6	**Ley a utilizar hacia aquellas conductas que lesionan el honor y la intimidad y que según la experiencia en el cargo utilizan los entrevistados de las Instituciones correspondientes.**	Se aplica la LEIV y es de acción pública y se puede iniciar sin el consentimiento de la víctima y contempla la prohibición de cualquier salida alterna no hay conciliación, no hay procedimiento abreviado.	En mi conocimiento por la inexistencia de una ley vigente que regule específicamente este tipo de conductas cometidas a través de un medio como lo es el internet, específicamente las redes sociales, las leyes idóneas que tengan validez utilizaría primeramente la Constitución de la Republica, en segundo lugar el Código Penal y claro para un procedimiento de legal forma el Código Procesal Penal.	Según la Ley Sustantiva Penal conocido también como Derecho Penal Material y es el que se encuentra consagrado en el Código Penal, cabe mencionar que el derecho penal sustantivo es la parte estática o imagen sin movimiento es decir donde solo hay modalidades como Estafa, Hurto, (es decir solo formas de comisión). Con esto es necesario decir que no hay ley especial.

PREG.	CATEGORIAS	EVIDENCIAS		
		FISCAL DE LA FISCALIA REGIONAL SANTA ANA.	**PROCURADOR AUXILIAR REGIONAL SANTA ANA.**	**JUEZ DEL TRIBUNAL PRIMERO DE SENTENCIA DE SANTA ANA.**
7	**Procedimiento, medidas a implementar y criterio profesional a utilizar por los informantes claves ante este tipo de conductas, Procedimiento, medidas a implementar y criterio profesional a utilizar por los informantes claves ante este tipo de conductas.**	Después de la denuncia de la víctima se tiene por ejemplo imágenes, mensajes de texto que se imprimen dentro del Messenger de Facebook se imprimen los diálogos, las imágenes, se brinda el número de teléfono para indagar las bitácoras de llamadas para hacer la interrelación entre la víctima y el supuesto agresor y es lo más que pueden hacer porque no han recibido ni capacitaciones de eso porque es una deuda del Estado.	Debido a la importancia que este tema está tomando en nuestra realidad social, es palpable la necesidad de que exista una mayor divulgación, concientización de lo que en sí son las redes sociales y de la manera idónea de utilizarlas y no solo las redes sociales sino todo lo que se refiere a una cibersociedad actual.	Se pueden cometer este tipo de delitos a través de estos medios pero; no es el criterio que se utiliza, es la prueba esta determinan la presunción de inocencia. Esta debe ser introducida en el Código Procesal Penal en lo referente a este tipo de delitos. Además los organismos encargados de aportar la prueba como la PNC aportan muy poca información en cuanto a este tipo de conductas, razón por la cual deber haber una mejor preparación de todos las partes intervinientes en el proceso.

PREG.	CATEGORIAS	EVIDENCIAS		
		FISCAL DE LA FISCALIA REGIONAL SANTA ANA.	**PROCURADOR AUXILIAR REGIONAL SANTA ANA.**	**JUEZ DEL TRIBUNAL PRIMERO DE SENTENCIA DE SANTA ANA.**
8	**Medidas a implementar por parte de las instituciones correspondientes en este tema y función del Estado Salvadoreño ante los delitos cibernéticos.**	Cada caso es en particular, quizás implementar no en la institución sino más bien crear dentro de la sociedad y luego ir en una escala uno la ciudadanía a que denuncie y dos seria el hecho de poner a la disposición de las instituciones dotar de herramientas de todo tipo se refiere a los insumos que van a tener para terminar la investigación de todo tipo porque de nada sirve iniciar el caso si van a saber que nunca van a poder establecer algunas conductas.	En pro de la defensa del imputado, y de acuerdo a la naturaleza del delito podría desvirtuarse, demostrando la inexistencia del dolo de realizar el daño, que el imputado no es quien vertió el contenido en las red, tomando desde el punto de vista que las herramientas que la institución como la fiscalía y la Policía Nacional Civil poseen no es la idónea para probar los hechos controvertidos.	El Estado como garante de fomentar el resguardo de las garantías de la población debería regular todas aquellas conductas al honor de las personas sin importar, que existen personas que se opone a que sean tuteladas dichas conductas lesivas.

PREG.	CATEGORIAS	EVIDENCIAS		
		FISCAL DE LA FISCALIA REGIONAL SANTA ANA.	**PROCURADOR AUXILIAR REGIONAL SANTA ANA.**	**JUEZ DEL TRIBUNAL PRIMERO DE SENTENCIA DE SANTA ANA.**
9	**Factores que inciden en la impunidad de los delitos relativos a la libertad sexual cometidos por medio de las redes sociales.**	El medio idóneo para establecer que fue cometido a través de internet es un aparato, el decomiso de un aparato pero no se puede privar del uso del aparato porque se estaría violentando su derecho a la intimidad, es algo tan complejo por eso lo que se les piden es que impriman nada mas de sus usuarios sea de WhatsApp, Facebook, Instagran las imágenes, los diálogos, que correspondan al hecho que se está denunciando, generalmente es un ex novio, ex esposo.	No, la realidad es que la institución no los posee, si es difícil, investigar un delito común, debido a los pocos recursos limitados que la institución posee, ya que en las defensas que ejerce la institución el mejor recurso que poseemos es el ingenio y astucia del defensor que está a cargo del caso.	El uso de las redes sociales no está regulado en el Código Penal, tampoco en el Código Procesal Penal, las regulaciones existentes van más orientadas a los delitos de tipo económico cometidos a través de medios informáticos razón por la cual se debe incluir en la Ley Penal un Capítulo específico sobre los Ciberdelitos o la creación y aprobación de una ley especial y por consiguiente una regulación al Código Procesal Penal para determinar un procedimiento que se deba realizar para estos nuevos tipos de delitos.

PREG.	CATEGORIAS	EVIDENCIAS		
		FISCAL DE LA FISCALIA REGIONAL SANTA ANA.	**PROCURADOR AUXILIAR REGIONAL SANTA ANA.**	**JUEZ DEL TRIBUNAL PRIMERO DE SENTENCIA DE SANTA ANA.**
10	**Factores que influyen en la judicialización de los casos relacionados a los ciberdelitos.**	Si se cuenta, la fiscalía tiene una Unidad de Análisis dentro de la fiscalía que es de la que nos auxiliamos conjuntamente con la unidad de análisis de la Policía Nacional Civil pero como les reitero y les dije anteriormente llegan hasta el aparato de donde salió la información hasta ahí establecen ellos.	Lo idóneo no es la creación de una nueva ley, si no crear dentro del Código Penal un apartado, un capitulo que vaya en función de tipificar conductas de esta índole específicamente, por supuesto esto indicaría que el Código Procesal Penal tiene que incluir el proceso para este nuevo capítulo de Ciberdelitos que existiría en el Código Penal, una ley aparte que no reúna un procedimiento adecuado sería seguir caminando en círculo sin pretender solucionar la problemática actual.	Pues hasta donde tengo conocimiento existe un anteproyecto de ley referente a este tipo de delitos pero que en su mayoría van tutelando el patrimonio, razón por la cual a mi criterio de no ponerse de acuerdo en la aprobación de la misma debe realizarse reformas a los artículos así como también una reforma al Código Procesal Penal para incluir los medios de prueba, porque no puede aprobarse una ley sin establecer el procedimiento para judicializarlos, sería como identificar la enfermedad sin tener la cura.

PREG.	CATEGORIAS	EVIDENCIAS		
		FISCAL DE LA FISCALIA REGIONAL SANTA ANA.	**PROCURADOR AUXILIAR REGIONAL SANTA ANA.**	**JUEZ DEL TRIBUNAL PRIMERO DE SENTENCIA DE SANTA ANA.**
11	**La cultura como un obstáculo para conocer de los ciberdelitos por parte de las instituciones competentes.**	Es falta de información y conocimiento, la difusión en la población en general, es importante hay muchas personas que ni siquiera conocen la existencia de la ley, que conductas son las que sancionan creen que eso no es delito entonces es importantísimo la difusión y este tipo de delitos se da en otros niveles porque una persona del campo del área rural por poco conocimiento y poca preparación escolar y con una capacidad social limitada no va a tener a su disposición medios electrónicos.	No es que no existan los casos, no de la forma del funcionamiento, es que las víctimas no lo denuncian por ende, si no hay denuncia, no hay judicialización, no conocemos de este tipo de casos, procuraduría es el último eslabón de la cadena por decirlo de algún modo ya que es la Policía Nacional Civil junto con la Fiscalía General de la República que inician un proceso, si tiene que ver mucho el factor cultura por temor a ser victimizada, a que se sepa, es falta de conocimiento no académico como tal, sino como puede ser ayudada en estos casos.	Todos estamos en las redes pero pocos tienen la conciencia que conlleva el estar en estas, es así que es necesario crear la conciencia del factor cultural del buen uso de las redes sociales por medio de un comportamiento educativo del uso por parte de las personas jóvenes las cuales carecen de conciencia por la falta de factores culturales y educativos, las personas que están a la vanguardia de las redes hay que concientizarlas de la naturaleza de la información que se publica.

CONCLUSIONES.

1. Durante el desarrollo del presente trabajo como equipo de investigación pudimos comprobar que no existe una legislación que regule conductas lesivas cometidas contra el honor y la intimidad usando como medio el internet por tal motivo es necesaria la creación de un cuerpo normativo que regule este tipo de conductas para garantizar la mayor protección de los derechos fundamentales de la persona relacionados al honor y la intimidad que protege la Constitución de la Republica, esta legislación debe ser creada por el Órgano Legislativo dentro de las facultades que les otorga la Constitución de la Republica y le corresponde al Órgano Judicial la aplicación y el cumplimiento de la ley, para poder garantizar el orden jurídico en un Estado de derecho.

2. En base a los resultados obtenidos se pudo constatar en lo concerniente al procedimiento que la Fiscalía General de la Republica está implementando situaciones que versen sobre conductas relativas a la libertad sexual cometidas a través de internet, se pudo observar que las conductas que dañan el honor y la intimidad especialmente de las mujeres están siendo tipificadas en la Ley Especial Integral para una Vida Libre de Violencia para las Mujeres como una forma de violencia de genero situación por la cual los casos no son fundamentados como una conducta lesiva cometida a través de internet sino como una agravante de un tipo penal, por lo que podemos concluir la necesidad de que exista legislación que le dé un tratamiento integral a estas conductas por su medio de cometimiento.

3. Después de realizar el análisis e interpretación el equipo concluye que es necesario la creación no solo de una ley que estipule el catálogo de conductas lesivas que dañen el honor y la intimidad, sino también la creación de un procedimiento específico de este tipo de conductas para dar una mayor

efectividad a la creación de la ley, por lo tanto no es suficiente que exista materialmente una ley sino existe un procedimiento para aplicarla correctamente, esto se debe a lo complejo de estas conductas lesivas cometidas contra el honor y la intimidad usando como medio el internet que necesitan un tratamiento especial en la obtención de los medios probatorios a la hora de judicializarlo para así evitar la impunidad para el elemento activo del delito.

4. Se verifica que la falta de información y preparación del personal de las instituciones del órgano público como del órgano judicial que intervienen en el proceso de judicialización de los casos de conductas relativas a la libertad sexual es indispensable ya que el desconocimiento por parte de ellos conlleva a un mal desempeño en sus funciones en relación a estas conductas y dificulta la efectiva protección de los derechos de la población, por eso es necesario la intervención del Estado en la capacitación del personal de las mismas, ya que son estas las encargadas de garantizar la correcta aplicación y el cumplimiento de la ley así como establecer los límites de uso a las empresas proveedoras que ofertan el servicio de internet en nuestro país.

5. Al realizar el análisis y la correspondiente interpretación de la información obtenida por parte de los informantes claves observamos la falta de importancia del gobierno central de incluir mayor aporte económico por parte a las instituciones encargadas de investigar y judicializar los casos relativos a conductas realizadas a través de internet, quedando en evidencia que la falta de recursos económicos, materiales y humanos imposibilita una efectiva investigación y evitar con esto la impunidad de la mayoría de los casos por no contar con el suficiente personal que responda con características especiales para la investigación en lo relativo a la captación de prueba que es lo fundamental para probar este tipo de conductas.

6. En lo concerniente al factor cultural por parte de la población con respecto a las instituciones que pueden acudir en busca de ayuda judicial por ser víctimas de conductas lesivas cometidas a través de internet se ha identificado que no existe un amplio conocimiento de cuáles son las instituciones públicas o privadas a las que se debe acudir por parte de la población a denunciar estos casos, manifestando que no poseen la suficiente información de las instituciones a la que ellos pueden acudir para que los hechos sean investigados y posteriormente judicializados y que no queden en la impunidad; es por esto que se vuelve importante implementar medidas de divulgación que den a conocer cuáles son las instituciones de gobierno que pueden brindar ayuda en un caso de este tipo y al mismo tiempo surge la necesidad de concientizar a la población de efectuar un buen uso de las redes sociales evitando divulgar información personal en estas y que posteriormente pueda convertirse en el contenido de un hecho que implique una conducta lesiva para su honor e intimidad.

7. Después de haber realizado nuestro trabajo de investigación, como grupo investigador podemos concluir que a pesar del esfuerzo por que se apruebe una legislación que tipifique las conductas lesivas relativas al honor y a la intimidad, el día Jueves 04 de Febrero del año 2016 se aprobó la Ley Especial contra Delitos Informáticos y Conexos donde cabe mencionar se excluyeron los delitos contra el honor y la intimidad cometidos a través de las redes sociales, por lo tanto nos lleva a reforzar nuestra postura en cuanto a que es necesario que se regulen estas conductas cometidas a través de estos medios para evitar la impunidad de estas conductas.

RECOMENDACIONES.

1. Tomando como base todo lo investigado tanto en su fundamento teórico como práctico el equipo encargado de realizar la correspondiente investigación, recomienda que se debe de buscar por parte del gobierno central la creación de una ley especial que regule conductas lesivas cometidas a través de internet o en su defecto agregar un acápite al Código Penal salvadoreño en el cual se describan los tipos penales en base al principio de Legalidad, debido a que la sociedad es cambiante las leyes también deben de serlo con el objetivo de no remitirse a normativa supletoria evitando con esto que los ilícitos queden impunes por falta de una legislación adecuada a la necesidad de la sociedad actual.

2. La Asamblea Legislativa a partir de su misión constitucional debe de reformar el Código Procesal Penal en lo referente a establecer un proceso especifico y adecuado para tutelar las conductas lesivas que se cometen a través de internet, así mismo se debe de establecer los parámetros de medios probatorios tecnológicos para garantizar la efectividad y el cumplimiento dentro del proceso penal de la ley que se crearía y evitar con esto que los procesos queden impunes por falta de un procedimiento que se adecue a las necesidades que estos delitos no convencionales.

3. El Estado debe de implementar mecanismos de formación, inducción y capacitación del personal de las instituciones del ministerio público y del Órgano Judicial intervinientes en el proceso de investigación y judicialización de conductas lesivas a las personas humanas que utilizan como medio de cometimiento el internet a través de las diferentes redes sociales existentes, buscando con esto garantizar la efectividad y cumplimiento de la ley que tutele dichas conductas.

4. Las instituciones del Estado como la Fiscalía General de la Republica, la Procuraduría General de la Republica, Órgano Judicial, deben de crear campañas de divulgación sobre las instituciones que pueden brindar ayuda con el fin de que las personas conozcan en donde pueden abocarse en caso de que sufran de un acto que dañan el honor y la intimidad de su persona, así mismo es necesario la creación de talleres en escuelas e instituciones públicas en realizar un buen uso de las redes sociales y evitar con esto el incremento de casos de las conductas antes descritas.

5. Se debe de buscar por parte de las instituciones del Ministerio Publico y del Órgano Judicial que el Estado le dé más importancia a la política criminal a implementar sobre los casos de ciberdelitos, incluyendo un mayor aporte económico con el fin de dotar de recursos materiales y humanos y que estos posean características especiales como el conocimiento y habilidades encaminadas al desarrollo del procedimiento de investigación debido a la importancia de esta etapa por la naturaleza del delito y lograr con esto su posterior judicialización.

6. Después de haber realizado nuestro trabajo de investigación hemos concluido como investigadores la imperante necesidad por parte del estado salvadoreño de que se suscriba al convenio de Budapest del cual en su oportunidad estuvo como país observador en las reunión realizada en el año 2001, por lo que posteriormente el país debe de suscribir y ratificar el convenio para que pase a formar parte del sistema normativo salvadoreño cumpliendo con esto el compromiso adquirido en su momento.

7. Como grupo de investigación recomendamos anteriormente crear una ley o un acápite en el Código Penal que regule las conductas lesivas contra el honor y la intimidad cometidas a través de internet, y aunque la Ley Especial contra delitos informáticos y conexos fue aprobada, no incluyen los delitos

contra el honor y la intimidad cuando se cometen desde internet, específicamente a través de las Redes Sociales; por lo tanto como grupo de investigación por consiguiente proponemos realizar las reformas respectivas a dicha ley para incluir los delitos que atenten contra el honor y la intimidad que sean cometidos utilizando como medio el internet y las redes sociales.

BIBLIOGRAFIA.

- **Apuntes de clase**. (2013) Lic. Raymundo Alirio Carballo Mejía.
- **Libro de Derecho de Internet.** Anibal, A. (2002). Buenos Aires. El ámbito electrónico y sus formas de comunicación.
- **La Valoración de la Prueba Electrónica.** Eduardo.-, C. d. (2009). Valencia: Tirant to Bllanch.
- **Cibercriminalidad y Derecho Penal 2006.** Gustavo Eduardo Aboso.
- **Revista Justicia de Paz, 163.** Muñoz Campos, M. y. (Diciembre 2002 / Año V-VOL. IV). CORTE SUPREMA DE JUSTICIA.
- **Tesis: La aplicabilidad de la ordenanza para la protección de recursos naturales del municipio de Santa Ana y su concordancia con las normas constitucionales y el debido proceso.** Presentada por Tejada Torres Irene Elizabeth.

NORMAS LEGALES UTILIZADAS.

- **Constitución de la República de El Salvador** Decreto N°38, Diario Oficial N°234, Tomo 281, Fecha de Emisión 15/12/1983 , Fecha de Publicación 16/12/1983.
- **Ley Orgánica Judicial:** decreto**:** N° 123, Diario Oficial N°115,Tomo 283, Fecha de Emisión 06/06/1984, Fecha de Publicación 20/06/1984.
- **Código Penal** Decreto N°1030, Diario Oficial N°105, Tomo 335, Fecha de Emisión 26/04/1997 , Fecha de Publicación 10/06/1997.

- **Código Procesal Penal** Decreto N°733, Diario Oficial N°20, Tomo 382, Fecha de Emisión 22/10/2008 , Fecha de Publicación 30/01/2009.

- **Ley Integral para una Vida Libre de Violencia contra las Mujeres** Decreto N°520, Diario Oficial N°2, Tomo 390, Fecha de Emisión 25/11/2010, Fecha de Publicación 04/01/2011.

- **Ley Orgánica de la Procuraduría General de la República:** Decreto N°775, Diario Oficial N°241, Tomo 381, Fecha de Emisión 03/12/2008 , Fecha de Publicación 22/05/2013.

- **Ley Orgánica de Fiscalía General de la República** Decreto N°1037, Diario Oficial N°95, Tomo 371, Fecha de Emisión 27/04/2006. Fecha de Publicación 25/05/2006.

DIRECCIONES ELECTRONICAS CONSULTADAS.

- **https://es.wikipedia.org/wiki/Sociedad**

- **http://www.cad.com.mx/que_es_una_computadora.html**

- **http://www.nodo50.org/manuales/internet/1.html**

- **http://www.masadelante.com/faqs/twitter**

- **http://www.csj.gob.sv**

- **www.oas.org/juridico/spanish/tratados/a-52.html**

- **www.asamblea.gob.sv**

- **fgip.blgspot.com/2002-11-metodologia-de-al-tesis-politica.html**
- **www.fiscalia.gob.sv**
- **www.pgr.gob.sv**

ANEXOS

MARCO CONCEPTUAL.

ALUSIÓN: Referencia o mención que se hace de una persona o una cosa sin nombrarlos de forma expresa o mencionándolos de manera breve.

ANDROID: es un sistema operativo orientado a dispositivos móviles, basado en una versión modificada del núcleo Linux. Inicialmente fue desarrollado por Android Inc., una pequeña empresa, El android se trata de un sistema abierto, multitarea, que permite a los desarrolladores acceder a las funcionalidades principales del dispositivo mediante aplicaciones, cualquier aplicación puede ser reemplazada libremente, además desarrollarlas por terceros, a través de herramientas proporcionadas por Google, y mediante los lenguajes de programación Java y C.

ANTIVIRUS: son programas de computación cuyo objetivo es detectar, prevenir, desarmar o eliminar virus informáticos o programas maliciosos que quieran interferir con los datos que tenemos en nuestra computadora.

ARCHIVOS: es un fichero informático es un conjunto de bits que son almacenados en un dispositivo. Un archivo es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene. A los archivos informáticos se les llama así porque son los equivalentes digitales de los archivos escritos en expedientes, tarjetas, libretas, papel o micro fichas del entorno de oficina tradicional.

BANCOS DE DATOS: información que contienen datos relativos a diversas temáticas y categorizados de distinta manera, pero que comparten entre sí algún tipo de vínculo o relación que busca ordenarlos y clasificarlos en conjunto, Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

BLOG: Página web, generalmente de carácter personal, con una estructura cronológica que se actualiza regularmente y que se suele dedicar a tratar un tema concreto.

CELULAR: o móvil es un teléfono que funciona sin cables y que puede ser trasladado de un lugar a otro, ya que se conecta a la red de telefonía móvil mediante ondas de radio.

CHAT: Comunicación en tiempo real que se realiza entre varios usuarios cuyas computadoras están conectadas a una red, generalmente Internet; los usuarios escriben mensajes en su teclado, y el texto aparece automáticamente y al instante en el monitor de todos los participantes.

CIBERDELINCUENCIA: La ciberdelincuencia se define con carácter general como cualquier tipo de actividad ilegal en la que se utilice Internet, una red privada o pública o un sistema informático doméstico.

CIBERNAUTAS:persona que mediante un ordenador y a través de la red infor mática Internet accedaccede a bases de datos y secomunica con usuarios conectad os a la misma red en cualquier parte del mundo.

CIBERSOCIEDAD: denominada ordenador u computadora (delfrancés: ordinateur; y este del latín: ordinator), es una máquina electrónica que recibe y procesa datos para convertirlos en información conveniente y útil. Un ordenador está formado, físicamente, por numerosos circuitos integrados y otros muchos componentes de apoyo, extensión y accesorios, que en conjunto pueden ejecutar tareas diversas con suma rapidez y bajo el control de un programa.

CLARO: En El Salvador, la fusión se da en 2004 cuando TELMEX adquiere las acciones de CTE Telecom, que era la empresa de telefonía líder en el país,[4] y que años atrás adquiriera la firma francesa France Télécom. El cambio de nombre se realizó en 2006 en un principio únicamente en el servicio de telefonía móvil y entra con la campaña "Claro que tienes más", los servicios de telefonía fija, pública e Internet seguían denominándose como "Telecom".

COMPUTADORA PERSONAL: ordenador personal, conocida como PC (sigla en inglés de personal computer), es un tipo de microcomputadora diseñada en principio para ser utilizada por una sola persona a la vez. Habitualmente, la sigla PC

se refiere más específicamente a las computadoras IBM PC compatibles. Una computadora personal es generalmente de tamaño medio y es usado por un solo usuario (aunque hay sistemas operativos que permiten varios usuarios simultáneamente, lo que es conocido como multiusuario).

COMUNIDAD VIRTUAL: Conjunto de personas vinculadas por características o intereses comunes, cuyas relaciones e interacciones tienen lugar en un espacio virtual, no físico o real, como Internet.

COMUNIDADES VIRTUALES: Una comunidad virtual es un sitio creado por una o más personas que establecen relaciones a partir de temas comunes. Dialogan, discuten, opinan, mientras su identidad real, incluso su identidad social, puede permanecer oculta. Cada comunidad, llamada también "aldea", elabora un código de acuerdo a las diferentes hablas y procedencias de sus integrantes. “Parece haber en los miembros de estas comunidades una motivación más expresiva que receptiva. Son innumerables los temas que tratan. Sus miembros crean páginas, publican eventos, administran sus foros de discusión, salas de chat, álbumes de fotos, y archivos para compartir. Pueden participar todas aquellas personas que tengan algún interés particular, ganas de comunicar sus pensamientos, intercambiar información, y sentirse parte de un grupo con sus mismos anhelos. El acceso a las "aldeas" es gratuito. Pero en algunos casos se encuentra restringido, ya que existen comunidades "públicas abiertas", "públicas cerradas" o "privadas”. Las comunidades "públicas abiertas" son colocadas en buscadores y los usuarios pueden unirse sin pedir autorización al Fundador. Las comunidades "públicas cerradas" son puestas en buscadores pero el Fundador debe autorizar a los usuarios para que ingresen, enviándoles un código luego de que hayan respondido algunas preguntas.

CONDUCTAS MISÓGINAS: Se define como el odio o la aversión hacia las mujeres o niñas. De acuerdo a la teoría feminista, la misoginia puede manifestarse de diversas maneras, que incluyen denigración, discriminación, violencia contra la mujer, y cosificación sexual de la mujer.

CUENTA: Conjunto de información que permite el acceso a una red social a través de la identificación de usuario. La cuenta se crea con un nombre de usuario y contraseña, en algunos casos, a través de una cuenta de correo electrónico.

DELITO ANALÓGICO: es una conducta delictiva cometida y que no necesitan que el medio de cometimiento reúna características especiales.

DELITOS DE LA RED: delitos cometidos mediante el uso de sistemas informáticos, cuando hablamos del ciberespacio como un mundo virtual distinto a la "vida real", me refiero al delito informático como aquél que está íntimamente ligado a la informática o a los bienes jurídicos que históricamente se han relacionado con las tecnologías de la información:

DELITOS INFORMÁTICOS: es toda aquella acción antijurídica y culpable, que se da por vías informáticas o utilizando dispositivos como computadoras, teléfonos celulares que se tienen que conectar a la red o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet

DEONTOLOGÍA: procede del griego: *to deon* (lo conveniente, lo debido) y *logía* (conocimiento, estudio…); lo que significa, en términos generales, el estudio o la creencia de los hechos. El objeto de estudio de la Deontología son los fundamentos del deber y las normas morales, se aplica fundamentalmente al ámbito de la moral; es decir, a aquellas conductas del hombre que no forman parte de las hipótesis normativas del derecho vigente, aquellas acciones que no están sometidas al control de la legislación pública.

DERECHO A LA INTIMIDAD: El derecho a la intimidad consiste en la defensa de la persona en su totalidad a través de un muro que prohíbe publicar o dar a conocer datos sobre temas como la religión, la política o la vida íntima. La revelación de estos datos conlleva a una pena, en algunos países perpetua y en España de 6 o 7 años. El ser humano tiene derecho absoluto a mantener su vida privada y bajo ningún concepto esto puede ser revelado ni siquiera a una persona muy cercana.

DERECHO PENAL DEMOCRÁTICO: Para que la justicia sea el sustento de la democracia, el derecho penal debe garantizar los derechos fundamentales del

individuo frente al poder arbitrario del Estado. En un Estado de derecho es indispensable el control constitucionales sus leyes, el imperio de la ley como expresión de la voluntad general, la independencia de los poderes legislativo, ejecutivo y judicial, la legalidad de los actos de la administración como mecanismo jurídico anti totalitario y su control judicial, la garantía de las libertades públicas y los derechos fundamentales.

DERECHO PENAL PRINCIPIALISTA: que la legitimación del derecho penal a partir de los principios Constitucionales.

DESARROLLO TECNOLÓGICO: es la Intensificación del empleo de la tecnología para elevar el nivel económico de una región o para proporcionar medios concretos que mejoren el rendimiento de una función o programa de producción.

DIFUSIÓN DE DATOS: Es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

DIGICEL: Digicel Group, más conocido como Digicel o Digicel Caribbean, es una compañía de telecomunicaciones fundada en Bermuda y con sede en Jamaica, opera en gran parte del caribe. La empresa ofrece una variada gama de servicios relacionados con las telecomunicaciones entre los que se incluyen una extensa red de teléfonos móviles y servicio de conexión a internet.

DIRECCIONES IP: Las direcciones IP (IP es un acrónimo para Internet Protocol) son un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP. Una dirección IP (o simplemente IP como a veces se les refiere) es un conjunto de cuatro números del 0 al 255 separados por puntos.

DISCOS MAGNÉTICOS: es una pieza metálica sirve como soporte de almacenamiento de datos para archivos de información, Almacena los bytes de estos archivos en uno o varios sectores

DISPOSITIVOS ELECTRÓNICOS: Consisten en la combinación de diversos elementos organizados en circuitos, destinados a controlar y aprovechar las señales

eléctricas, a diferencia de un dispositivo eléctrico, el cual sirve para controlar y aprovechar el flujo de la corriente eléctrica.

DISPOSITIVOS MÓVILES: Los dispositivos móviles son aparatos de pequeño o gran tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, diseñados específicamente para una función, pero que pueden llevar acabo otras funciones más generales.

DISPOSITIVOS: Un aparato electrónico consiste en una combinación de componentes electrónicos organizados en circuitos, destinados a controlar y aprovechar las eléctricas. Ejemplo de dispositivo electrónico es un amplificador de sonido que controla el flujo de energía de un micrófono hacia los altavoces. También son aparatos electrónicos dispositivos mucho más complejos como puede ser una computadora o un teléfono inteligente.

DOCUMENTOS ELECTRÓNICOS: es un documento electrónico o magnético que contiene un código digital el cual puede: leerse**,** reproducirse**,** interpretarse por cada individuo, se puede manifestar como un medio de expresión y creatividad de cada persona con extensión de algunos medios que se manifiestan en: informática electrónica este documento se queda plasmado y guardado el cual se puede realizar las modificaciones adecuadas en el lenguaje o estructura, este tiene un soporte de contener un mensaje de alfanumérico. Cada individuo realiza lo necesario para el cambio o modificación del texto editándolo y guardándolo con las modificaciones necesarias.

DOMICILIO ELECTRÓNICO: es sitio informático seguro, personalizado, válido y optativo, registrado por los ciudadanos, empresas o representantes, para la entrega o recepción de comunicaciones de cualquier naturaleza y eventualmente para el cumplimiento de obligaciones fiscales, es por medio de este que los usuarios realizan pagos por utilizar la red.

E-MAIL: Correo electrónico es un servicio de red que permite a los usuarios reenviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante sistemas de comunicación electrónica.

ENLACES: Un enlace o link es texto o imágenes en un sitio web que un usuario puede pinchar para tener acceso o conectar con otro documento. Los enlaces son como la tecnología que conecta dos sitios web o dos páginas web. En el navegador se ven como palabras subrayadas (como *Ir al índice de FAQ's* al final de ésta página). Es hasta 2009 que la empresa cambia totalmente su nombre a Claro El Salvador, y todos sus servicios pasan a identificarse con ese nombre y se da la incursión de Claro TV con servicio de Televisión por cable.

ESTADO: Información de la situación, circunstancia o disposición del usuario de una red social. Esta información puede ser compartida por el propio usuario, o por la plataforma de comunicación de manera automática, indicando su disponibilidad o actividad en ese momento.

EVENTO: Acontecimiento creado como una publicación o mensaje que se anuncia a otros usuarios de la red social para que participen del mismo.

EXTRATERRITORIALIDAD: Ficción jurídica, admitida en Derecho internacional, por la cual un edificio o un terreno se considera en país extranjero, como una prolongación del país propietario, como en el caso de las embajadas, consulados, bases militares y, en ciertos aspectos, los buques.

FACEBOOK: es una red social creada por Mark Zuckerberg mientras estudiaba en la universidad de Harvard. Su objetivo era diseñar un espacio en el que los alumnos de dicha universidad pudieran intercambiar una comunicación fluida y compartir contenido de forma sencilla a través de Internet. Fue tan innovador su proyecto que con el tiempo se extendió hasta estar disponible para cualquier usuario de la red.

FICHEROS: es un archivo, o sistema real o virtual de organización de la información mediante una clasificación determinada, se le llama fichero a un conjunto de información clasificada y almacenada de diversas formas para su conservación y fácil acceso a ellas

GRUPO: Servicio que proporcionan las redes sociales para la configuración de colectivos de usuarios con un interés u objetivo común. Los grupos permiten crear espacios donde los miembros pueden compartir información y contenidos de forma privada o abierta.

HARDWARE: Se refiere a todas las partes físicas de un sistema informático; sus componentes son eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

HASHTAG: Etiqueta de Twitter para clasificar las publicaciones o mensajes (tweets) por temas específicos. Se representa mediante una almohadilla (#) delante de la palabra o palabras clave del tema dentro del cual se etiqueta el mensaje, con la finalidad de seguir, buscar y encontrar más fácilmente los temas interesantes para el usuario. Por ejemplo, #Educación o #TIC, para los mensajes que se etiquetan en estos temas

HECHO PUNIBLE: acción sancionada por el Derecho con una pena, también es denominado conducta delictiva, hecho penal o acción punible. El hecho punible se identifica con el delito penal que según Carrara implica una contradicción entre un hecho humano, positivo o negativo, y una ley que lo condena. Este hecho debe provocar un daño y ser imputable moralmente. La ley que los castiga tiene por objeto proteger la seguridad pública.

HI (FIVE): o Hi5 como red social brinda la posibilidad de crear un perfil, una página con la información personal, con gustos, aficiones e intereses, permitiendo buscar así personas afines. La red cuenta con afiliados que brindan juegos, desarrollados externamente pero que se pueden jugar a través de la plataforma de

Hi5.Asi mismo, mientras los usuarios navegan, las empresas afiliadas muestran avisos de sus productos y servicios, de acuerdo a la ubicación del usuario.

INALIENABLE: Se aplica al derecho que no puede ser negado o quitado a una persona. Ejemplo: la libertad es un derecho inalienable del ser humano.

INFORMACIÓN VIRTUAL: en la informática y la tecnología es utilizado para referirse a la realidad construida mediante sistemas o formatos digitales y la transferencia de información que se produce en estos.

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

INHERENTE: Que es esencial y permanente en un ser o en una cosa o no se puede separar de él por formar parte de su naturaleza y no depender de algo externo. Que por su naturaleza está de tal manera unido a algo, que no se puede separar de ello.

INSIDER TRADING: Expresión Anglosajona que corresponde a un acto delictivo referido al uso de información privilegiada con la que conseguir beneficios no habituales mediante inversiones en los mercados financieros realizada por empleados de la administración pública o de empresas.

INSTAGRAM: es una red social y aplicación para compartir fotos y videos. Permite a los usuarios aplicar efectos fotográficos como filtros, marcos, similitudes térmicas, áreas subyacentes en las bases cóncavas, colores retro y vintage, y posteriormente compartir las fotografías en diferentes redes sociales como Facebook, Tumblr, Flickr y Twitter.

INTERCOMUNICACIÓN GLOBAL: La intercomunicación es la capacidad y la necesidad de transmisión reciproca de información, datos, conocimientos, experiencias entre dos o más personas, seres vivos, lugares o mecanismos. Para conseguir una buena intercomunicación es necesaria la existencia de un medio óptimo de conexión entre el transmisor y el receptor. Ya sea un medio natural o

mediante infraestructuras artificiales, cuantos más medios se posean mejor y más eficientes será la capacidad de intercomunicación.

INTERNET: Red informática de nivel mundial que utiliza la línea telefónica para transmitir la información.

LESIVO: Que causa o puede causar daño o perjuicio.

MEDIO DE COMUNICACIÓN: Un medio de comunicación es el elemento o el modo utilizado para poder llevar a cabo cualquier tipo de comunicación. En regla general, cuando se mencionan los medios de comunicación se está refiriendo directamente a aquellos medios que son de carácter masivo**,** es decir, aquellos cuya comunicación se extiende a las masas. Sin embargo, existen medios comunicacionales que se establecen en grupos reducidos de personas y que son de carácter exclusivamente interpersonal.

MEDIOS INFORMÁTICOS: Son un Conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión digitalizados de la información

MEDIOS TECNOLÓGICOS: Son un conjunto de procedimientos y estrategias que se utilizan como recursos didácticos en el proceso de enseñanza- aprendizaje para optimizar el proceso de formación profesional promoviendo aprendizaje altamente significativos.

MENOSCABO: Mengua o descrédito en la honra o la fama de una persona.

MENSAJERÍA MULTIMEDIA: El término multimedia se utiliza para referirse a cualquier objeto o sistema que utiliza múltiples medios de expresión (físicos o digitales) para presentar o comunicar información. De allí la expresión «multimedios». Los medios pueden ser variados, desde texto e imágenes, hasta animación, sonido, video.

MESSENGER: es el nombre con el que se conocía popularmente al programa informático Windows Live Messenger. Este software, creado por Microsoft, permitía la comunicación instantánea entre dos o más usuarios. El Messenger podía usarse en una computadora **(**ordenador**)** o desde ciertos dispositivos móviles. Pese a que fue creado como un cliente de chat (para intercambiar mensajes escritos en tiempo real), el programa fue creciendo hasta convertirse en un software muy completo que facilitaba todo tipo de comunicaciones e intercambio de archivos..

MODUS OPERANDI: que literalmente significa 'modo de operar', es una expresión latina de uso frecuente tanto en español como en otras lenguas occidentales. En el lenguaje común, esta expresión se refiere a la manera habitual o característica de actuar de una persona o de un grupo, y puede ser utilizada en numerosos contextos: organizacional, logístico, profesional y científico

MOVISTAR: en el Salvador es la filial de la empresa española Telefónica. Movistar opera en el salvador a través de Telefónica Móviles El Salvador y Movistar Empresas. Actualmente es, junto a las empresas Tigo y Claro, de las mayores operadoras de Telecomunicaciones del país.

MURO: Espacio del usuario de una red social que comparte con el resto de sus contactos, donde estos pueden publicar sus comentarios u opiniones

NODOS O CENTRALES: Definimos genéricamente como Nodo a cada uno de los espacios reales o abstractos en el cual se confluyen las conexiones de otros espacios, compartiendo sus mismas características y siendo también un Nodo, teniendo una relación entre sí y conformando entonces lo que conocemos como Red.Es por ello que a veces notamos que el término de Red es definido bajo el concepto de Conjunto de Nodos Interconectados, siendo entonces éste un punto en el cual una conexión puede realizar una intersección sobre sí misma, estableciendo una especie de enlace. De esta manera, si tenemos lo que es conocido como Red de Computadoras, debemos tener en cuenta que cada uno de los ordenadores forma parte de un nodo, y el conjunto de ellas, o más precisamente el punto donde estas se cruzan entre sí, es el establecimiento de una Red determinada.

ON-LINE: Expresión inglesa que se traduce por las locuciones en línea o a través de Internet.

ORDENADORES: El ordenador (del inglés: computer; y este del latín: computare, 'calcular'), también denominada ordenador3 1 u computadora4 5 (del francés: ordinateur; y este del latín: ordinator), es una máquina electrónica que recibe y procesa datos para convertirlos en información conveniente y útil. Un ordenador está formado, físicamente, por numerosos circuitos integrados y otros muchos componentes de apoyo, extensión y accesorios, que en conjunto pueden ejecutar tareas diversas con suma rapidez y bajo el control de un programa.

PASSWORD: en español significa Contraseña**,** es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa. En sistemas multiusos, las contraseñas ayudan a asegurar que los usuarios desautorizados no tengan acceso al ordenador

PERFIL CON DATOS PERSONALES: Los datos personales implican toda aquella información inherente a una persona y que como tal permiten identificarlo conforme, es decir, le aportan una existencia real.
Entre estos datos podemos destacar: el nombre y apellido, la fecha y el lugar de nacimiento, edad, domicilio real, teléfono, estado civil, nombres y apellidos de sus progenitores, situación laboral, estudios cursados, por citar aquellos que están signados como datos personales básicos de una persona.

PERFIL DE USUARIO: En sentido general, un perfil de usuario es un conjunto de datos que se refieren al usuario de un servicio informático. Un modelo de usuario es una fuente de conocimientos que contiene adquisiciones sobre todos los aspectos del usuario que pueden ser útiles para el comportamiento del sistema. Los perfiles de usuarios se utilizan en informática en numerosos ámbitos. Permiten prestar servicios personalizados, adaptar ofertas, etc.

PERFIL: Datos personales y rasgos propios que caracterizan a un usuario dentro de una red social, como su nombre, fotografía, lugar de residencia o preferencias. El perfil representa su identidad virtual.

POST: Entrada, mensaje o publicación en una red social que puede consistir en un texto, opinión, comentario, enlace o archivo compartido.

PRINCIPIO DE LA DIGNIDAD HUMANA: La dignidad humana es el derecho que tiene cada ser humano, de ser respetado y valorado como ser individual y social, con sus características y condiciones particulares, por el solo hecho de ser persona.

PRINCIPIO DE LESIVIDAD: Implica que ningún derecho puede legitimar una intervención punitiva cuando no media por lo menos un conflicto jurídico, entendido como la afectación de un bien jurídico total o parcialmente ajeno, individual o colectivo.

PROBLEMA SOCIO JURÍDICO: estima la eficacia del derecho en sociedad. Se abordan problemas sobre la técnica jurídica, la implementación del derecho; entiende el derecho como un instrumento para el desarrollo y la solución de problemas sociales.

PRUEBA ELECTRÓNICA: En materia penal es un medio de convencer al juez sobre la existencia de un hecho punible, mediante el rastro de hechos actuados o constantes en medios electrónicos como pueden ser mensajes de texto actuados en celulares y ordenadores.

PUERTO USB: es la sigla de Universal Serial Bus (Bus Universal en Serie**,** en castellano). Se trata de un concepto de la informática para nombrar al puerto que permite conectar periféricos o dispositivos a una computadora, permitiendo el fácil intercambio de datos y la ejecución o intercambio de datos y la ejecución de operaciones. Típicamente, los dispositivos que utilizan USB pueden ser teclado, mouse, impresora, teléfonos móviles, cámaras, escáner entre otros

PUNTO DE VISTA CONSECUENCIALISTA: es decir por el grado de afectación que puede llegar a producirse sobre un determinado bien y que afecte el grado de satisfacción que este le cauce a la persona.

PUNTO DE VISTA PRINCIPIALISTA: es decir visto desde el punto de vista de principios enmarcados en la constitución.

RED : red de computadoras también llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios

REDES DE CONMUTACIÓN DE CIRCUITOS: es un tipo de conexión que realizan los diferentes nodos de una red para lograr un camino apropiado para conectar dos usuarios de una red de telecomunicaciones. A diferencia de lo que ocurre en la conmutación de paquetes, en este tipo de conmutación se establece un canal de comunicaciones dedicado entre dos estaciones. Se reservan recursos de transmisión y de conmutación de la red para su uso exclusivo en el circuito durante la conexión. Ésta es transparente: una vez establecida parece como si los dispositivos estuvieran realmente conectados.

REDES DE CONMUTACIÓN DE PAQUETES: es un método de envío de datos en una red de computadoras. Un paquete es un grupo de información que consta de dos partes: los datos propiamente dichos y la información de control, que indica la ruta a seguir a lo largo de la red hasta el destino del paquete. Existe un límite superior para el tamaño de los paquetes; si se excede, es necesario dividir el paquete en otros más pequeños.

REDES SOCIALES: es una estructura social compuesta por un conjunto de actores (tales como individuos u organizaciones) que están relacionados de acuerdo a algún criterio (relación profesional, amistad, parentesco, etc.). Servicio de red social, es un medio de comunicación social que se centra en establecer un contacto

con otras personas por medio de Internet. Están conformadas por un conjunto de equipos, servidores, programas, conductores, transmisores, receptores y sobre todo por personas que comparten alguna relación, principalmente de amistad, donde mantienen intereses y actividades en común, o se encuentran interesados en explorar los intereses y las actividades de otros usuarios. Red social, Página web en la que los internautas intercambian información personal y contenidos multimedia de modo que crean una comunidad de amigos virtual e interactiva.

SABOTAJE INFORMÁTICO: una conducta que afecta el bien jurídico intermedio de la información, sí se afirma que lesiona directamente el patrimonio económico destinado a actividades laborales. En muchos países ya se consideran las bases de datos

SEGUIDOR: Llamado follower en la terminología de Twitter. Usuario de esta red social que se suscribe a los mensajes o publicaciones (tweets) de otros usuarios, bien por admiración, como en el caso de los seguidores de deportistas o cantantes; por simpatizar con sus ideas; por mantenerse informado de sus actividades en Twitter; o, simplemente, por amistad. Este seguimiento o suscripción no es necesariamente recíproco.

SISTEMA: Un sistema informático (SI) es un sistema que permite almacenar y procesar información; es el conjunto de partes interrelacionadas: hardware, software y personal informático.

SISTEMAS TELEMÁTICOS: La telemática se trata de un conjunto de métodos que resultan de usar conjuntamente las telecomunicaciones y la informática. Un sistema telemático se encarga de interconectar ordenadores, terminales, switch, Reuter, usando algún medio adecuado como el cable del teléfono, coaxiales, fibra. Cada vez que conectamos dos equipos informáticos separados por una distancia y realizamos una transmisión de datos, estaremos hablando de un sistema telemático. No solo se compone de un ordenador y un cable o wifi sino que, detrás de todo eso, hay una información codificada que hay que convertir y los dispositivos que realizan esas funciones, también están dentro de la definición.

SITIOS WEB: es un lugar que sirve para algo o un espacio ocupado(o que puede llegar a serlo). La noción de web, por su parte, hace referencia a internet, una red de redes que permite la interconexión de computadoras mediante un conjunto de protocolos denominado TCP/IP. Un sitio web por lo tanto, es un espacio virtual en internet. Se trata de un conjunto de páginas web que son accesibles desde un mismo dominio subdominio de la world wide web (www).

SMARTPHONE: el término Smartphone pertenece a la lengua inglesa y hace referencia a aquello que, en nuestro idioma, conocemos como teléfono inteligente. Se trata de un teléfono celular (móvil) que ofrece prestaciones similares a las que brinda una computadora (ordenador) y que se destaca por su conectividad. Es habitual que se ubique al Smartphone a mitad de camino entre un teléfono celular convencional y una computadora portátil. El Smartphone cuenta con todas las funciones básicas del celular (permite realizar llamadas telefónicas, enviar mensajes de texto, etc.) y le agrega características avanzadas (conexión a Internet, capacidad multimedia, pantalla táctil).

SOCIEDAD JURÍDICAMENTE ORGANIZADA: es El Estado, es la sociedad política y jurídicamente organizada capaz de imponer la autoridad de la ley en el interior y afirmar su personalidad y responsabilidad frente a las similares del exterior.

SOFTWARE: Al equipo lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

SOLICITUD DE AMISTAD: Mensaje enviado a otro usuario como petición para pertenecer a su lista de contactos, y viceversa. Una vez recibida la solicitud, el usuario puede aceptar y agregar un nuevo contacto para compartir con él su contenido e información.

SUJETO ACTIVO: es la persona individual con capacidad penal que realiza la conducta típica. Solamente una persona individual puede cometer delitos, aún en los casos de asociación criminal, las penas recaen sólo en sus miembros integrantes.

Solo en la persona individual se da la unidad de voluntad y el principio de individualidad de la pena.

SUJETO PASIVO: es el titular del interés jurídico lesionado o puesto en peligro.

TABLET: Es un término de la lengua inglesa que no forma parte del diccionario de la Real Academia Española **(**RAE**).** El concepto puede traducirse como tableta**,** aunque las acepciones de esta noción mencionadas por la RAE no coinciden con el significado actual. Una tablet, en definitiva, es una computadora (ordenador) portátil más grande que un smartphone pero más pequeña que una netbook. Se caracteriza por contar con pantalla táctil: esto quiere decir que para utilizar la tablet no se necesita mouse (ratón) ni teclado.

TECNOLOGIA: es el conjunto de conocimientos técnicos, científicamente ordenados, que permiten diseñar, crear bienes, servicios que facilitan la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de la humanidad.

TIGO: fue lanzado en El Salvador en agosto de 2004, como parte de un proceso de integración de la marca nacional TELEMOVIL con las internacionales, siendo el mayor operador de telefonía móvil del país, contando con más de 2.1 millones de usuarios. Tigo compite con operadores regionales como Claro (América Móvil), Movistar (Telefónica) y Digicel (Digicel Group). Provee servicios sobre redes AMPS/TDMA y GSM/GPRS, en 800 y 850 MHz respectivamente. El 28/08/2008 Tigo lanzó comercialmente el servicio de 3G con UMTS/HSDPA en 850 MHz.Actualmente opera con los servicios residenciales de la empresa Amnet. Actualmente propiedad de millicom.

TIPIFICAR: Ajustar varias cosas semejantes a un tipo o norma común. En la legislación penal o sancionatoria, definir una acción u omisión concretas, a las que se asigna una pena o sanción.

TRANSMITIR INFORMACIÓN: es la recepción y transmisión de datos entre las miles redes de ordenadores que componen Internet, el cual se lleva a cabo mediante el empleo de un conjunto de protocolos de comunicaciones

TRENDING TOPIC: Tema popular en un momento determinado, en relación al número de publicaciones o mensajes (tweets) que se hacen sobre él en Twitter.

TWEET: Mensaje o publicación de 140 caracteres que se escribe y envía a los usuarios seguidores mediante la red social de microblogging Twitter. También existe el Retweet (RT) que es, sencillamente, el reenvío de un tweet. **TWITTER:** un término inglés que puede traducirse como "gorjear" o **"**trinar**"**, es el nombre de una reddemicroblogging que permite escribir y leer mensajes en Internet que no superen los 140caracteres. Estas entradas son conocidas como tweets**.**

UPDATES: es utilizado justamente para el vocablo en español destinado a la Actualización, que implica la modificación de datos tanto en un archivo como en una base de datos o en una explicación en general, siendo generalmente asociada a la palabra "Parche" que también es empleada como sinónimo.

USUARIO: Persona o entidad que utiliza y forma parte de una red social. El usuario puede acceder a ella con su propio nombre o mediante un alias, aunque con la revolución de la Web 2.0 se aprecia un cambio en el que los usuarios se identifican con nombres reales. En la red social de microblogging Twitter, la cuenta y perfil adoptan el nombre real, pero sus miembros identifican sus actividades en la red mediante un nombre de usuario que puede ser diferente, similar o idéntico a su nombre real, y que, además, añade delante de éste el símbolo @. Por ejemplo, la red social docente Internet en el aula tiene como nombre de usuario en Twitter @rediaula, y Educación INTEF el nombre @educacion_intef.

UTÓPICO: se denomina la idea, ideación o representación de una civilización ideal, fantástica, imaginaria e irrealizable, paralela o alternativa al mundo actual.El término utopía también puede designar aquel proyecto o doctrina que se considera

idóneo, pero inviable o de difícil puesta en práctica: “utopía comunista”, “utopía anarquista”.En este sentido, como utopía también se puede considerar un modo optimista de concebir cómo nos gustaría que fuera el mundo y las cosas: “Sé que es una utopía la manera en que propongo que funcione el país”.

WEFT QDA: cuyo significado de sus siglas en ingle es paquete gratuito de código abierto para el análisis de datos cualitativos o de textos no estructurado).un programa de computación para investigaciones cualitativas tiene un conjunto de herramientas para administrar datos que con tres funciones básica: Guarda los datos en forma organizada (categorías analísticas ó demográficas suministradas por el investigador), Busca y Clasifica los datos (entrevistas, notas de campo, documentos, reflexiones, observaciones, etc.) en categorías analíticas establecidas por el investigador. Establece relaciones con los datos a través de diversas búsquedas, Permite visualizar las búsquedas en forma de textos o cuadros de doble entrada.

DECRETO Nº 520

LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR,

CONSIDERANDO:

I.- Que la Constitución reconoce a la persona humana como el origen y el fin de la actividad del Estado, que está organizado para la consecución de la justicia, de la seguridad jurídica y del bien común. En consecuencia es obligación del Estado asegurar a las personas habitantes de la República, el goce de la libertad, la salud, la cultura, el bienestar económico y la justicia social. Así mismo, el artículo 144, establece que los tratados internacionales celebrados por El Salvador con otros Estados o con organismos internacionales, constituyen leyes de la República.

II.- Que mediante Decreto Legislativo Nº 430, de fecha 23 de agosto de 1995, publicado en el Diario Oficial Nº 154, Tomo Nº 328, de esa misma fecha, se ratificó la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer, "Convención Belem do Pará", la cual establece la obligación a los Estados parte, de incluir en su legislación interna normas penales, civiles y administrativas; así como, las de otra naturaleza que sean necesarias para prevenir, sancionar y erradicar la violencia contra la mujer.

III.- Que es necesario contar con una legislación que regule de manera adecuada la política de detección, prevención, atención, protección, reparación y sanción, para la erradicación de todas las formas de violencia contra las mujeres y el respeto de sus derechos humanos como una obligación del Estado; se vuelve indispensable, la introducción de un instrumento legal que oriente adecuadamente, las actuaciones públicas y privadas a favor de las mujeres, y que garantice, una mejor calidad de vida y un adelanto en sus capacidades de manera integral.

IV.- Que las violaciones de los derechos humanos derivadas de las diferentes formas de violencia que afectan la vida, integridad y seguridad ciudadana, tienen un impacto diferenciado según el género de las víctimas; ya que toda agresión perpetrada contra una mujer, está directamente vinculada con la desigual distribución del poder y con las relaciones asimétricas entre mujeres y hombres en la sociedad.

V.- Que las desigualdades de poder entre hombres y mujeres perpetuadas a través de la violencia, no le permiten a la mujeres ejercer plenamente sus derechos en el campo social, político, económico, cultural y familiar, negándoseles el acceso a una vida libre de violencia, lo cual constituye una violación de sus derechos humanos y libertades fundamentales; en razón de lo cual es necesario, legislar de manera integral a través de medidas que incluyan la detección, prevención, atención, protección, reparación y sanción de la violencia contra las mujeres en

cualquiera de sus manifestaciones.

POR TANTO,

en uso de sus facultades constitucionales, y a iniciativa de las Diputadas y Diputados: Lorena Guadalupe Peña Mendoza, Irma Lourdes Palacios Vásquez, Federico Guillermo Ávila Qüehl, Ana Lucía Baires de Martínez, Eduardo Enrique Barrientos Zepeda, Carmen Elena Calderón Sol de Escalón, José Alvaro Cornejo Mena, Nery Arely Díaz de Rivera, Margarita Escobar, Emma Julia Fabián Hernández, Carmen Elena Figueroa Rodríguez, Gloria Elizabeth Gómez de Salgado, Hortensia Margarita López Quintana, Mario Marroquín Mejía, Manuel Vicente Menjívar Esquivel, Mariella Peña Pinto, Sonia Margarita Rodríguez Sigüenza, Ana Silvia Romero, Sandra Marlene Salgado García, Rodrigo Samayoa Rivas, Manuel Rigoberto Soto Lazo, Enrique Alberto Luis Valdés Soto, Donato Eugenio Vaquerano Rivas, Margarita Velado; con adhesión a la misma de las Diputadas y Diputados: Lucía del Carmen Ayala de León, Patricia María Salazar Mejía, Patricia Elena Valdivieso de Gallardo; y con el apoyo a la misma de las Diputadas y Diputados: José Francisco Merino López, Alberto Armando Romero Rodríguez, Francisco Roberto Lorenzana Durán,César Humberto García Aguilera, Elizardo González Lovo, Roberto José d'Aubuisson Munguía, Karla Gisela Abrego Cáceres, Félix Agreda Chachagua, Ernesto Antonio Angulo Milla, Marta Lorena Araujo, José Orlando Arévalo Pineda, Fernando Alberto José Ávila Quetglas, Ana Lucía Baires de Martínez, Reynaldo Antonio López Cardoza, José Vidal Carrillo Delgado, Darío Alejandro Chicas Argueta, Norma Cristina Cornejo Amaya, Carlos Cortez Hernández, Blanca Noemí Coto Estrada, Rosa Alma Cruz de Henríquez, Ana Vilma Castro de Cabrera, Omar Arturo Escobar Oviedo, José Rinaldo Garzona Villeda, Medardo González Trejo, José Nelson Guardado Menjivar, Iris Marisol Guerra Henríquez, Norma Fidelia Guevara de Ramirios, Carlos Walter Guzman Coto, Gladis Marina Landaverde Paredes, Mildred Guadalupe Machado Argueta, Segundo Alejandro Dagoberto Marroquín, Ana Guadalupe Martínez Menéndez, Heidy Carolina Mira Saravia, Edgar Alfonso Montoya Martínez, Rafael Ricardo Moran Tobar, Ana Virginia Morataya Gómez, Yeimi Elizabeth Muñoz Moran, José Margarito Nolasco Díaz, María Irma Elizabeth Orellana Osorio, Rubén Orellana, Rafael Eduardo Paz Velis, Mario Antonio Ponce López, Zoila Beatriz Quijada Solís, Carlos René Retana Martínez, David Ernesto Reyes Molina, Javier Ernesto Reyes Palacios, Dolores Alberto Rivas Echeverría, Gilberto Rivera Mejía, Jackeline Noemí Rivera Avalos, Pedrina Rivera Hernández, Cesar René Florentín Reyes Dheming, Luis Enrique Salamanca Martínez, Marcos Francisco Salazar Umaña, Karina Ivette Sosa de Lara, Jaime Gilberto Valdez Hernández, Mario Eduardo Valiente Ortiz, Guadalupe Antonio Vásquez Martínez, Ana Daysi Villalobos de Cruz, Francisco José Zablah Safie, Ciro Alexis Zepeda Menjivar,

DECRETA la siguiente:

LEY ESPECIAL INTEGRAL PARA UNA VIDA LIBRE DE VIOLENCIA PARA LAS MUJERES

Título I
Garantía y Aplicación de la ley

Capítulo I
Disposiciones Preliminares
Artículo 1.- Objeto de la Ley

La presente ley tiene por objeto establecer, reconocer y garantizar el derecho de las mujeres a una vida libre de violencia, por medio de Políticas Públicas orientadas a la detección, prevención, atención,

protección, reparación y sanción de la violencia contra las mujeres; a fin de proteger su derecho a la vida, la integridad física y moral, la libertad, la no discriminación, la dignidad, la tutela efectiva, la seguridad personal, la igualdad real y la equidad.

Articulo 2.- Derecho de las Mujeres a una Vida Libre de Violencia

El derecho de las mujeres a una vida libre de violencia comprende, ser libres de toda forma de discriminación, ser valoradas y educadas libres de patrones estereotipados de comportamiento, prácticas sociales y culturales basadas en conceptos de inferioridad o subordinación.

Así mismo, se refiere al goce, ejercicio y protección de los derechos humanos y las libertades e consagradas en la Constitución y en los Instrumentos Nacionales Internacionales sobre la materia vigentes, incluido el derecho a:

2. Que se respete su vida y su integridad física, psíquica y moral.

3. Que se respete la dignidad inherente a su persona y se le brinde protección a su familia.

4. La libertad y a la seguridad personal.

5. No ser sometida a tortura o tratos humillantes.

6. La igualdad de protección ante la ley y de la ley.

7. Un recurso sencillo y rápido ante los tribunales competentes que la amparen frente a hechos que violen sus derechos.

8. La libertad de asociación.

9. Profesar la religión y las creencias.

10. Participar en los asuntos públicos incluyendo los cargos públicos.

Artículo 3.- Ámbito de Aplicación

La presente ley se aplicará en beneficio de las mujeres que se encuentren en el territorio nacional, sean éstas nacionales o no, o que teniendo la calidad de salvadoreñas, estén fuera del territorio nacional, siempre que las acciones u omisiones de que trata la presente ley puedan ser perseguidas con base en parámetros de extraterritorialidad.

Artículo 4.- Principios Rectores

Los principios rectores de la presente ley son:

3. **Especialización:** Es el derecho a una atención diferenciada y especializada, de acuerdo a las necesidades y circunstancias específicas de las mujeres y de manera especial, de

aquellas que se encuentren en condiciones de vulnerabilidad o de riesgo.

4. **Favorabilidad:** En caso de conflicto o duda sobre la aplicación de las disposiciones contenidas en la presente ley, prevalecerá la más favorable a las mujeres que enfrentan violencia.

5. **Integralidad:** Se refiere a la coordinación y articulación de las Instituciones del Estado para la erradicación de la violencia contra la mujer.

6. **Intersectorialidad:** Es el principio que fundamenta la articulación de programas, acciones y recursos de los diferentes sectores y actores a nivel nacional y local, para la detección, prevención, atención, protección y sanción, así como para la reparación del daño a las víctimas.

7. **Laicidad:** Se refiere a que no puede invocarse ninguna costumbre, tradición, ni consideración religiosa para justificar la violencia contra la mujer.

8. **Prioridad absoluta:** Se refiere al respeto del derecho de las mujeres a una vida libre de violencia, en cualquier ámbito.

Artículo 5.- Sujetos de Derechos

La presente ley se aplicará en beneficio de las mujeres, sin distinción de edad, que se encuentren en el territorio nacional; para ello se prohíbe toda forma de discriminación, entendida ésta, como toda distinción, exclusión, restricción o diferenciación arbitraria basada en el sexo, la edad, identidad sexual, estado familiar, procedencia rural o urbana, origen étnico, condición económica, nacionalidad, religión o creencias, discapacidad física, psíquica o sensorial, o cualquier causa análoga, sea que provenga del Estado, de sus agentes o de particulares.

Artículo 6.- Sujetos Obligados

Son sujetos obligados para efectos de esta ley, toda persona natural o jurídica, que se encuentre o actúe en territorio salvadoreño, quienes deberán cumplir y hacer cumplir las disposiciones de esta ley, cualquiera que fuese su nacionalidad, domicilio o residencia.

Artículo 7.- Relaciones de Poder o de Confianza

Para la aplicación e interpretación de esta ley, se presume que los tipos y modalidades de violencia contemplados en la presente ley, tienen como origen la relación desigual de poder o de confianza; en la cual, la mujer se encuentra en posición de desventaja respecto de los hombres, consistiendo las mismas en:

5. **Relaciones de poder:** Son las caracterizadas por la asimetría, el dominio y el control de una o varias personas sobre otra u otras.

3 **Relaciones de confianza:** Son las que se basan en los supuestos de lealtad, credibilidad, honestidad y seguridad que se establecen entre dos o más personas.

La desigualdad en las relaciones de poder o confianza pueden subsistir, aun cuando haya finalizado el vínculo que las originó, independientemente del ámbito en que se hayan llevado a cabo.

Artículo 8.- Definiciones

Para efectos de esta ley se entenderá por:

11. **Atención Integral:** Son todas las acciones para detectar, atender, proteger y restablecer los derechos de las mujeres que enfrentan cualquier tipo de violencia; para lo cual, el Estado deberá destinar los recursos humanos, logísticos y financieros necesarios y apropiados para instaurar los servicios especializados, que garanticen la restitución de derechos y la anulación de riesgos o daños ulteriores.

12. **Acoso Laboral:** Es la acción de hostilidad física o psicológica, que de forma sistemática y recurrente, se ejerce sobre una mujer por el hecho de ser mujer en el lugar de trabajo, con la finalidad de aislar, intimidar o destruir las redes de comunicación de la persona que enfrenta estos hechos, dañar su reputación, desacreditar el trabajo realizado o perturbar u obstaculizar el ejercicio de sus labores.

13. **Desaprendizaje:** Es el proceso mediante el cual una persona o grupo de personas, desestructura o invalida lo aprendido por considerarlo susceptible de cuestionamiento o inapropiado para su propio desarrollo y el de la comunidad a la que pertenece.

14. **Misoginia:** Son las conductas de odio, implícitas o explícitas, contra todo lo relacionado con lo femenino tales como rechazo, aversión y desprecio contra las mujeres.

15. **Persona Agresora:** Quien ejerce cualquiera de los tipos de violencia contra las mujeres, en una relación desigual de poder y en cualquiera de sus modalidades.

16. **Prevención:** Son normas y políticas para reducir la violencia contra las mujeres interviniendo desde las causas identificadas de la misma, y cuyo objetivo es evitar su reproducción y reducir la probabilidad de aparición del problema; por tanto, se dirigen a transformar el entorno del riesgo y a fortalecer las habilidades y condiciones de las personas y comunidades para su erradicación, asegurando una identificación rápida y eficaz, así como la reducción de los impactos y secuelas cuando se presente el problema y reincidencia.

17. **Publicidad Sexista:** Es cualquier forma de publicidad que transmita valores, roles, estereotipos, actitudes, conductas femeninas y masculinas, lenguaje verbal y no verbal, que fomenten la discriminación, subordinación, violencia y la misoginia.

18. **Reaprendizaje:** Es el proceso a través del cual las personas, asimilan un conocimiento

o conducta luego de su deconstrucción androcéntrica, a partir de una visión crítica y no tradicional como producto de las nuevas relaciones establecidas con su entorno social natural.

a. **Revictimizar:** Son acciones que tienen como propósito o resultado causar sufrimiento a las víctimas directas o indirectas de los hechos de violencia contemplados o no en la presente ley, mediante acciones u omisiones tales como: rechazo, indolencia, indiferencia, descalificación, minimización de hechos, retardo injustificado en los procesos, falta de credibilidad, culpabilización, desprotección, negación y falta injustificada de asistencia efectiva.

b. **Sexismo:** Es toda discriminación que se fundamenta en la diferencia sexual que afecta toda relación entre seres humanos y abarca todas las dimensiones cotidianas de la vida privada o pública que define sentimientos, concepciones, actitudes y acciones.

c. **Violencia contra las Mujeres:** Es cualquier acción basada en su género, que cause muerte, daño o sufrimiento físico, sexual o psicológico a la mujer tanto en el ámbito público como privado.

d. **Víctima Directa:** Se refiere a toda mujer a quien se le vulnere el derecho a vivir libre de violencia, independientemente de que se denuncie, individualice, aprehenda, enjuicie o condene a la persona agresora.

e. **Víctima Indirecta:** Es toda persona a quien se le vulnere el derecho a vivir una vida libre de violencia o que sufra daños al intervenir para asistir a la víctima directa o prevenir su victimización, indistintamente del tipo de relación que exista entre ellas.

Artículo 9.- Tipos de Violencia

Para los efectos de la presente ley, se consideran tipos de violencia:

c. **Violencia Económica:** Es toda acción u omisión de la persona agresora, que afecta la supervivencia económica de la mujer, la cual se manifiesta a través de actos encaminados a limitar, controlar o impedir el ingreso de sus percepciones económicas.

d. **Violencia Feminicida:** Es la forma extrema de violencia de género contra las mujeres, producto de la violación de sus derechos humanos, en los ámbitos público y privado, conformada por el conjunto de conductas misóginas que conllevan a la impunidad social o del Estado, pudiendo culminar en feminicidio y en otras formas de muerte violenta de mujeres.

e. **Violencia Física:** Es toda conducta que directa o indirectamente, está dirigida a ocasionar daño o sufrimiento físico contra la mujer, con resultado o riesgo de producir lesión física o daño, ejercida por quien sea o haya sido su cónyuge o por quien esté o haya estado ligado a ella por análoga relación de afectividad, aun sin convivencia.

Asimismo, tendrán la consideración de actos de violencia física contra la mujer, los ejercidos por la persona agresora en su entorno familiar, social o laboral.

13. **Violencia Psicológica y Emocional:** Es toda conducta directa o indirecta que ocasione daño emocional, disminuya el autoestima, perjudique o perturbe el sano desarrollo de la mujer; ya sea que esta conducta sea verbal o no verbal, que produzca en la mujer desvalorización o sufrimiento, mediante amenazas, exigencia de obediencia o sumisión, coerción, culpabilización o limitaciones de su ámbito de libertad, y cualquier alteración en su salud que se desencadene en la distorsión del concepto de sí misma, del valor como persona, de la visión del mundo o de las propias capacidades afectivas, ejercidas en cualquier tipo de relación.

14. **Violencia Patrimonial:** Son las acciones, omisiones o conductas que afectan la libre disposición del patrimonio de la mujer; incluyéndose los daños a los bienes comunes o propios mediante la transformación, sustracción, destrucción, distracción, daño, pérdida, limitación, retención de objetos, documentos personales, bienes, valores y derechos patrimoniales. En consecuencia, serán nulos los actos de alzamiento, simulación de enajenación de los bienes muebles o inmuebles; cualquiera que sea el régimen patrimonial del matrimonio, incluyéndose el de la unión no matrimonial.

15. **Violencia Sexual:** Es toda conducta que amenace o vulnere el derecho de la mujer a decidir voluntariamente su vida sexual, comprendida en ésta no sólo el acto sexual sino toda forma de contacto o acceso sexual, genital o no genital, con independencia de que la persona agresora guarde o no relación conyugal, de pareja, social, laboral, afectiva o de parentesco con la mujer víctima.

16. **Violencia Simbólica:** Son mensajes, valores, iconos o signos que transmiten y reproducen relaciones de dominación, desigualdad y discriminación en las relaciones sociales que se establecen entre las personas y naturalizan la subordinación de la mujer en la sociedad.

Artículo 10.- Modalidades de Violencia

Para los efectos de la presente ley, se consideran modalidades de la Violencia:

14. **Violencia Comunitaria:** Toda acción u omisión abusiva que a partir de actos individuales o colectivos transgreden los derechos fundamentales de la mujer y propician su denigración, discriminación, marginación o exclusión.

15. **Violencia Institucional:** Es toda acción u omisión abusiva de cualquier servidor público, que discrimine o tenga como fin dilatar, obstaculizar o impedir el goce y disfrute de los derechos y libertades fundamentales de las mujeres; así como, la que pretenda obstaculizar u obstaculice el acceso de las mujeres al disfrute de políticas públicas destinadas a prevenir, atender, investigar, sancionar y erradicar las manifestaciones, tipos y modalidades de violencia conceptualizadas en esta ley.

5 **Violencia Laboral:** Son acciones u omisiones contra las mujeres, ejercidas en forma repetida y que se mantiene en el tiempo en los centros de trabajo públicos o privados, que constituyan agresiones físicas o psicológicas atentatorias a su integridad, dignidad personal y profesional, que obstaculicen su acceso al empleo, ascenso o estabilidad en el mismo, o que quebranten el derecho a igual salario por igual trabajo.

Artículo 11.- Interpretación

Esta ley se interpretará y se aplicará en concordancia con las disposiciones de la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer, la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer, la Convención sobre los Derechos del Niño, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y su Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y los demás Instrumentos Internacionales de Derechos Humanos vigentes.

Capítulo II

Rectoría

Artículo 12.- Institución Rectora y su Objeto

El Instituto Salvadoreño para el Desarrollo de la Mujer es la Institución rectora de la presente ley; y su objeto es:

418 Asegurar, vigilar y garantizar el cumplimiento y ejecución integral de la ley.

419 Coordinar las acciones conjuntas de las instituciones de la administración pública para el cumplimiento de la Política Nacional para el Acceso de las Mujeres a una Vida Libre de Violencia.

420 Formular las Políticas Públicas para el Acceso de las Mujeres a una Vida Libre de Violencia, a los Órganos del Estado, Instituciones Autónomas y Municipales.

421 Convocar en carácter consultivo o de coordinación a organizaciones de la sociedad civil, universidades, organismos internacionales y de cooperación.

Artículo 13.- Funciones y Atribuciones del Instituto Salvadoreño para el Desarrollo de la Mujer

En la presente ley el Instituto Salvadoreño para el Desarrollo de la Mujer, tiene las siguientes atribuciones:

1 Elaborar una política marco que será la referente para el diseño de las políticas públicas a que se refiere la presente ley.

2 Presentar propuestas a las instituciones del Estado de Políticas Públicas para el Acceso de las Mujeres a una Vida Libre de Violencia.

3 Aprobar, modificar, monitorear, evaluar y velar por el cumplimiento de la Política Nacional para el Acceso de las Mujeres a una Vida Libre de Violencia, que se define en la presente ley.

4 Definir estrategias y gestionar ante la situación de emergencia nacional o local, a efecto de prevenir y detectar hechos de violencia contra las mujeres.

5 Rendir informe anual al Órgano Legislativo sobre el estado y situación de la violencia contra las mujeres de conformidad con esta ley y con los compromisos internacionales adquiridos en esta materia.

6 Establecer mecanismos y acciones de coordinación y comunicación con los Órganos del Estado, Alcaldías Municipales y otras Instituciones Autónomas.

7 Efectuar evaluaciones y recomendaciones sobre la aplicación de la presente ley.

8 Otras acciones que sean indispensables y convenientes para el mejor desempeño de sus objetivos, el adecuado cumplimiento de esta ley o que se le atribuyan en otras leyes.

Artículo 14.- Comisión Técnica Especializada

Para garantizar la operativización de la presente ley y la de las Políticas Públicas para el Acceso de las Mujeres a una Vida Libre de Violencia, se crea la Comisión Técnica Especializada, cuya coordinación estará a cargo del Instituto Salvadoreño para el Desarrollo de la Mujer y estará conformada por una persona representante de cada institución que forma parte de la junta directiva de dicho Instituto, así como una persona representante de las siguientes instituciones:

16. Órgano Judicial.

17. Ministerio de Hacienda.

18. Ministerio de Gobernación.

19. Ministerio de Relaciones Exteriores.

20. Ministerio Economía.

21. Una persona designada por la Presidencia de la República.

22. Ministerio de Agricultura y Ganadería.

Artículo 15.- Integrantes de la Comisión Técnica Especializada

Para ser integrante de la Comisión Técnica Especializada, las personas representantes de cada una de las instituciones, deberán cumplir con el perfil siguiente:

20. Demostrable honorabilidad.

21. No haber sido condenado por delitos, en los últimos diez años.

22. Especialización en materia de derechos de las mujeres.

23. Sensibilización en el respeto y cumplimiento a los derechos humanos de las mujeres.

Las Funciones de la Comisión Técnica, se establecerán en base a un instructivo de trabajo formulado por las instituciones que la integran y deberá estar en concordancia con la Política Nacional para el Acceso de las Mujeres a una Vida Libre de Violencia.

Capítulo III
Política Nacional para el Acceso de las Mujeres a una Vida Libre de Violencia Artículo 16.-

Política Nacional para el Acceso de las Mujeres a una Vida Libre de Violencia

La Política Nacional para el Acceso de las Mujeres a una Vida Libre de Violencia, en adelante Política Nacional, es el conjunto de objetivos y estrategias de naturaleza pública que tiene como finalidad garantizar el derecho de las mujeres a una vida libre de violencia, a través de su prevención, detección, atención y protección. Su Plan de Acción tendrá un período de cinco años.

Artículo 17.- Contenidos de la Política Nacional para el Acceso de las Mujeres a una Vida Libre de Violencia

La Política Nacional, deberá contener programas de:

2. Detección, que tengan como fin la identificación temprana y focalización de los factores que originan los hechos de violencia contra las mujeres tanto en el ámbito público como privado, estableciendo modelos de detección de acuerdo a los tipos y modalidades de violencia contempladas en la presente ley.

3. Prevención, que tengan como fin evitar la violencia contra las mujeres en cualquiera de sus tipos y modalidades, a partir del desaprendizaje de los modelos convencionales que históricamente han sido atribuidos a la imagen y al concepto de las mujeres, y del reaprendizaje de nuevos modelos basados en principios de igualdad, equidad, diversidad y democracia.

12. Atención, que tengan como fin atender, proteger y restablecer, de forma expedita y eficaz, los derechos de las víctimas directas e indirectas de cualquier tipo de violencia ejercida contra las mujeres, tanto en el ámbito público como privado.

13. Protección, que tengan como fin atender y favorecer de manera integral los derechos de las mujeres víctimas de violencia, ya sea que se encuentren o no en situación de riesgo.

14. Erradicación de la violencia contra las mujeres, que tengan como fin la desestructuración de las prácticas, conductas, normas y costumbres sociales y culturales que vayan en detrimento de la identidad, dignidad e integridad física y emocional de las mujeres, o que las sitúen en condiciones de vulnerabilidad.

15. Seguridad ciudadana, a través del diseño de estrategias que promuevan espacios públicos seguros para las mujeres, la creación de mapas de ubicación de violencia territorial, redes ciudadanas nacionales y locales, así como instituciones que participen activamente en la detección y prevención de la violencia contra las mujeres.

16. Formación y capacitación, que facilite la inserción laboral y la generación de ingresos a mujeres que enfrenten hechos de violencia.

17. Desarrollo de estudios e investigaciones sobre violencia contra las mujeres a nivel nacional.

Así mismo, la Política Nacional, para su cumplimiento e implementación deberá contener programas de sensibilización, conocimiento y especialización para el personal prestatario de servicios para la detección, prevención, atención y protección de los casos de violencia contra las mujeres, así como Protocolos de Actuación y Coordinación con las diferentes Instituciones del Estado.

Artículo 18.- Del cumplimiento y articulación de la Política Nacional para el Acceso de las Mujeres a una Vida Libre de Violencia

Las Instituciones del Estado de acuerdo a sus competencias, deberán adoptar y ejecutar los programas y acciones de erradicación de la violencia contra las mujeres establecidas en la Política Nacional.

Artículo 19.- Participación Ciudadana

Los mecanismos de participación y representación ciudadana a nivel nacional y local, deberán incluir dentro de sus normativas o reglamentos, acciones para erradicar la violencia contra las mujeres en coherencia con la Política Nacional.

Capítulo IV
Responsabilidades del Estado

Sección Primera
Responsabilidades Ministeriales

Artículo 20.- Responsabilidades en el Ambito Educativo

El Ministerio de Educación a través de los programas y procesos educativos de enseñanza-aprendizaje formales y no formales, en los niveles de educación: parvulario, básica, media, superior y no universitaria, incluirá dentro de la obligación que tiene de planificar y normar de manera integral la formación de las personas educadoras, así como en las actividades curriculares y extracurriculares, la promoción del derecho de las mujeres a vivir libre de violencia y de discriminación, así como la divulgación de las medidas destinadas a la prevención y erradicación de cualquier tipo de violencia contra las mujeres, fomentando para tal efecto las relaciones de respeto, igualdad y promoción de los derechos humanos de las mujeres.

Así mismo, deberán eliminar de todos los programas educativos las normativas, reglamentos y materiales que promuevan directa o indirectamente cualquiera de las formas de violencia contra las mujeres, los esquemas de conducta, prejuicios y costumbres estereotipadas que promuevan, legitimen, naturalicen, invisibilicen y justifiquen la violencia contra las mujeres, para lo cual, el Ministerio de Educación deberá garantizar que los contenidos de todos los materiales que circulan dentro del sistema educativo cumplan con lo establecido en la presente ley.

Las personas que ejerzan la dirección de los centros educativos públicos y privados, deberán adoptar las medidas necesarias para la detección y atención de los actos de violencia contra las mujeres dentro del ámbito escolar, de conformidad con lo establecido en la Política Nacional.

Artículo 21.- Educación Superior

El Ministerio de Educación, en el ámbito de Educación Superior, garantizará en los estudios universitarios de grado y en los programas de postgrado relacionados con los ámbitos de esta ley, conocimientos orientados a la prevención e investigación para la erradicación de la violencia contra las mujeres y el fomento de las relaciones de igualdad y no discriminación.

Las instituciones de educación superior deberán reglamentar internamente las acciones de detección y prevención de toda forma de violencia contra la mujer.

Artículo 22.- Responsabilidades del Ministerio de Gobernación

El Ministerio de Gobernación a través de:

a. La Dirección General de Espectáculos Públicos de Radio y Televisión, protegerá y defenderá, la imagen de las mujeres en el más amplio sentido conforme a los principios constitucionales de respeto a la dignidad humana y los derechos fundamentales.

Garantizando para tal fin, que los anunciantes, medios de comunicación y agencias de publicidad, incluidos los electrónicos, informáticos y telemáticos, cuya actividad esté

sometida al ámbito de la publicidad y comunicaciones, no difundan contenidos, ni emitan espacios o publicidad sexista contra las mujeres, considerándose ésta, cuando se promueva la agresividad, malos tratos o discriminación contra las mujeres, la salud, la dignidad y la igualdad.

Para el cumplimiento de lo anterior, el Ministerio de Gobernación, por medio de la Dirección General de Espectáculos Públicos de Radio y Televisión, garantizará la observancia y aplicación de los Códigos de Ética de los medios de comunicación.

e. El Sistema Nacional de Protección Civil, Prevención y Mitigación de Desastres a través de la Comisión Nacional de Protección Civil, Prevención y Mitigación de Desastres, deberá garantizar que en las situaciones de riesgo y desastre, la atención a las mujeres se diseñe y ejecute tomando en cuenta su condición de vulnerabilidad de género y las necesidades propias de su sexo, para lo cual se deberán incorporar acciones y medidas de prevención, atención y protección de las diferentes modalidades de violencia contra las mujeres, en el Plan Nacional de Protección Civil, Prevención y Mitigación de Desastres.

Entre otras, podrán adoptarse las medidas siguientes:

25. Establecer espacios físicos segregados de hombres y mujeres para prevenir situaciones de violencia.

26. Atención sanitaria, médica y psicosocial que tome en cuenta el entorno de riesgo de violencia y necesidades específicas de las mujeres.

27. Exclusión de potenciales personas agresoras que muestren conductas de violencia, hostigamiento y acoso hacia las mujeres.

28. Establecer procedimientos administrativos para la entrega equitativa de recursos acorde a las responsabilidades que afrontan las mujeres.

Artículo 23.- Responsabilidades del Ministerio de Salud Pública y Asistencia Social

El Ministerio de Salud Pública y Asistencia Social, será el responsable de:

26. Garantizar las medidas específicas en el ámbito de los servicios de salud pública, para la prevención, detección temprana, atención e intervención en los casos de violencia contra las mujeres.

27. Incorporar las medidas necesarias para el seguimiento y evaluación del impacto en la salud de las mujeres afectadas por la violencia, dando especial atención a la salud mental y emocional.

28. La prevención y detección temprana de las situaciones de violencia contra las mujeres, será un objetivo en el ámbito de los servicios de salud pública.

a. Garantizar la no discriminación de las mujeres en cuanto al acceso de los servicios de salud, así mismo, que el personal de salud no ejerza ningún tipo de violencia a las usuarias de los servicios, sin que anteponga sus creencias, ni prejuicios durante la prestación de los mismos.

b. Registrar estadísticamente casos de violencia contra las mujeres manifestados a través de enfermedades, accidentes y padecimientos atendidos dentro del servicio de salud pública.

c. Elaborar un informe anual relativo al número de mujeres que han sido atendidas e identificadas en situaciones de violencia, el cual se remitirá al Comité Técnico Especializado y al Sistema Nacional de Datos y Estadísticas.

d. Garantizar el cumplimiento en todo el Sistema Nacional de Salud, de las Normativas Internas en materia de procedimientos de atención para mujeres, así como, el conocimiento y acceso de las mismas a esos procedimientos.

Artículo 24.- Responsabilidades del Ministerio de Trabajo y Previsión Social

El Estado, a través del Ministerio de Trabajo y Previsión Social, tanto en el sector público como privado, garantizará:

30. La realización en los centros de trabajo de acciones de sensibilización y prevención de cualquier tipo de violencia contra las trabajadoras, que afecten sus condiciones de acceso, promoción, retribución o formación.

31. Que las ausencias o faltas de puntualidad al trabajo motivadas por la situación física o psicológica derivada de cualquier tipo de violencia, tengan la consideración de justificadas.

32. La protección de los derechos laborales de las trabajadoras que enfrentan hechos de violencia.

En los casos en que las mujeres se encuentren en ciclos de violencia y procesos de denuncia, si así lo solicitaren, se gestionará con el patrón la reubicación temporal o permanente de su lugar de trabajo, en el caso de las empresas que tienen sucursales; así como, la reorganización de sus horarios, en los términos que se determinen en los Convenios Laborales, Tratados Internacionales y legislación vigente.

Artículo 25.- Creación de Unidades Institucionales de Atención Especializada para las Mujeres

Créanse las Unidades Institucionales de Atención Especializada para las mujeres que enfrentan hechos de violencia, cuya finalidad será brindar servicios integrales en condiciones higiénicas y de privacidad, con atención con calidad y calidez, con prioridad a la atención en crisis; así como también, asesorar e informar sobre los derechos que les asisten, las medidas relativas a su protección y seguridad, los servicios de emergencia y acogida, incluido la del lugar de prestación de estos servicios y el estado en que se encuentran las actuaciones jurídicas o administrativas de sus denuncias.

Existirá una unidad de atención especializada en las siguientes instituciones y en sus correspondientes delegaciones departamentales:

1. Órgano Judicial.

2. Fiscalía General de la República.

3. Procuraduría General de la República.

4. Procuraduría para la Defensa de los Derechos Humanos.

5. Policía Nacional Civil.

6. Instituto de Medicina Legal.

7. Ministerio de Salud Pública y Asistencia Social.

8. Otras que tengan competencia en la materia.

El Instituto Salvadoreño para el Desarrollo de la Mujer será el encargado de velar y supervisar que la atención de las unidades sea prestada de la manera prevista en el inciso primero del presente artículo.

Artículo 26.- Casas de Acogida

Créase el programa de Casas de Acogida, que estará bajo la coordinación y supervisión del Instituto Salvadoreño para el Desarrollo de la Mujer, cuyos servicios podrán ser prestados, además del Estado y las municipalidades, por organizaciones no gubernamentales de protección a mujeres y la sociedad civil, debidamente acreditados por dicho Instituto, los cuales tendrán como objetivo:

32. Atender a las mujeres y su grupo familiar afectado que se encuentran en riesgo y desprotección generadas por situaciones de violencia, referidas por las Instituciones Gubernamentales y no gubernamentales facultadas por esta ley.

33. Asegurar el apoyo inmediato, la integridad física, emocional y la atención psicosocial.

Sección Segunda
Otras Instituciones Educadoras

Artículo 27.- Otras Instituciones

Las Instituciones del Estado directamente responsables de la detección, prevención, atención, protección y sanción de la violencia contra las mujeres, deberán formar integralmente a su personal en conocimientos sobre el derecho de las mujeres a una vida libre de violencia y de discriminación, así como, sobre la divulgación de las medidas destinadas a la prevención y erradicación de cualquier forma de violencia, fomentando para tal efecto las relaciones de respeto, igualdad y promoción de sus derechos

humanos.

Dentro de estas instituciones se encuentran comprendidas:

33. Academia Nacional de Seguridad Pública.
34. Consejo Nacional de la Judicatura.
35. Fiscalía General de la República.
36. Instituto de Medicina Legal.
37. Procuraduría General de la República.
38. Procuraduría para la Defensa de los Derechos Humanos.
39. Unidad Técnica Ejecutiva del Sector Justicia.
40. Ministerio de Salud Pública y Asistencia Social.
41. Corte Suprema de Justicia.
42. Escuela Penitenciaria.
43. Asamblea Legislativa.
44. Ministerio de Educación.
45. Centros de Formación Municipal.
46. Escuela Militar.
47. Otras instituciones que lleven a cabo procesos de educación superior especializada, no formal.

Dichas instituciones garantizarán que la formación de su personal capacitador sea sistemática y especializada en la sensibilización, prevención y atención de las mujeres que enfrentan hechos de violencia. Dichos capacitadores, deberán conocer y transmitir el enfoque de género, enfatizando en las causas estructurales de la violencia contra las mujeres, las causas de desigualdad de relaciones de poder entre hombres y mujeres, y las teorías de construcción de las identidades masculinas.

Artículo 28.- Responsabilidades de Instituciones Colegiadas

El Instituto Salvadoreño para el Desarrollo de la Mujer, fomentará programas formativos con el objeto de promover la formación especializada, sensibilización e investigación en los colegios profesionales, entidades de desarrollo científico, universidades y organizaciones no gubernamentales; en especial, de

las áreas social, jurídica y sanitaria. Asimismo, velará para que los colectivos, facilitadores e investigadores desarrollen los procesos de manera eficaz y por personas que por su trayectoria, garanticen conocimientos y valores coherentes con los objetivos de esta ley.

Capítulo V
De los Concejos Municipales

Artículo 29.- Concejos Municipales

Los Concejos Municipales, para la aplicación de la presente ley, de acuerdo a las facultades y atribuciones conferidas por el Código Municipal, desarrollarán acciones coherentes con esta ley y con la Política Nacional, tales como:

d) Elaborar cada tres años, el Plan Municipal para la Prevención y Atención de la Violencia contra las Mujeres, el cual deberá dar cumplimiento a lo establecido en la Política Nacional para el Acceso de las Mujeres a una Vida Libre de Violencia.

e) Convocar y articular a las instituciones y organizaciones locales, para generar acciones de coordinación, intercambio de información y colaboración para el cumplimiento de su Plan Municipal.

f) Establecer dentro de su presupuesto una partida etiquetada para la ejecución de su Plan Municipal y rendir informe anual sobre el mismo, a los y las ciudadanas de sus municipios y al Instituto Salvadoreño para el Desarrollo de la Mujer.

g) Remitir al Ministerio de Justicia y Seguridad Pública, los datos y estadísticas sobre los casos de violencia contra las mujeres de los cuales tienen conocimiento.

Los Concejos Municipales no podrán mediar o conciliar ningún tipo o modalidad de violencia contra las mujeres.

Capítulo VI
Sistema Nacional de Datos, Estadísticas e Información de Violencia Contra las Mujeres

Artículo 30.- Sistema Nacional de Datos y Estadísticas

El Ministerio de Justicia y Seguridad Pública, será el responsable de manejar el Sistema Nacional de Datos, Estadísticas e Información de violencia contra las mujeres, en adelante S istema Nacional de Datos y Estadísticas; que deberá coordinar con la Dirección General de Estadísticas y Censos. Dicha Dirección, será la encargada de solicitar y recibir la información del resto de instituciones que posean y procesen datos, estadísticas o información sobre hechos de violencia contra las mujeres.

Los informes de dicho Sistema deberán contener:

g) Sistema de indicadores.

m) Evaluación del impacto de las políticas que se desarrollen para la erradicación de cualquier tipo de violencia contra las mujeres, y de las acciones que se implementen, para garantizar la atención integral a aquellas que la hayan enfrentado.

n) Datos según ubicación geográfica de ocurrencia del hecho o hechos; así como, la procedencia territorial, edad, ocupación, estado familiar y nivel de escolaridad de las mujeres que han enfrentado hechos de violencia y de la persona agresora.

o) Datos de los hechos atendidos, como tipos, ámbitos y modalidades de la violencia contra las mujeres, frecuencia, tipos de armas o medios utilizados para ejecutar la violencia, medidas otorgadas y el historial del proceso judicial.

p) Efectos causados por la violencia contra las mujeres.

q) Datos relativos al número de mujeres que han enfrentado hechos de violencia atendidas en los centros y servicios hospitalarios, educativos, centros de trabajo y recurrencia de los diferentes sectores de la economía.

r) Las referencias hechas a otras instancias.

s) Los recursos erogados para la atención de las mujeres que han enfrentado hechos de violencia.

t) Otros que se consideren necesarios.

El Ministerio de Justicia y Seguridad Pública, deberá publicar anualmente los resultados de la sistematización de datos sobre los hechos de violencia contra las mujeres, mediante la presentación de informes en medios impresos y electrónicos, los cuales deberán estar disponibles a solicitud de cualquier persona natural o jurídica que así lo requiera.

Artículo 31.- Finalidad y Conformación del Sistema Nacional de Datos, Estadísticas e Información de Violencia Contra las Mujeres

La finalidad del Sistema Nacional de Datos y Estadísticas, será garantizar la base nacional de datos de hechos de violencia contra las mujeres, para lo cual deberá recopilar y homologar los datos estadísticos e información brindada, para cuyo efecto el Ministerio de Justicia y Seguridad Pública en coordinación con la Dirección General de Estadísticas y Censos, tendrán la obligación de solicitar la información pertinente a las Instituciones correspondientes; así como, la de rendir mensualmente la información que se solicite.

Artículo 32.- Informe de Indicadores de Violencia Contra las Mujeres

El Instituto de Medicina Legal, anualmente deberá presentar indicadores diagnósticos basados en los peritajes realizados que deberán incluir:

34. La prevalencia de casos de Feminicidio.

35. Los efectos de la violencia física, psíquica y sexual en las mujeres que enfrentan hechos de violencia.

36. Los efectos de la exposición a la violencia y de las agresiones sufridas por los hijos, hijas, niñas, niños o adolescentes, a cargo de la mujer que enfrenta hechos de violencia.

37. Valoración de la incidencia, la peligrosidad objetiva y el riesgo de reincidencia de la persona agresora.

Capítulo VII
Presupuesto, Finanzas y Fondo Especial

Artículo 33.- Presupuesto

Los recursos para financiar la presente ley serán los siguientes:

1 Las asignaciones de las partidas del Presupuesto General de la Nación, que deberán consignar cada año o aquellos recursos etiquetados en materia de violencia contra las mujeres en cualquiera de sus modalidades, a cada una de las instancias públicas facultadas por esta ley.

2 Aquellos fondos especiales destinados para mujeres víctimas de violencia.

3 Donaciones nacionales e internacionales.

4 Cooperaciones regionales o internacionales.

5 Otras fuentes de financiamiento nacional o internacional.

Artículo 34.- Financiamiento para la Aplicación de la Presente Ley

El Estado a través del Ministerio de Hacienda, deberá garantizar para la ejecución de la presente ley la asignación de partidas presupuestarias etiquetadas en el Presupuesto General de la Nación para cada año, a cada una de las instituciones públicas facultadas en esta ley para su aplicación.

Artículo 35.- Fondo Especial para Mujeres Víctimas de Violencia

Los fondos obtenidos por las sanciones económicas impuestas por infracciones cometidas a la presente ley, ingresarán al Fondo General de la Nación; y el Ministerio de Hacienda, deberá trasladarlos íntegramente para financiar aquellos proyectos a que se refiere esta ley.

Artículo 36.- Fiscalización de Fondos

Corresponderá a la Corte de Cuentas de la República, la fiscalización posterior de la correcta

utilización de los fondos asignados para la ejecución de la presente ley.

Capítulo VIII
Protección de la Vivienda

Artículo 37.- Ayudas Sociales y Subsidio

Las ayudas sociales o subsidios, serán compatibles con cualquiera de las previstas en las leyes vigentes con programas sociales; y provendrán, del Fondo Especial para mujeres víctimas de violencia.

Artículo 38.-Acceso a Vivienda Social para Mujeres

Las mujeres sujetas a esta ley, serán consideradas colectivos prioritarios en el acceso a viviendas sociales protegidas y programas, en los términos que determine la legislación vigente, valorando sus circunstancias y el contexto de desprotección y de vulnerabilidad.

Artículo 39.- Protección del Uso de Vivienda Arrendada

En los casos y hechos de violencia contra la mujer por su pareja, y éste arriende la vivienda de habitación, la mujer podrá continuar con el uso de la misma por orden judicial mediante la medida de protección correspondiente. Lo anterior no exime del pago de los cánones de arrendamiento, al que deberá ser condenado la persona agresora.

Dicha medida, se notificará a la persona agresora y al arrendatario, para que la mujer haga uso de la vivienda hasta por un plazo máximo de noventa días desde que fue notificada la resolución judicial correspondiente, acompañando de la copia de dicha resolución judicial o de la parte de la misma, que afecte el uso de la vivienda al arrendante.

Artículo 40.- Acceso a la Vivienda

El Ministerio de Obras Públicas, a través del Viceministerio de Vivienda y Desarrollo Urbano, del Fondo Social para la Vivienda (FSV), y del Fondo Nacional de Vivienda Popular (FONAVIPO), deberá elaborar una Política de Vivienda que progresivamente incorpore una reserva de viviendas específica para mujeres que enfrentan hechos violencia, y que se encuentren en total desprotección y condiciones de alto riesgo. Siendo prioridad las mujeres adultas mayores y las mujeres con discapacidades.

Artículo 41.- Habitación Tutelada

La habitación tutelada, consiste en espacios de vivienda temporal bajo la figura de la vivienda en protección pública para mujeres que se encuentran en ciclos de violencia y que hayan establecido dicha situación.

Los espacios de vivienda temporal, serán garantizados por el Estado; para lo cual, deberá emitir un Reglamento que regule el procedimiento para que las mujeres que establezcan la situación de violencia, puedan tener acceso a la habitación tutelada.

Artículo 42.- Certificación de Denuncia

Las Instituciones obligadas por esta ley, garantizarán a las mujeres que enfrentan hechos de violencia, el derecho a obtener la certificación de denuncia, la cual deberá ser expedida dentro del término establecido por la ley.

El funcionario o funcionaria que incumpliere con esta obligación incurrirá en una sanción equivalente a diez salarios mínimos establecidos para trabajadores del comercio y servicios vigente, sin perjuicio de la responsabilidad penal correspondiente.

Artículo 43.- Establecimiento de la Situación de Violencia

En los casos en que así lo requieran, o que se exija el establecimiento de la situación de violencia contra las mujeres para el reconocimiento de sus derechos, ésta se acreditará, sin perjuicio de lo establecido para cada caso, a través de:

1 Certificación de resolución judicial por cualquier tipo y modalidad de violencia.

2 Certificación que acredite la atención especializada, por un organismo público competente en materia de violencia.

Título II
Delitos y Sanciones

Capítulo I
Delitos y Sanciones

Artículo 44.- Delitos de Acción Pública

Todos los delitos contemplados en el presente capítulo son de acción pública.

Artículo 45.- Feminicidio

Quien le causare la muerte a una mujer mediando motivos de odio o menosprecio por su condición de mujer, será sancionado con pena de prisión de veinte a treinta y cinco años.

Se considera que existe odio o menosprecio a la condición de mujer cuando ocurra cualquiera de las siguientes circunstancias:

c. Que a la muerte le haya precedido algún incidente de violencia cometido por el autor contra la mujer, independientemente que el hecho haya sido denunciado o no por la víctima.

d. Que el autor se hubiere aprovechado de cualquier condición de riesgo o vulnerabilidad física o psíquica en que se encontraba la mujer víctima.

7 Que el autor se hubiere aprovechado de la superioridad que le generaban las relaciones desiguales de poder basadas en el género.

8 Que previo a la muerte de la mujer el autor hubiere cometido contra ella cualquier conducta calificada como delito contra la libertad sexual.

9 Muerte precedida por causa de mutilación.

Artículo 46.- Feminicidio Agravado

El delito de feminicidio será sancionado con pena de treinta a cincuenta años de prisión, en los siguientes casos:

38. Si fuere realizado por funcionario o empleado público o municipal, autoridad pública o agente de autoridad.

39. Si fuere realizado por dos o más personas.

40. Si fuere cometido frente a cualquier familiar de la víctima.

41. Cuando la víctima sea menor de dieciocho años de edad, adulta mayor o sufriere discapacidad física o mental.

42. Si el autor se prevaleciere de la superioridad originada por relaciones de confianza, amistad, doméstica, educativa o de trabajo.

Artículo 47.- Obstaculización al Acceso a la Justicia

Quien en el ejercicio de una función pública propiciare, promoviere o tolerare, la impunidad u obstaculizare la investigación, persecución y sanción de los delitos establecidos en esta ley, será sancionado con pena de prisión de dos a cuatro años e inhabilitación para la función pública que desempeña por el mismo plazo.

Artículo 48.- Suicidio Feminicida por Inducción o Ayuda

Quien indujere a una mujer al suicidio o le prestare ayuda para cometerlo, valiéndose de cualquiera de las siguientes circunstancias, será sancionado con prisión de cinco a siete años:

39. Que le preceda cualquiera de los tipos o modalidades de violencia contemplados en la presente ley ó en cualquier otra ley.

40. Que el denunciado se haya aprovechado de cualquier situación de riesgo o condición física o psíquica en que se encontrare la víctima, por haberse ejercido contra ésta, cualquiera de los tipos o modalidades de violencia contemplados en la presente ó en

cualquier otra ley.

1 Que el inductor se haya aprovechado de la superioridad generada por las relaciones preexistentes o existentes entre él y la víctima.

Artículo 49.- Inducción, Promoción y Favorecimiento de Actos Sexuales o Eróticos por Medios Informáticos o Electrónicos

Quien de manera individual, colectiva u organizada publicare, distribuyere, enviare, promoviere, facilitare, administrare, financiare u organizare, de cualquier forma la utilización de mujeres, mayores de dieciocho años, sin su consentimiento en actos sexuales o eróticos, utilizando medios informáticos o electrónicos, será sancionado con prisión de cinco a diez años.

Artículo 50.- Difusión Ilegal de Información

Quien publicare, compartiere, enviare o distribuyere información personal que dañe el honor, la intimidad personal y familiar, y la propia imagen de la mujer sin su consentimiento, será sancionado con pena de uno a tres años.

Artículo 51.- Difusión de Pornografía

Quien publicare, compartiere, enviare o distribuyere material pornográfico por cualquier medio informático o electrónico en el que se utilice la imagen o identidad de la mujer sin su consentimiento, será sancionado con pena de tres a cinco años.

Artículo 52.- Favorecimiento al Incumplimiento de los Deberes de Asistencia Económica

Quien estando obligado a informar acerca de los ingresos de quienes deban cumplir con los deberes de asistencia económica, ocultare o diere información falsa, tardía, o incumpliere con orden de autoridad judicial o administrativa, será sancionado con prisión de uno a tres años, y multa equivalente a treinta salarios mínimos del comercio y servicios.

Artículo 53.- Sustracción Patrimonial

Quien sustrajere, algún bien o valor de la posesión o patrimonio de una mujer con quien mantuviere una relación de parentesco, matrimonio o convivencia sin su consentimiento, será sancionado con prisión de dos a cuatro años.

Artículo 54.- Sustracción de las utilidades de las actividades económicas familiares

Quien sustrajere las ganancias o ingresos derivados de una actividad económica familiar, o dispusiere de ellas para su beneficio personal y en perjuicio de los derechos de una mujer con quien mantenga una relación de parentesco, matrimonio o convivencia declarada o no, será sancionado con prisión de tres a seis años.

Artículo 55.- Expresiones de violencia contra las mujeres

Quien realizare cualquiera de las siguientes conductas, será sancionado con multa de dos a veinticinco salarios mínimos del comercio y servicio:

43. Elaborar, publicar, difundir o transmitir por cualquier medio, imágenes o mensajes visuales, audiovisuales, multimedia o plataformas informáticas con contenido de odio o menosprecio hacia las mujeres.

44. Utilizar expresiones verbales o no verbales relativas al ejercicio de la autoridad parental que tengan por fin intimidar a las mujeres.

45. Burlarse, desacreditar, degradar o aislar a las mujeres dentro de sus ámbitos de trabajo, educativo, comunitario, espacios de participación política o ciudadana, institucional u otro análogo como forma de expresión de discriminación de acuerdo a la presente ley.

46. Impedir, limitar u obstaculizar la participación de las mujeres en cualquier proceso de formación académica, participación política, inserción laboral o atención en salud.

47. Exponer a las mujeres a un riesgo inminente para su integridad física o emocional.

48. Mostrar o compartir pornografía de personas mayores de edad en los espacios públicos, de trabajo y comunitario.

Capítulo II
Disposiciones Procesales Específicas

Artículo 56.- Política de Persecución Penal en Materia de Violencia Contra las Mujeres

La Fiscalía General de la República deberá crear, la política de persecución penal en materia de Violencia contra las Mujeres de acuerdo a los principios establecidos en ésta ley.

Artículo 57.- Garantías Procesales de las Mujeres que Enfrentan Hechos de Violencia

A las mujeres que enfrenten hechos de violencia se les garantizará:

46. Que se preserve en todo momento su intimidad y privacidad. En consecuencia, su vida sexual no podrá ser expuesta directa o indirectamente, para justificar, minimizar o relativizar el daño causado.

47. Que se les extienda copia del requerimiento fiscal, de la denuncia administrativa, del reconocimiento médico legal y de cualquier otro documento de interés para la mujer que enfrenta hechos de violencia; así como, a ser tratadas con dignidad y respeto, especialmente por las partes intervinientes en el proceso.

48. Ser atendidas en la medida de lo posible, por personas del mismo sexo expertas y

capacitadas en derechos de las víctimas, derechos humanos de las mujeres, perspectiva de género y prevención de la violencia de género, en lugares accesibles y que garanticen la privacidad, seguridad y comodidad.

48. No ser discriminadas en razón de su historial sexual o por ninguna otra causa.

49. Que se proteja debidamente su intimidad y se aplique la reserva total o parcial del expediente, para evitar la divulgación de información que pueda conducir a su identificación o la de sus familiares, manteniendo la confidencialidad de la información sobre su residencia, teléfono, lugar de trabajo o estudio, entre otros aspectos. Dicha protección incluye a su familia y allegados.

50. Ser informada y notificada en forma oportuna y veraz, de las actuaciones que se vayan realizando durante todo el proceso judicial o administrativo, así como de los recursos pertinentes y de los servicios de ayuda. Así mismo, a qué se le extienda copia de la denuncia administrativa y del requerimiento fiscal, del reconocimiento médico legal y de cualquier otro documento de interés para la mujer, garantizando un trato digno y respetuoso.

51. Recibir asistencia integral, adecuada y oportuna, la cual podrá exceder la duración del proceso administrativo o judicial, independientemente del resultado.

52. Recibir atención médica, tratamiento adecuado y especializado, en los casos que lo ameriten. Así como la utilización del Protocolo de atención en caso de violencia sexual, para prevenir Infecciones de Transmisión Sexual y la Guía Técnica de Atención en Planificación Familiar.

53. El designar a un acompañante durante todo el proceso judicial o administrativo.

54. No ser coercionadas por las declaraciones vertidas durante el proceso.

55. Que de manera inmediata se decreten las medidas emergentes, de protección o cautelares establecidas en ésta o en el resto de leyes vigentes.

56. Recibir el auxilio y la protección, oportuna y adecuada, de la Policía Nacional Civil, o de cualquier otra instancia y de la comunidad.

57. Prestar testimonio en condiciones especiales de protección y cuidado; así como, a utilizar la figura del anticipo de prueba.

58. A que se tome en cuenta su estado emocional para declarar en el juicio, y que este sea realizado de manera individual.

59. Recibir información sobre sus derechos y el proceso en un idioma, lenguaje o dialecto que comprendan, en forma accesible a su edad y madurez.

51. Solicitar medidas de emergencia, protección y cautelares en caso de que se otorgue la libertad anticipada a la persona agresora.

Las víctimas del delito de trata además de las garantías ya establecidas, gozarán de las siguientes:

53. A que no se le apliquen las sanciones o impedimentos establecidos en la legislación migratoria, cuando las infracciones sean consecuencia de la actividad desplegada durante la comisión del ilícito que han sido víctimas.

54. A permanecer en el país, de conformidad con la legislación vigente, y a recibir la documentación o constancia que acredite tal circunstancia.

55. Asesoría jurídica migratoria gratuita.

Las mujeres que enfrentan hechos de violencia, gozarán de todos los derechos establecidos en la presente ley, en el resto del ordenamiento jurídico y en los Convenios Internacionales vigentes.

Artículo 58.- Prohibición de la Conciliación y Mediación

Se prohíbe la Conciliación o Mediación de cualquiera de los delitos comprendidos en la presente ley.

Disposiciones Finales

Artículo 59.- Declaración de Interés Público y Nacional

Se declara de interés público y nacional la implementación de la presente ley.

Artículo 60.- Regla Supletoria

En lo no previsto en la presente ley, se aplicarán las reglas procesales comunes en lo que fuere compatible con la naturaleza de la misma; así como, las disposiciones contenidas en el Código Procesal Penal.

Artículo 61.- Vigencia de la Ley

La presente ley entrará en vigencia el uno de enero del dos mil doce, previa publicación en el Diario Oficial.

DADO EN EL SA LON AZUL DEL PALACIO LEGISLATIVO: San Salvador, a los veinticinco días del mes de noviembre del año dos mil diez.

CIRO CRUZ ZEPEDA PEÑA,
PRESIDENTE.

OTHON SIGFRIDO REYES MORALES,
PRIMER VICEPRESIDENTE.

GUILLERMO ANTONIO GALLEGOS NAVARRETE,
SEGUNDO VICEPRESIDENTE.

JOSÉ FRANCISCO MERINO LÓPEZ,
TERCER VICEPRESIDENTE.

ALBERTO ARMANDO ROMERO RODRÍGUEZ,
CUARTO VICEPRESIDENTE.

FRANCISCO ROBERTO LORENZANA DURAN,
QUINTO VICEPRESIDENTE.

LORENA GUADALUPE PEÑA MENDOZA,
PRIMERA SECRETARIA.

CESAR HUMBERTO GARCÍA AGUILERA,
SEGUNDO SECRETARIO.

ELIZARDO GONZÁLEZ LOVO,
TERCER SECRETARIO.

ROBERTO JOSÉ d'AUBUISSON MUNGUÍA,
CUARTO SECRETARIO.

IRMA LOURDES PALACIOS VÁSQUEZ,
QUINTA SECRETARIA.

SEXTA SECRETARIA.

MARIO ALBERTO TENORIO GUERRERO,
SÉPTIMO SECRETARIO.

CASA PRESIDENCIAL: San Salvador, a los catorce días del mes de diciembre del año dos mil diez.

PUBLIQUESE,

Carlos Mauricio Funes Cartagena,
Presidente de la República.

Humberto Centeno Najarro,
Ministro de Gobernación.

D. O. Nº 2
Tomo Nº 390
Fecha: 4 de enero de 2011

SV/adar
1-2-
2011

ANALISIS DE LA LEGISLACION COMPARADA.

Para entrar a realizar el análisis de los tipos penales a nivel de Derecho comparado, se verán a continuación los casos de España, el Proyecto de Código Penal de Nicaragua, el Proyecto de Código Penal de Costa Rica y finalmente, el Código penal de El Salvador.

Dicho análisis se limitara a la reflexión en torno de los tipos penales propiamente dichos, omitiendo consideraciones en torno a la antijuridicidad y la culpabilidad, pues a efectos de subsunción de la conducta al tipo penal descrito, basta dicho análisis.

Para tal efecto, seguiremos en modelo del tipo complejo, que comprende dentro del tipo objetivo, los elementos descriptivos (sujeto activo, sujeto pasivo, acción, objeto, bien jurídico, resultado, nexo causal entre acción y resultado, circunstancias de tiempo, lugar, modo u otras circunstancias), los elementos normativos y los elementos subjetivos especiales del tipo objetivo (relaciones, calidades y circunstancias). Y dentro del tipo subjetivo, comprende tanto el dolo (conocimiento del hecho elemento cognoscitivo y voluntad de realizarlo –elemento volitivo) como la culpa, comprendida como la infracción al deber objetivo de cuidado.

De tal forma que el análisis ira orientado en ese sentido, especialmente a determinar:

- ✓ Cuál es el bien jurídico que protege el tipo penal.
- ✓ Si el tipo penal comprende acciones dolosas o culposas.
- ✓ Si son delitos de resultado, y por lo tanto admitirán la tentativa, o si son delitos de mera activad.
- ✓ Si se han tipificado resoluciones manifestadas (proposición y conspiración como delitos sui generis) adelantando las barreras de protección y punición.
- ✓ Si el tipo penal comprende, en forma precisa e inequívoca, la diversidad de conductas lesivas de determinados bienes jurídicos que merezcan punibilidad y que no han quedado descritas en el tipo pena, y que cabría la posibilidad de que

la jurisprudencia utilizarla la “analogía in malam parten” o si es posible hacer caber la conducta u otros elementos objetivos en la descripción penal al tratarse de tipos abiertos ; o tipos penales en blanco, en cuyo caso analizar si el “núcleo esencial del tipo” se encuentra descrito en el tipo penal, o si tal descripción se encuentra en las normas extrapenales, y por lo tanto serian lesivas al principio de legalidad penal.

- ✓ Determinar si existen lagunas de punibilidad.

España.

a) Lortad

La ley orgánica 5/1992 de 29 de Octubre de Regulación del Tratamiento Automatizado de los Datos de carácter personal (por sus siglas LORTAD) publicada en B.O.E. No. 262 del 31 octubre de 1992, se advierte que la lectura de su artículo 1 que la finalidad de la ley es hacer frente a los riesgos que para los derechos de personalidad puede suponer el acopio y tratamiento de datos por medios informáticos, por lo que la ley gira entorno a los que convencionalmente se denominan ficheros de datos.

Por ello se hace necesario delimitar el derecho a la intimidad y el honor, dándoles un nuevo contenido, por ser protegidos frente a la utilización mecanizada, ordenada y discriminada de los ordenadores, una frontera, que garantice que un elemento objetivamente provechoso para la humanidad no sea perjudicial para las personas.

Los derechos de acceso a los datos, de rectificación de cancelación, constituyen piezas centrales del sistema instaurados por la ley. Se propone, de la nueva garantía de la intimidad y del honor, resulta esencial la correcta regulación de la cesión de los datos almacenados cuya violación transgrediría los límites de la privacidad.

Así, “para asegurar la máxima eficacia de sus disposiciones, la ley encomienda el control de su aplicación a un órgano independiente, al que atribuye el estatuto de ente público en los términos del artículo de3 la ley general presupuestaria. A tal

efecto la ley configura un órgano especializado denominado Agencia de Protección de Datos, a cuyo frente sitúa un director.

La ley no consagra nuevos tipos delictivos, ni define presupuestos de responsabilidad penal para la eventualidad de su incumplimiento. Ello obedece a que se entiende que la sede lógica para tales menesteres no es esta ley, sino solo el código penal.

Es necesario limitar el derecho a la intimidad y el honor, dándoles un nuevo contenido, para ser protegidos frente a la utilización mecanizada, ordenada y discriminada de los ordenadores, una frontera, que garantice que un elemento objetivamente provechoso para la humanidad no sea perjudicial para las personas.

b) Código Penal de España.

El Código Penal Español incorpora nuevos bienes jurídicos que van a ser objeto de tutela a partir de ahora, al tiempo que refuerza bienes jurídicos tradicionales que se trasladan al nuevo ámbito jurídicos del ciberespacio.

El Código Penal de 1995 complementa tipos penales ya existentes con el objeto de dar cabida a las nuevas formas de lesión mediante el uso de la informática: bien como objeto de ataque, como el sabotaje informático (destrucción de datos-cracking), acceso ilegitimo a sistemas de datos (hacking), piratería informática o el uso ilícito de terminales de comunicación en lo que los elementos informáticos se ven como el objeto de protección penal y otros supuestos como los fraudes informáticos (abarcando a las estafas por medios informáticos y a los apoderamientos de dinero mediante tarjetas de crédito) en los que la informática aparece como el instrumento (medio) necesario para la realización de la correspondiente conducta típica.

La falta de respuesta legal adecuada a los delitos informáticos general una serie de problemas que van desde la impunidad hasta la aplicación de la analogía in malam partem, al no estar previstas tales conductas dentro de la descripción de los tipos penales.

Tal problemática no era exclusiva del caso español, sino que constituía una realidad común a prácticamente todos los ordenamientos, que se vieron sorprendidos por el desarrollo de un fenómeno cuya extraordinaria progresión no habían previsto.

De tal forma, que a continuación se analizan la respuesta que el Derecho Penal español ha dado a esta novedosa forma de criminalidad, mediante la reflexión sobre los tipos penales previstos en el Código Penal Español; y los distintos bienes jurídicos protegidos a través de la norma penal.

i) Delitos contra la indemnidad sexual.

El Titulo VIII trata de los Delitos contra la Libertad e indemnidad sexual, y su capítulo IV trata de los delitos de exhibicionismo y provocación sexual. Dentro de las figuras delictivas relacionadas con la informática, tenemos:

Artículo 186: Difusión de Material Pornográfico.

El artículo 186 tipifica como delito la conducta consistente en la difusión, venta o exhibición entre menores de edad o incapaces, de material pornográfico.

El tipo objetivo señala como acción, la difusión, venta o exhibición de materia pornográfico a menores o incapaces, siendo que dicha exhibición o difusión puede efectuarse mediante cualquier medio directo, entendemos incluido en este supuesto la difusión a través de internet mediante correo electrónico dirigidos a menores de edad o la exhibición a través de un web o una base de datos sin tomar las precauciones oportunas para impedir el acceso a menores. Siendo pues, un elemento descriptivo abierto, que comprende tales medios directos. De igual forma, es un delito de resultado, pues la difusión, venta o exhibición puede producirse o simplemente quedar en tentativa, con lo que es posible aplicar el tratamiento del art. 24 CP.

El tipo objetivo es doloso, excluyéndose la forma de comisión culposa, por lo que no habría sanción en caso de un error de tipo vencible.

ii) Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio y autodeterminación informativa.

En el Titulo X del libro II del Código Penal Español, se regulan los Delitos contra la Intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y en su capítulo I trata del descubrimiento y revelación de secretos, en la que regula figuras delictivas que tutelan tales bienes jurídicos, como se expone adelante.

Artículo 198: Interceptación, usurpación y cesión de datos personales.

El artículo 197 tiene como bien jurídico tutelado la intimidad de las personas, desde la interceptación de correo electrónico y la usurpación y cesión de datos reservados de carácter personal.

En el tipo objetivo, se advierte dentro de los elementos descriptivos que tanto los sujetos, tanto el activo como el pasivo, son genéricos, pudiendo ser cualquier persona.

Dentro de la acción de esta figura delictiva, se introduce la interceptación de correo electrónico, que queda asimilada a la violación de correspondencia, así extiende el ámbito de aplicación de este delito a las siguientes conductas:

1- Apoderamiento de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales.
2- Interceptación de las telecomunicaciones, en las mismas condiciones.
3- Utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, en las mismas condiciones de invasión de la intimidad y vulneración de secretos.

   También quedan tipificados los actos consistentes en apoderarse, utilizar, modificar revelar, difundir o ceder datos reservados de carácter personal que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos.

Encontramos acá un elemento descriptivos, pero a su vez, de enorme contenido normativo, como es el consentimiento de la persona que accede a que su intimidad sea lesionada, pues estas actividades deben producirse sin consentimiento del afectado y con la intención de descubrir secretos o vulnerar su intimidad. De tal forma que si se da el consentimiento del sujeto pasivo- lo que no comprende su asentimiento posterior, sino un consentimiento previo, nos atreveríamos a decir- el tipo penal no logra configurarse, quedando tal conducta en la atipicidad.

La pena que se establece de prisión, de uno a cuatro años y multa de doce a veinticuatro meses.

En los primeros dos casos (1,2), cuando se refiere al apoderamiento o interceptación de la comunicación, se trata de un delito de resultado, pues el hecho punible describe no únicamente la acción encaminada al apoderamiento e interceptación se produzcan efectivamente, por lo que puede darse la tentativa.

Diferente el supuesto que se señala en el número 3, que se refiere a la "utilización de artificios técnicos" de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, en las mismas condiciones de invasión de la intimidad y vulneración de secretos, en lo que no exige que se produzca el apoderamiento ni la interceptación, sino que es la mera actividad encaminada al fin de lograr el apoderamiento e interceptación.

En tal descripción, ciertamente está tipificado como un delito consumado, una conducta que está orientada a ese fin, pero que aún no ha logrado consumarse. Se está sancionando la tentativa como delito consumado, pues la mera actividad de usar tales artificios técnicos con tal finalidad (actos de ejecución), están siendo sancionados como si en efecto se hubiesen producido la interceptación u apoderamiento (consumación del delito); por lo tanto, con la misma penalidad del delito consumado se está sancionando una tentativa encaminada a ese fin, lo que lesiona los principios de proporcionalidad y de prohibición de exceso.

De igual forma, la parte final del art. 197.2 del Código Penal español, sanciona de igual forma "a quien sin estar autorizado, acceda por cualquier medio a los mismos". Habrá que analizar si se trata de un delito de resultado o si estamos en presencia de un delito de mera actividad. Distinción que como ya se apuntó, incide en el ámbito de la tentativa, pero sobre todo, en el principio de lesividad.

La acción descrita implica accesar por cualquier medio a los datos reservados de carácter personal registrados en ficheros o soportes informáticos, electrónicos o telemáticos; es decir, estamos en presencia de una actividad de hacking propiamente dicha.

Si lo consideramos como delito de mera actividad, bien podría considerarse un acto de preparación dentro del inter criminis, para la comisión de un futuro delito, como sería la utilización indebida de la información accesada o un daño a los soportes informáticos. Pero si el único fin es ingresar a tales archivos y violar los

códigos y sistemas de seguridad solo para efecto de revelar las diferencias o falencias de tales sistemas, sin un fin ulterior de perjudicar, dañar, revelar o difundir tales datos, no podría considerarse tampoco un acto preparatorio o acto de ejecución y por lo tanto tentativa. Por lo que estaríamos en presencia de un delito sui generis, adelantando el Derecho penal las barreras protectoras hacia estados previos a la lesión o puesta en peligro del bien jurídico.

Por el contrario, si consideramos que lo que se tutela es el "secreto" e "intimidad" como bienes jurídicos en sentido estricto, y con tal acceso se produzca ya el resultado lesivo, como es el supuesto del delito de "Allanamiento de morada" (art.188 CP), lo sería un delito de resultado de consumación instantánea de efectos permanentes, pues bastaría la introducción al banco de datos, permaneciendo en el y accediendo a la información.

Por otra parte, la decisión de Política criminal de sancionar estas conductas, que se refiere directamente a los Hackers, es como un fin de prevención general, para evitar que muchas conductas intimas en sí mismas, al acumularlas si generan en conjunto un daño o lesión considerable. Es lo que se conoce como tipos acumulativos y en los que es objetable la transparencia de la culpabilidad de otros hacia el sujeto que delinque. Por ejemplo en materia de Derecho penal ambiental, aunque la contaminación o daño ambiental sea ínfimo, al acumularse esta conducta a la de otros, en conjunto si sea considerable dicho daño. Es decir, el efecto acumulado de muchas lesiones individuales íntimas si configuran una lesión importante, por lo que como medida de Política Criminal se decide no dejar de penalizar tales hechos individuales.

Sin embargo, ello presenta problemas a nivel de la culpabilidad del autor, especialmente a la lesión del principio de responsabilidad, e implica una infracción al principio de no transferibilidad de la culpabilidad, pues tanto en el delito contra el medio ambiente, como el supuesto del hackers al ingresar o accesar sin autorización aun sistema informático, tales lesiones son ínfimas y no pueden hacérseles responsables penalmente por las lesiones que otros causen o hayan causado contra tales bienes jurídicos, pues su culpabilidad debe restringirse a su acción y a la lesión

producida. Sobre tales puntos debe reflexionarse pues se amplía la intervención del derecho penal.

Además, se infringe el principio de proporcionalidad pues se sanciona de igual forma al que simplemente accede al sistema, como a quien infiere, interrumpe, difunde o revela la información, que en tales casos si hay revelación u obstrucción al secreto, por lo que debería sancionarse con mayor severidad que el simple acceso. Ellos respecto al tipo objetivo contemplado en el art. 197 CP.

El tipo subjetivo contempla únicamente acciones dolosas, que exigen el conocimiento del hecho (elemento cognoscitivo) y la voluntad de realizarlo (elemento volitivo), pues para que se tipifique la acción como por culpa, debe regularlo expresamente el legislador, pues nuestros sistemas (Costa Rica y El Salvador) acogen la noción de numerus clausus en los tipos culposos. Ello implica que en el caso se producirse un error de tipo vencible (sobre el conocimiento del hecho y sobre la voluntad de realizarlo), tal acción seria impune pues no está sancionada la forma culposa de comisión.

El artículo 197.3 castiga con prisión de 1 a 4 años para el caso de acceso, utilización, etc. Y de 2 a 5 años si los datos se difunden, revelan o ceden a terceros. Cuando dichos actos afectan a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la victima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

Artículo 198: Interceptación, usurpación y cesión de datos personales por una autoridad o funcionario público.

El artículo 198 también contempla como bien jurídico la intimidad, y contempla dentro de los elementos descriptivos del tipo objetivo, las mismas conductas que penaliza el artículo anterior, con la diferencia en cuanto al sujeto activo, que se refiere a que tales conductas sean realizadas por una autoridad o funcionario público sin que medie causa legal.

iii) Delitos contra el Honor.

El titulo XI regula los delitos contra el Honor, y en su capítulo III que trata de las disposiciones generales a los capítulos I (De la calumnia) y II (De la injuria), introduce una presunción de publicidad, como se señala.

Artículo 211: Calumnia e injuria con publicidad.

El artículo 211, complementando a los delitos de calumnia e injuria, señala que se reputaran hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o cualquier otro medio de eficacia semejante.

Dentro de “cualquier otro medio de eficacia semejante” puede incluirse perfectamente en este supuesto la difusión de mensajes injuriosos o calumniosos a través de internet, en especial, en el entorno web (www) que es el más similar a la prensa tradicional.

Las penas establecidas pueden llegar a los 2 años de prisión en el caso de la calumnia, y la, multa de hasta 14 meses en el caso de la injuria.

Artículo 212: Responsabilidad solidaria.

Por su parte, el artículo 212 establece la responsabilidad solidaria del propietario del medio informativo a través del que se haya propagado la calumnia o injuria.

En el caso de internet, la responsabilidad civil podría incluso alcanzar al propietario del servidor en el que publico la información constitutiva de delito, aun que debería tenerse en cuenta, en este caso, si existió la posibilidad de conocer dicha situación, ya que el volumen de la información contenida en un servidor no es comparable al de una revista, un periódico, o un programa de TV o radio.

NICARAGUA.

El Proyecto de Código Penal de la República de Nicaragua contempla una serie de tipos Penales que hacen referencia a los delitos Informáticos.

Delitos Contra la Intimidad

En su libro segundo, titulo cuarto capítulo primero, el proyecto de Código Penal de Nicaragua regula los delitos contra la intimidad a través de los siguientes tipos penales

Artículo 195: Descubrimiento de Correspondencia

Contempla dentro de sus elementos descriptivos del tipo objetivo el hecho de abrir ilegítimamente un documento electrónico que no le este destinado. Acá

encontramos un elemento normativo del tipo objetivo, como es el no estar legitimado para abrir el documento , pudiendo encontrarse legitimado para abrir el documento, pudiendo estar legitimado si la persona titular del documento electrónico lo autoriza y da el consentimiento que esta persona abra el documento y se imponga de él. Otra acción contemplada en el tipo objetivo, es el difundir el contenido, con una pena de inhabilitación especial si el sujeto activo se tratare de un funcionario o autoridad pública. El tipo subjetivo es doloso, no contemplado la culpa en su comisión y por lo tanto, a nivel de error de tipo vencible, este también seria impune.

Articulo 201 Registro Prohibido

Tipifica y sanciona los "registros prohibidos" y regula dentro del tipo objetivo, referido a sujetos genéricos, señala como acción del delito el crear registros informáticos que puedan afectar la intimidad de las personas esta prohibíos. Se advierte que se trata de un delito de mera Actividad, pues no exige un resultado lesivo, y por otra parte, se configura como un delito en abstracto, pues está en realidad no se ponga en peligro efectivo o concreto. Por otra parte, el tipo subjetivo es Doloso, no contemplando la comisión Culposa.

Artículo 202: Uso de Información

A quien sin autorización utilice los registros informáticos de otros, ingresos por cualquier medio al banco de datos, será penado con prisión de uno a dos años y multa de doscientos a quinientos.

COSTA RICA.

El proyecto de Código Penal en su título IV regula los delitos contra el ámbito de la intimidad, específicamente la violación de datos personales y comunicaciones

El actual Código Penal deja sin tutela una importante área de la intimidad, como es la autodeterminación informativa. Así, el proyecto de Código Penal amplia la tutela de la intimidad al ámbito de la libertad informática

Delitos Contra Intimidad

Artículo 187 del proyecto, tipifica el "tratamiento ilícito de datos personales y comunicaciones", donde la intimidad se tutela a las comunicaciones, imágenes o

datos en programas de cómputo a partir del apoderamiento o un trato no autorización de las mismas.

La redacción del artículo parece ser amplia, al establecer que quien se apodere, abra, accese, imponga, copie, trasmita, publique, recopile, use, intercepte, retenga .suprima, oculte, desvié, o de un tratamiento no autorizado, sin embargo, deja de lado el procesamiento de los datos, puesto que lo que se debe de garantizar es la seguridad de los ciudadanos, puesto que mediante la colecta de los datos se puede formar el perfil económico, político, social de la persona.

Artículo 188 “Propalación, tutela, la intimidad y el secreto de las comunicaciones entre las personas, la prohibición de la publicidad responde a las necesidades de limitar las posibilidades de la comisión de los delitos. No solo se sanciona a quien ilícitamente tenga conocimiento de ellos si no a quien le han sido dirigidos lo haga públicos.

Este artículo se puede considerar complemento del artículo anterior, pues introduce la prohibición para aquel que estamos en posesión legal del contenido no puede hacerlos público.

Articulo 189 Obtención de datos personales mediante engaño, pues el engaño para obtener datos personales es prohibido. No es Necesaria la publicación de los mismos, pues basta la recolección

El problema que plantea este Artículo es la prueba. Laper4sona que tenga conocimiento de ser víctima de un delito informático, quizá no llegue a saber quién es el delincuente, pues en muchas ocasiones el delincuente y el procesamiento de datos ilícitos no dejan rastro para su persecución Esto cuando la víctima tenga conocimiento del Delito que contra su intimidad sufre. De esta manera es fácil crear archivos de datos y formar perfiles de personas.

Artículo 190: Divulgación de secreto, guarda este el mismo espíritu del profesional o persona que en su calidad tengan el deber jurídico de guardar el secreto, solo que este articulo lo traslada al ámbito informático. El cuestionamiento que se presenta es si se hace público el secreto y no causa daño. Castigo de las personas que en su cargo, encargados responsables de los ficheros, soportes

informáticos, archivos o registros o su función de empleados o autoridades públicos realicen las conductas contempladas en este capitulo

Los encargados de la fidelidad de estos datos, deben velar por el secreto y la intimidad de la información, así tienen acceso a ellos solo cuando sea necesario y por razones del objeto del tratamiento, es decir cuando me medie causa legal

Artículo 192. Establece la sanción de inhabilitación como pena accesoria, importante es destacar que las sancione penales para delincuente informáticos, esto no serviría para rehabilitarlos, en este sentido las sanciones extrapenales, resulta de, mejor aplicación así como sanción.

Serie de Tratados Europeos- n°185

CONVENIO SOBRE LA CIBERDELINCUENCIA

Budapest, 23.XI.2001

Preámbulo

Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio,

Considerando que el objetivo del Consejo de Europa es lograr una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los otros Estados Partes en el presente Convenio;

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

Reconociendo la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información;

Estimando que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal;

Convencidos de que el presente Convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable;

Teniendo presente la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de derechos humanos, que reafirman el derecho a defender la propia opinión sin interferencia, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar información e ideas de toda índole, sin consideración de fronteras, así como el respeto de la vida privada;

Conscientes igualmente del derecho a la protección de los datos personales, tal como se define, por ejemplo, en el Convenio de 1981 del Consejo de Europa para la protección de las personas con respecto al tratamiento informatizado de datos personales;

Teniendo presentes la Convención sobre los Derechos del Niño de las Naciones Unidas (1989) y el Convenio sobre las peores formas de trabajo infantil de la Organización Internacional del Trabajo (1999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el objeto del presente Convenio es completar dichos Convenios con el fin de incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como permitir la obtención de pruebas electrónicas de los delitos;

Congratulándose de las recientes iniciativas destinadas a mejorar el entendimiento y la cooperación internacionales en la lucha contra la delincuencia cibernética, y en particular las acciones organizadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8;

Recordando las Recomendaciones del Comité de Ministros nº R (85) 10 relativa a la aplicación práctica del Convenio Europeo de Asistencia Judicial en Materia Penal en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, nº R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, nº R (87) 15 relativa a la regulación de la utilización de datos de personales por la policía, nº R (95) 4 sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos, nº R (89) 9 sobre la delincuencia relacionada con la informática, que ofrece a los legisladores nacionales directrices para definir ciertos delitos informáticos, y nº R (95) 13 relativa a los problemas de procedimiento penal vinculados a la tecnología de la información;

Teniendo presente la Resolución nº 1, adoptada por los Ministros de Justicia europeos, en su XXI Conferencia (Praga, 10 y 11 de junio de 1997), que recomendaba al Comité de Ministros apoyar las actividades en relación con la ciberdelincuencia organizadas por el Comité Europeo para Problemas Criminales (CDPC) con el fin de aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos, así como la Resolución nº 3, adoptada en la XXIII Conferencia de Ministros de Justicia europeos (Londres, 8 y 9 de junio de 2000), que exhortaba a las partes negociadoras a persistir en sus esfuerzos por encontrar soluciones que permitan al mayor número posible de Estados ser partes en el Convenio, y reconocía la necesidad de disponer de un mecanismo rápido y eficaz de cooperación internacional que tenga debidamente en cuenta las exigencias específicas de la lucha contra la ciberdelincuencia;

Teniendo asimismo en cuenta el plan de acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa, con ocasión de su segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997) con objeto de encontrar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa,

Han convenido en lo siguiente:

Capítulo I – Terminología

Artículo 1 – Definiciones

A los efectos del presente Convenio:

a. por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;
b. por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;
c. por "proveedor de servicios" se entenderá:

   i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y
   ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo;

d. por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Capítulo II – Medidas que deberán adoptarse a nivel nacional

Sección 1 – Derecho penal sustantivo

Título 1 – Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2 – Acceso ilícito

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Artículo 3 – Interceptación ilícita

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del

mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 4 – Ataques a la integridad de los datos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

Artículo 5 – Ataques a la integridad del sistema

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6 – Abuso de los dispositivos

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

   i. cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio;
   ii. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático,

   con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y

b. la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del presente artículo.

Título 2 – delitos informáticos

Artículo 7 – Falsificación informática

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8 – Fraude informático

Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a. la introducción, alteración, borrado o supresión de datos informáticos;
b. cualquier interferencia en el funcionamiento de un sistema informático,

con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Título 3 – Delitos relacionados con el contenido

Artículo 9 – Delitos relacionados con la pornografía infantil

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

   a. la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
   b. la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;
   c. la difusión o la transmisión de pornografía infantil a través de un sistema informático;
   d. la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;
   e. la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 anterior, se entenderá por «pornografía infantil» todo material pornográfico que contenga la representación visual de:

a. un menor adoptando un comportamiento sexualmente explícito;
b. una persona que parezca un menor adoptando un comportamiento sexualmente explícito;
c. imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

3. A los efectos del párrafo 2 anterior, se entenderá por «menor» toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

4. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.

Título 4 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de París de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3. En circunstancias bien delimitadas, toda Parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Título 5 – Otras formas de responsabilidad y de sanción

Artículo 11 – Tentativa y complicidad

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en aplicación de los artículos 2 a 10 del presente Convenio, con la intención de que dicho delito sea cometido.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos previstos en aplicación de los artículos 3 a 5, 7, 8, 9.1.a) y 9.1.c) del presente Convenio.

3. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Artículo 12 – Responsabilidad de las personas jurídicas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del presente Convenio, cuando éstos sean cometidos por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:

a. un poder de representación de la persona jurídica;
b. una autorización para tomar decisiones en nombre de la persona jurídica;
c. una autorización para ejercer funciones de control en el seno de la persona jurídica.

2. Además de los casos previstos en el párrafo 1 del presente artículo, Cada Parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito previsto en aplicación del presente Convenio por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad.

3. Dependiendo de los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Artículo 13 – Sanciones y medidas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en aplicación de los artículos 2 a 11 estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2. Las Partes garantizarán la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

Sección 2 – Derecho procesal

Título 1 – Disposiciones comunes

Artículo 14 – Ámbito de aplicación de las disposiciones de procedimiento

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección a los efectos de investigación o de procedimientos penales específicos.

2. Salvo que se establezca lo contrario en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del presente artículo:

a. a los delitos previstos en aplicación de los artículos 2 a 11 del presente Convenio;
b. a cualquier otro delito cometido por medio de un sistema informático; y
c. a la obtención de pruebas electrónicas de cualquier delito.

3. a. Las Partes podrán reservarse el derecho a aplicar las medidas mencionadas en el artículo 20 únicamente a los delitos o categorías de delitos especificados en su reserva, siempre que el repertorio de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que dicha Parte aplique las medidas mencionadas en el artículo 21. Las Partes tratarán de limitar tal reserva de modo que sea posible la más amplia aplicación de la medida mencionada en el artículo 20.

b. Cuando, a causa de las restricciones que imponga su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas previstas en los artículos 20 y 21 a las comunicaciones transmitidas dentro de un sistema informático de un proveedor de servicios:

i. que se haya puesto en funcionamiento para un grupo restringido de usuarios, y
ii. que no emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado,

dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Las Partes tratarán de limitar este tipo de reservas de modo que de modo que sea posible la más amplia aplicación de las medidas previstas en los artículos 20 y 21.

Artículo 15 – Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos

derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.

3. Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Parte examinará los efectos de los poderes y procedimientos mencionados en la presente Sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

Título 2 – Conservación rápida de datos informáticos almacenados

Artículo 16 – Conservación rápida de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación.

2. Cuando una Parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y a proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el fin de que las autoridades competentes puedan obtener su revelación. Las Partes podrán prever la renovación de dicha orden.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a la persona que custodia los datos o a otra persona encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 17 – Conservación y revelación parcial rápidas de los datos relativos al tráfico

1. Con el fin de garantizar la conservación de los datos relativos al tráfico, en aplicación del artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para:

a. garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de dicha comunicación; y
b. asegurar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicha Parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 3 – Orden de presentación

Artículo 18 – Orden de presentación

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a. a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; y
b. a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios;

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

3. A los efectos del presente artículo, se entenderá por «datos relativos a los abonados» cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:

a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;
b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio;
c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

Título 4 – Registro y confiscación de datos informáticos almacenados

Artículo 19 – Registro y confiscación de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de un modo similar:

a. a todo sistema informático o a parte del mismo, así como a los datos informáticos en él almacenados; y
b. a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos

en su territorio.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurarse de que, cuando, de conformidad con el apartado 1.a), sus autoridades registren o tengan acceso de un modo similar a un sistema informático específico o a una parte del mismo y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial, puedan extender rápidamente el registro o el acceso de un modo similar al otro sistema.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1 o 2. Estas medidas incluirán las siguientes prerrogativas:

a. confiscar u obtener de un modo similar un sistema informático o una parte del mismo, o un dispositivo de almacenamiento informático;
b. realizar y conservar una copia de esos datos informáticos;
c. preservar la integridad de los datos informáticos almacenados pertinentes; y
d. hacer inaccesibles o suprimir dichos datos informáticos del sistema informático consultado.

4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.

5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 5 – Obtención en tiempo real de datos informáticos

Artículo 20 – Obtención en tiempo real de datos relativos al tráfico

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes:

a. a obtener o grabar con medios técnicos existentes en su territorio, y
b. a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas:

    i. a obtener o a grabar con medios técnicos existentes en su territorio, o

ii. a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar

en tiempo real los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 21 – Interceptación de datos relativos al contenido

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno a:

a. obtener o grabar con medios técnicos existentes en su territorio, y
b. obligar a un proveedor de servicios, en la medida de sus capacidades técnicas, a:

i. obtener o grabar con medios técnicos existentes en su territorio, o
ii. prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar,

en tiempo real los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio con medios técnicos existentes en ese territorio.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Sección 3 – Jurisdicción

Artículo 22 – Jurisdicción

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del presente Convenio, cuando el delito se haya cometido:

a. en su territorio; o
b. a bordo de un buque que enarbole su pabellón; o
c. a bordo de una aeronave matriculada según sus leyes; o
d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

2. Las Partes podrán reservarse el derecho a no aplicar, o a aplicar sólo en determinados casos o condiciones, las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier parte de dichos apartados.

3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito mencionado en el párrafo 1 del artículo 24 del presente Convenio cuando el presunto autor del mismo se halle en su territorio y no pueda ser extraditado a otra Parte por razón únicamente de su nacionalidad, previa demanda de extradición.

4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

5. En el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción penal.

Capítulo III – Cooperación internacional

Sección 1 – Principios generales

Título 1 – Principios generales relativos a la cooperación internacional

Artículo 23 – Principios generales relativos a la cooperación internacional

Las Partes cooperarán entre sí en la mayor medida posible de conformidad con las disposiciones del presente Capítulo, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno, a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

Título 2 – Principios relativos a la extradición

Artículo 24 – Extradición

1. a. El presente artículo se aplicará a la extradición entre las Partes por los delitos definidos de conformidad con los artículos 2 a 11 del presente Convenio, siempre que sean castigados por la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración de al menos un año, o con una pena más grave.

b. Cuando se aplique una pena mínima diferente en virtud de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE nº 24), o de un acuerdo basado en legislación uniforme o recíproca, se aplicará la pena mínima prevista en dicho tratado o acuerdo.

2. Se considerará que los delitos descritos en el párrafo 1 del presente artículo están incluidos entre los delitos que pueden dar lugar a extradición en todos los tratados de extradición concluidos entre o por las Partes. Las Partes se comprometerán a incluir dichos delitos entre los que pueden dar lugar a extradición en todos los tratados de extradición que puedan concluir.

3. Cuando una parte que condicione la extradición a la existencia de un tratado reciba una demanda de extradición de otra Parte con la que no ha concluido ningún tratado de extradición, podrá tomar el presente Convenio como fundamento jurídico de la extradición en relación con cualquiera de los delitos previstos en el párrafo 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el párrafo 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.

5. La extradición estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de extradición vigentes, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6. Si se deniega la extradición por un delito mencionado en el párrafo 1 del presente artículo únicamente por razón de la nacionalidad de la persona reclamada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes a efectos de la acción penal pertinente, e informará, a su debido tiempo, de la conclusión del asunto a la Parte requirente. Dichas autoridades tomarán su decisión y realizarán sus investigaciones y procedimientos del mismo modo que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.

7. a. Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de las demandas de extradición o de detención provisional, en ausencia de tratado.

b. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

Título 3 – Principios generales relativos a la asistencia mutua

Artículo 25 – Principios generales relativos a la asistencia mutua

1. Las Partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.

2. Cada Parte adoptará asimismo las medidas legislativas y de otro tipo que resulten necesarias para cumplir con las obligaciones establecidas en los artículos 27 a 35.

3. Cada Parte podrá, en caso de urgencia, formular una solicitud de asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y de autenticación (incluido el criptado, en caso necesario), con confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación.

4. Salvo en caso de que se disponga expresamente otra cosa en los artículos del presente Capítulo, la asistencia mutua estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de los cuales la Parte requerida puede rechazar la cooperación. La Parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los artículos 2 a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal.

5. Cuando, de conformidad con lo dispuesto en el presente Capítulo, la Parte requerida esté autorizada a condicionar la asistencia mutua a la existencia de doble tipificación penal, se considerará que dicha condición se satisface si el acto que constituye delito, y para el que se solicita la asistencia mutua, está tipificado como tal en su derecho interno, independientemente de que dicho derecho interno incluya o no el delito en la misma categoría o lo denomine o no con la misma terminología que la Parte requirente.

Artículo 26 – Información espontánea

1. Dentro de los límites de su derecho interno y sin que exista demanda previa, una Parte podrá comunicar a otra Parte información obtenida de sus propias investigaciones si considera que ello puede ayudar a la Parte destinataria a iniciar o a concluir investigaciones o procedimientos en relación con delitos previstos de conformidad con el presente Convenio, o cuando dicha información pueda conducir a una petición de cooperación de dicha Parte en virtud del presente Capítulo.

2. Antes de comunicar dicha información, la Parte que la proporciona podrá pedir que sea tratada de forma confidencial o que sólo se utilice bajo ciertas condiciones. Si la Parte destinataria no puede atender a dicha petición, deberá informar de ello a la otra Parte, que decidirá a continuación si, no obstante, debe proporcionar la información. Si la Parte destinataria acepta la información bajo las condiciones establecidas, estará obligada a respetarlas.

Título 4 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Artículo 27 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones de los párrafos 2 a 9 del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes implicadas decidan aplicar en su lugar la totalidad o una parte del resto del presente artículo.

2. a. Cada Parte designará una o varias autoridades centrales encargadas de enviar las solicitudes de asistencia mutua o de responder a las mismas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución;

b. las autoridades centrales comunicarán directamente entre sí;

c. en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicará al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en aplicación del presente párrafo.

d. el Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con el procedimiento especificado por la Parte requirente, salvo cuando dicho procedimiento sea incompatible con la legislación de la Parte requerida.

4. Además de las condiciones o los motivos de denegación previstos en el párrafo 4 del artículo 25, la asistencia mutua puede ser denegada por la Parte requerida:

a. si la solicitud tiene que ver con un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
b. si la Parte requerida estima que acceder a la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

5. La Parte requerida podrá aplazar su actuación en respuesta a una solicitud si dicha actuación puede perjudicar a investigaciones o procedimientos llevados a cabo por sus autoridades.

6. Antes de denegar o aplazar su cooperación, la Parte requerida estudiará, previa consulta con la Parte requirente cuando proceda, si puede atenderse la solicitud parcialmente o bajo las condiciones que considere necesarias.

7. La Parte requerida informará rápidamente a la Parte requirente del curso que prevé dar a la solicitud de asistencia. Deberá motivar toda denegación o aplazamiento de la misma. La Parte requerida informará asimismo a la Parte requirente de cualquier motivo que imposibilite la ejecución de la asistencia o que pueda retrasarla sustancialmente.

8. La Parte requirente podrá solicitar que la Parte requerida mantenga confidenciales la presentación y el objeto de cualquier solicitud formulada en virtud del presente Capítulo, salvo en la medida en que sea necesario para la ejecución de la misma. Si la Parte requerida no puede acceder a la petición de confidencialidad, deberá informar de ello sin demora a la Parte requirente, quien decidirá a continuación si, no obstante, la solicitud debe ser ejecutada.

9. a. En caso de urgencia, las autoridades judiciales de la Parte requirente podrán dirigir directamente a las autoridades homólogas de la Parte requerida las solicitudes de asistencia y las comunicaciones relativas a las mismas. En tales casos, se remitirá simultáneamente una copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente.

b. Toda solicitud o comunicación en virtud del presente párrafo podrá formularse a través de la Organización Internacional de Policía Criminal (Interpol).

c. Cuando se formule una solicitud en aplicación del apartado a) del presente artículo y la autoridad no tenga competencia para tratarla, la remitirá a la autoridad nacional competente e informará directamente de ello a la Parte requirente.

d. Las solicitudes o comunicaciones realizadas en aplicación del presente párrafo que no impliquen medidas coercitivas podrán ser transmitidas directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida.

e. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, las Partes podrán informar al Secretario General del Consejo de Europa de que, en aras de la eficacia, las solicitudes formuladas en virtud del presente párrafo deberán dirigirse a su autoridad central.

Artículo 28 – Confidencialidad y restricciones de uso

1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes interesadas decidan aplicar en su lugar la totalidad o una parte del presente artículo.

2. La Parte requerida podrá supeditar la transmisión de información o de material en respuesta a una solicitud al cumplimiento de las siguientes condiciones:

a. que se preserve su confidencialidad cuando la solicitud de asistencia no pueda ser atendida en ausencia de dicha condición; o
b. que no se utilicen para investigaciones o procedimientos distintos a los indicados en la solicitud.

3. Si la Parte requirente no pudiera satisfacer alguna de las condiciones mencionadas en el párrafo 2, informará de ello sin demora a la Parte requerida, quien determinará a continuación si, no obstante, la información ha de ser proporcionada. Si la Parte requirente acepta esta condición, estará obligada a cumplirla.

4. Toda Parte que proporcione información o material supeditado a alguna de las condiciones mencionadas en el párrafo 2 podrá exigir a la otra Parte precisiones sobre el uso que haya hecho de dicha información o material en relación con dicha condición.

Sección 2 – Disposiciones específicas

Título 1 – Asistencia mutua en materia de medidas provisionales

Artículo 29 – Conservación rápida de datos informáticos almacenados

1. Una Parte podrá solicitar a otra Parte que ordene o imponga de otro modo la conservación rápida de datos almacenados por medio de sistemas informáticos que se encuentren en el territorio de esa otra Parte, y en relación con los cuales la Parte requirente tenga intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, la confiscación o la obtención por un medio similar, o a la revelación de dichos datos.

2. En toda solicitud de conservación formulada en virtud del párrafo 1 deberá precisarse:

a. la autoridad que solicita la conservación;
b. el delito objeto de la investigación o de procedimientos penales y una breve exposición de los hechos relacionados con el mismo;
c. los datos informáticos almacenados que deben conservarse y su relación con el delito;
d. toda información disponible que permita identificar al responsable de la custodia de los datos informáticos almacenados o el emplazamiento del sistema informático;
e. la necesidad de la medida de conservación; y
f. que la Parte tiene intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar, o a la revelación de los datos informáticos almacenados.

3. Tras recibir la solicitud de otra Parte, la Parte requerida deberá adoptar todas las medidas adecuadas para proceder sin demora a la conservación de los datos solicitados, de conformidad con su derecho interno. A los efectos de responder a solicitudes de este tipo no se requiere la doble tipificación penal como condición para proceder a la conservación.

4. Cuando una Parte exige la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de los datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11 del presente Convenio, podrá reservarse el derecho a denegar la solicitud de conservación en virtud del presente artículo en caso de que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá la condición de la doble tipificación penal.

5. Asimismo, las solicitudes de conservación sólo podrán ser denegadas si:

a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o

b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

6. Cuando la Parte requerida considere que la conservación por sí sola de los datos no bastará para garantizar su disponibilidad futura, o que pondrá en peligro la confidencialidad de la investigación de la Parte requirente, o causará cualquier otro perjuicio a la misma, informará de ello rápidamente a la Parte requirente, quien determinará a continuación la conveniencia, no obstante, de dar curso a la solicitud.

7. Las medidas de conservación adoptadas en respuesta a solicitudes como la prevista en el párrafo 1 serán válidas por un periodo mínimo de 60 días, con el fin de que la Parte requirente pueda presentar una solicitud con vistas al registro o el acceso por un medio similar, la confiscación o la obtención por un medio similar, o la revelación de los datos. Una vez recibida la solicitud, los datos deberán conservarse hasta que se tome una decisión sobre la misma.

Artículo 30 – Revelación rápida de datos conservados

1. Si, al ejecutar una solicitud formulada de conformidad con el artículo 29 para la conservación de datos relativos al tráfico de una determinada comunicación la Parte requerida descubriera que un proveedor de servicios de otro Estado ha participado en la transmisión de dicha comunicación, dicha Parte revelará rápidamente a la Parte requirente un volumen suficiente de datos relativos al tráfico para que pueda identificarse al proveedor de servicios, así como la vía por la que la comunicación ha sido transmitida.

2. La revelación de datos relativos al tráfico en aplicación del párrafo 1 sólo podrá ser denegada si:

a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

Título 2 – Asistencia mutua en relación con los poderes de investigación

Artículo 31 – Asistencia mutua en relación con el acceso a datos almacenados

1. Una Parte podrá solicitar a otra Parte el registro o el acceso de un modo similar, la confiscación o la obtención de un modo similar o la revelación de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, incluidos los datos conservados de conformidad con el artículo 29.

2. La Parte requerida responderá a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con las disposiciones pertinentes del presente Capítulo.

3. La solicitud deberá responderse lo más rápidamente posible en los siguientes casos:

a. cuando existan motivos para creer que los datos pertinentes están particularmente expuestos al riesgo de pérdida o de modificación; o

b. cuando los instrumentos, acuerdos o legislación mencionados en el párrafo 2 prevean una cooperación rápida.

Artículo 32 – Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público

Una Parte podrá, sin autorización de otra:

a. tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos; o
b. tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos por medio de ese sistema informático.

Artículo 33 – Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico

1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. A reserva de las disposiciones del párrafo 2, dicha asistencia mutua estará sujeta a las condiciones y procedimientos previstos en el derecho interno.

2. Cada Parte prestará dicha asistencia al menos en relación con los delitos para los cuales sería posible la obtención en tiempo real de datos relativos al tráfico en situaciones análogas a nivel interno.

Artículo 34 – Asistencia mutua en relación con la interceptación de datos relativos al contenido

Las Partes se prestarán asistencia mutua, en la medida en que lo permitan sus tratados y leyes internas aplicables, para la obtención o el registro en tiempo real de datos relativos al contenido de comunicaciones específicas transmitidas por medio de un sistema informático.

Título 3 – Red 24/7

Artículo 35 – Red 24/7

1. Cada Parte designará un punto de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que figuran a continuación, o su aplicación directa si lo permite el derecho y la práctica internos:

a. asesoramiento técnico;
b. conservación de datos, de conformidad con los artículos 29 y 30; y
c. obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos.

2. a. El punto de contacto de una Parte dispondrá de los medios para comunicarse con el punto de contacto de otra Parte siguiendo un procedimiento acelerado.

b. Si el punto de contacto designado por una Parte no depende de la autoridad o autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, dicho punto de contacto se asegurará de poder actuar coordinadamente con esta o estas autoridades por medio de un procedimiento acelerado.

3. Cada Parte garantizará la disponibilidad de personal formado y equipado con objeto de facilitar el funcionamiento de la red.

Capítulo IV – Cláusulas finales

Artículo 36 – Firma y entrada en vigor

1. El presente Convenio está abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.

2. El presente Convenio estará sujeto a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario General del Consejo de Europa.

3. El presente Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que cinco Estados, de los cuales al menos tres deberán ser miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio, de conformidad con lo dispuesto en los párrafos 1 y 2.

4. Para todo Estado signatario que exprese ulteriormente su consentimiento para quedar vinculado por el Convenio, éste entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado dicho consentimiento, de conformidad con lo dispuesto en los párrafos 1 y 2.

Artículo 37 – Adhesión al Convenio

1. A partir de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá, previa consulta con los Estados contratantes del Convenio y habiendo obtenido su consentimiento unánime, invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo de Europa y que no haya participado en su elaboración. La decisión se adoptará respetando la mayoría establecida en el artículo 20.d del Estatuto del Consejo de Europa y con el voto unánime de los representantes de los Estados contratantes con derecho a formar parte del Comité de Ministros.

2. Para todo Estado que se adhiera al Convenio de conformidad con el párrafo 1 precedente, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.

Artículo 38 – Aplicación territorial

1. En el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, todo Estado podrá designar el territorio o los territorios a los que se aplicará el presente Convenio.

2. Posteriormente, todo Estado podrá, en cualquier momento y por medio de una declaración dirigida al Secretario General del Consejo de Europa, hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. El Convenio entrará en vigor respecto de dicho territorio el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.

3. Toda declaración formulada en virtud de los dos párrafos precedentes podrá ser retirada, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 39 – Efectos del Convenio

1. El objeto del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones:

– del Convenio Europeo de Extradición, abierto a la firma el 13 de diciembre de 1957 en París (STE nº 24)

– del Convenio Europeo de Asistencia Judicial en Materia Penal, abierto a la firma el 20 de abril de 1959 en Estrasburgo (STE nº 30),

– del Protocolo adicional al Convenio Europeo de Asistencia Judicial en Materia Penal, abierto a la firma el 17 de marzo de 1978 en Estrasburgo (STE nº 99).

2. Si dos o más Partes han celebrado ya un acuerdo o un tratado relativo a las cuestiones contempladas en el presente Convenio, o han regulado de otro modo sus relaciones al respecto, o si lo hacen en el futuro, podrán asimismo aplicar el citado acuerdo o tratado, o regular sus relaciones de conformidad con el mismo, en lugar del presente Convenio. No obstante, cuando las Partes regulen sus relaciones respecto de las cuestiones objeto del presente Convenio de forma distinta a la prevista en el mismo, lo harán de modo que no sea incompatible con los objetivos y principios del Convenio.

3. Nada de lo dispuesto en el presente Convenio afectará a otros derechos, restricciones, obligaciones y responsabilidades de cada Parte.

Artículo 40 – Declaraciones

Mediante declaración por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir, llegado el caso, uno o varios elementos complementarios previstos en los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e).

Artículo 41 – Cláusula federal

1. Un Estado federal podrá reservarse el derecho a cumplir las obligaciones especificadas en el Capítulo II del presente Convenio en la medida en que éstas sean compatibles con los principios fundamentales por los que se rijan las relaciones entre su gobierno central y los estados que lo constituyen u otras entidades territoriales análogas, a condición de que pueda garantizar la cooperación según lo previsto en el Capítulo III.

2. Cuando formule una reserva en virtud del párrafo 1, un Estado federal no podrá hacer uso de los términos de dicha reserva para excluir o reducir de manera sustancial sus obligaciones en virtud del Capítulo II. En todo caso, se dotará de medios amplios y efectivos para aplicar las medidas previstas en el citado Capítulo.

3. En lo relativo a las disposiciones del presente Convenio cuya aplicación sea competencia legislativa de cada uno de los estados constituyentes u otras entidades territoriales análogas, que no estén obligados por el sistema constitucional de la federación a adoptar medidas legislativas, el gobierno federal pondrá dichas disposiciones en conocimiento de las autoridades competentes de los estados constituyentes junto con su opinión favorable, alentándolas a adoptar las medidas adecuadas para su aplicación.

Artículo 42 – Reservas

Mediante notificación por escrito dirigida al Secretario del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el párrafo 2 del artículo 4, el párrafo 3 del artículo 6, el párrafo 4 del artículo 9, el párrafo 3 del artículo 10, el párrafo 3 del artículo 11, el párrafo 3 del artículo 14, el párrafo 2 del artículo 22, el párrafo 4 del artículo 29 y el párrafo 1 del artículo 41. No podrá formularse ninguna otra reserva.

Artículo 43 – Mantenimiento y retirada de las reservas

1. Una Parte que haya formulado una reserva de conformidad con el artículo 42 podrá retirarla total o parcialmente mediante notificación por escrito dirigida al Secretario General del Consejo de Europa. Dicha retirada surtirá efecto en la fecha en que el Secretario General reciba la notificación. Si en la notificación se indica una fecha a partir de la cual ha de hacerse efectiva la retirada de una reserva y esta fecha es posterior a la fecha en la que el Secretario General ha recibido la notificación, la retirada se hará efectiva en dicha fecha posterior.

2. Una Parte que haya formulado una reserva de las mencionadas en el artículo 42 retirará dicha reserva, total o parcialmente, tan pronto como lo permitan las circunstancias.

3. El Secretario General del Consejo de Europa podrá solicitar periódicamente a las Partes que hayan formulado una o varias reservas conforme a lo dispuesto en el artículo 42, información sobre las perspectivas de su retirada.

Artículo 44 – Enmiendas

1. Cada Parte podrá proponer enmiendas al presente Convenio, que el Secretario General del Consejo de Europa comunicará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado que se haya adherido o que haya sido invitado a adherirse de conformidad con lo dispuesto en el artículo 37.

2. Toda enmienda propuesta por cualquiera de las Partes será comunicada al Comité Europeo para Problemas Criminales (CDPC), quien someterá al Comité de Ministros su opinión sobre la enmienda propuesta.

3. El Comité de Ministros examinará la enmienda propuesta y la opinión presentada por el CDPC y, previa consulta con los Estados no miembros Partes en el presente Convenio, podrá adoptar la enmienda.

4. El texto de cualquier enmienda adoptada por el Comité de Ministros de conformidad con lo dispuesto en el párrafo 3 del presente artículo será remitido a las Partes para su aceptación.

5. Toda enmienda adoptada de conformidad con el párrafo 3 del presente artículo entrará en vigor treinta días después de que todas las Partes hayan informado al Secretario General de su aceptación.

Artículo 45 – Solución de controversias

1. Se mantendrá informado al Comité Europeo para Problemas Criminales (CDPC) del Consejo de Europa acerca de la interpretación y la aplicación del presente Convenio.

2. En caso de controversia entre las Partes sobre la interpretación o la aplicación del presente Convenio, las Partes intentarán llegar a un acuerdo mediante negociación o por cualquier otro medio pacífico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes en litigio, o a la Corte Internacional de Justicia, según acuerden dichas Partes.

Artículo 46 – Consultas entre las Partes

1. Las Partes se consultarán periódicamente, según sea necesario, con el fin de facilitar:

a. la utilización y la aplicación efectivas del presente Convenio, incluida la identificación de cualquier problema al respecto, así como las repercusiones de toda declaración o reserva formulada de conformidad con el presente Convenio;
b. el intercambio de información sobre novedades jurídicas, políticas o técnicas importantes observadas en el ámbito de la delincuencia informática y la obtención de pruebas en formato electrónico;
c. el estudio de la posibilidad de ampliar o enmendar el Convenio.

2. Se informará periódicamente al Comité Europeo para Problemas Criminales (CDPC) del resultado de las consultas mencionadas en el párrafo 1.

3. En caso necesario, el Comité Europeo para Problemas Criminales (CDPC) facilitará las consultas mencionadas en el párrafo 1 y adoptará las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Expirado un

plazo de tres años como máximo desde la entrada en vigor del presente Convenio, el CDPC procederá, en cooperación con las Partes, a una revisión de todas las disposiciones de la Convención y propondrá, si procede, las enmiendas pertinentes.

4. Salvo cuando el Consejo de Europa los asuma, los gastos que ocasione la aplicación de las disposiciones del párrafo 1 serán sufragados por las Partes, en la forma que ellas mismas determinen.

5. Las Partes recibirán asistencia del Secretario del Consejo de Europa en el ejercicio de las funciones que dimanan del presente artículo.

Artículo 47 – Denuncia

1. Las Partes podrán denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.

2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 48 – Notificación

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio, así como a cualquier Estado que se haya adherido o que haya sido invitado a adherirse al mismo:

a. cualquier firma;
b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;
c. cualquier fecha de entrada en vigor del presente Convenio de conformidad con los artículos 36 y 37;
d. cualquier declaración presentada de conformidad con el artículo 40 o cualquier reserva formulada en virtud del artículo 42;
e. cualquier otro acto, notificación o comunicación relativos al presente Convenio.

En fe de lo cual, los infrascritos, debidamente autorizados a tal efecto, firman el presente Convenio.

Hecho en Budapest, el 23 de noviembre de 2001, en versión francesa e inglesa, ambos textos igualmente auténticos, y en un ejemplar único que se depositará en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copia certificada a cada uno de los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del Convenio y a cualquier Estado invitado a adherirse al mismo.

ANTEPROYECTO DE DECRETO "LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS."

EQUIPO INTERINSTITUCIONAL CONFORMADO POR VARIAS INSTITUCIONES RELACIONADAS A LA TEMÁTICA EN ESTUDIO.

24 DE MARZO DE 2015.

DECRETO No. ___.-

LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR,

CONSIDERANDO:

I. Que la Constitución de la República, reconoce a la persona humana como el origen y el fin de la actividad del Estado, que está organizado para la consecusión de la justicia, de la seguridad jurídica y del bien común;

II. Que mediante Decreto Legislativo No. 1030, de fecha 26 de abril de 1997, publicado en el Diario Oficial No. 105, Tomo 335, del 10 de junio del mismo año, se emitió el Código Penal, como un instrumento normativo orientado a una concepción garantista;

III. Que en la actualidad, los instrumentos electrónicos por medio de los cuales se envía, recibe o resguarda la información, han adquirido una especial relevancia, tanto a nivel internacional como nacional, para el desarrollo económico, político, social y cultural del país; por lo que se vuelve prioridad del Estado, proteger dicha información, ya que al no protegerla se atenta contra la confidencialidad, integridad y disponibilidad de los datos en general;

IV. Que esta diversidad de actividades delincuenciales que pueden cometerse a través de las Tecnologías de la Información y la Comunicación, no se encuentran suficientemente reguladas en nuestra normativa penal vigente, generándose una impunidad para quienes cometen estos tipos de delitos; en consecuencia, resulta necesaria su tipificación y la adopción de mecanismos suficientes para facilitar su detección, investigación y sanción de estos nuevos tipos de delitos

V. Que en la actualidad la Cibercriminalidad constituye una grave amenaza para las personas naturales o jurídicas, la seguridad y la paz del país, afectando directa e indirectamente a sus nacionales en su integridad física y moral; así como en la propiedad, posesión y conservación de sus derechos, lo que vuelve necesario la creación de una Ley Especial a fin de proteger 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 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, intimidad e imagen de las personas naturales o jurídicas;

VI. Que mediante la emisión de la presente Ley Especial, se crea un cuerpo normativo útil y eficaz en la persecución y sanción de estos nuevos tipos de delitos y el crimen organizado, a fin de garantizar que no se cometan abusos contra la intimidad de las personas.

POR TANTO,

en uso de sus facultades constitucionales y a iniciativa de los Diputados ...

DECRETA, el siguiente:

LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS.

TÍTULO I
DISPOSICIONES GENERALES.

Objeto de la Ley.

Art. 1.- La presente Ley tiene por objeto proteger 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 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, intimidad e imagen de las personas naturales o jurídicas en los términos previstos en esta Ley.

Ambito de Aplicación.

Art. 2.- La presente Ley se aplicará a los hechos punibles cometidos total o parcialmente en el territorio nacional o en los lugares sometidos a su jurisdicción. También se aplicará a cualquier persona, natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, de sus habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador.

De igual forma, se aplicará la presente Ley si la ejecución del hecho, se inició en territorio extranjero y se consumó en territorio nacional o si se hubieren realizado, utilizando Tecnologías de la Información y la Comunicación instaladas en el territorio nacional y el responsable no ha sido juzgado por el mismo hecho por tribunales extranjeros o ha evadido el juzgamiento o la condena.

Definiciones.

Art. 3.- Para los efectos de la presente Ley, se entenderá por:

a) **Delito Informático:** se considerará la comisión de este delito, cuando se haga uso de las Tecnologías de la Información y la Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información;

b) **Bien Jurídico Protegido:** es la información que garantice y proteja el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros;

c) **Datos Informáticos:** es cualquier representación de hechos, información o conceptos en un formato digital, que permita el procesamiento en un sistema informático o la información misma, cualquiera que sea su ubicación;

d) **Medio de Almacenamiento de Datos Informáticos:** es cualquier dispositivo a partir del cual la información es capaz de ser leída, grabada, reproducida o transmitida con o sin la ayuda de cualquier otro medio idóneo;

e) **Sistema Informático:** es un elemento o grupo de elementos interconectados o relacionados, pudiendo ser electrónicos, programas informáticos, enlaces de comunicación o la tecnología que en el futuro los reemplace, orientados al tratamiento y administración de datos e información;

f) **Comunicación Electrónica:** es toda transmisión de datos informáticos, cuyo contenido puede consistir en audio, texto, imágenes, videos, caracteres alfanuméricos, signos, graficos de diversa índole o cualquier otra forma de expresión equivalente, entre un remitente y un destinatario a través de un sistema informático y las demás relacionadas con las Tecnologías de la Información y la Comunicación;

g) **Dispositivo:** es cualquier mecanismo, instrumento, aparato, medio que se utiliza o puede ser utilizado para ejecutar cualquier función de la Tecnología de la Información y la Comunicación;

h) **Interceptar:** es la acción de apropiarse, interrumpir, escuchar o grabar datos informáticos contenídos o transmitidos en cualquier medio informatico antes de llegar a su destino;

i) **Programa Informático:** es la rutina o secuencia de instrucciones en un lenguaje informático determinado que se ejecuta en un sistema informático, pudiendo ser este un ordenador, servidor o cualquier dispositivo, con el propósito que realice el procesamiento y comunicación de los datos infomáticos;

j) **Proveedor de Servicios:** es la persona natural o jurídica que ofrece uno o mas servicios de información o comunicación por medio de sistemas informáticos, procesamiento o almacenamiento de datos;

k) **Tráfico de Datos Informáticos:** son aquellos que se transmiten por cualquier medio tecnológico, pudiendo mostrar el origen, destino, ruta, hora, fecha, tamaño, duración de la comunicación, entre otros;

l) **Tecnologías de la Información y la Comunicación:** es el conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros;

m) **Datos Personales:** es la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra similar;

n) **Datos Personales Sensibles:** son los que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral, familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, a la propia imagen, a la intimidad personal y familiar;

o) **Material Pornográfico de Niñas, Niños y Adolescentes:** es toda representación auditiva o visual, ya sea en imagen o en vídeo, adoptando un

comportamiento sexualmente explícito, real o simulado de una persona que aparente ser niña, niño o adolescente adoptando tal comportamiento. También se considerará material pornográfico, las imágenes realistas que representen a una niña, niño o adolescente adoptando un comportamiento sexualmente explícito o las imágenes reales o simuladas de las partes genitales o desnudos de una niña, niño o adolescente con fines sexuales;

p) **Tarjeta Inteligente:** es el dispositivo que permite mediante la ejecución de un programa la obtención de bienes, servicios, propiedades o información; y,

q) **Redes Sociales:** es la estructura o comunidad virtual que hace uso de medios tecnológicos y de la comunicación para acceder, establecer y mantener algún tipo de vínculo o relación, mediante el intercambio de información.

TÍTULO II
DE LOS DELITOS.

CAPÍTULO I
DE LOS DELITOS CONTRA LOS SISTEMAS TECNOLÓGICOS DE INFORMACIÓN.

Acceso Indebido a Sistemas Informáticos.

Art. 4.- El que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o utilice parcial o totalmente un sistema informático que utilice las Tecnologías de la Información o la Comunicación, será sancionado con prisión de uno a cuatro años.

Acceso Indebido a los Programas o Datos Informáticos.

Art. 5.- El que a sabiendas y con la intención de usar cualquier dispositivo de la Tecnología de la Información o la Comunicación, accediera parcial o totalmente a cualquier programa o a los datos almacenados en él, con el propósito de apropiarse de ellos o cometer otro delito con éstos, será sancionado con prisión de dos a cuatro años.

Interferencia del Sistema Informático.

Art. 6.- El que sin justificación interfiera o altere el funcionamiento de un sistema informático, de forma temporal o permanente, será sancionado con prisión de tres a cinco años.

Se considerará agravada la interferencia o alteración, si ésta recayera en programas o sistemas informáticos públicos o en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión y transporte de energía, de medios de transporte u otro servicio público, la sanción de prisión será de tres a séis años.

Daños a Sistemas Informáticos.

Art. 7.- El que destruya, dañe, modifique, ejecute un programa o realice cualquier acto que altere el funcionamiento o inhabilite parcial o totalmente un sistema informático que utilice las Tecnologías de la Información y la Comunicación o cualquiera de los componentes que las conforman, será sancionado con prisión de tres a cinco años.

Incurrirá en la misma pena quien destruya, dañe, modifique, ejecute un programa o inhabilite los datos informáticos contenidos en cualquier sistema informático parcial o totalmente que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes.

Si el delito previsto en el presente artículo se cometiere de forma culposa, por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, será sancionado con prisión de uno a tres años.

Si el delito previsto en el presente artículo se cometiere en contra de cualquiera de los componentes de un sistema informático que utilicen las Tecnologías de la Información y la Comunicación, que estén destinadas a la prestación de servicios públicos o que contengan información personal, confidencial, reservada, patrimonial, técnica o propia de personas naturales o jurídicas, la sanción de prisión será de tres a seis años.

Posesión de Equipos o Prestación de Servicios para la Vulneraración de la Seguridad.

Art. 8.- El que utilizando las Tecnologías de la Información y la Comunicación posea, produzca, facilite o venda equipos, dispositivos o programas informáticos, contraseñas o códigos de acceso, con el propósito de vulnerar o eliminar ilegítimamente la seguridad de cualquier sistema informático o de cometer cualquiera de los delitos establecidos en la presente Ley, será sancionado con prisión de tres a cinco años.

Violación de la Seguridad del Sistema.

Art. 9.- La persona que sin poseer la autorización correspondiente transgrede la seguridad de un sistema informático restringido o protegido con mecanismo de seguridad específico, será sancionado con prisión de tres a seis años.

CAPÍTULO II
DE LOS DELITOS INFORMÁTICOS.

Estafa informática.

Art. 10.- La persona natural o jurídica que manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que utilice Tecnologías de la Información y la Comunicación, 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 o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro, será sancionado con prisión de tres a cinco años.

Será sancionado con prisión de cinco a ocho años, si las conductas descritas en el inciso anterior se cometieren bajo los siguientes presupuestos:

a) En perjuicio de propiedades del Estado;

b) Contra sistemas bancarios y entidades financieras;

c) Cuando el autor sea un empleado encargado de administrar, dar soporte al sistema, red informática, telemática, o que en razón de sus funciones tenga acceso a dicho sistema o red, a los contenedores electrónicos, ópticos o magnéticos.

Fraude Informático.

Art. 11.- El que por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes; o en la de datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho en perjuicio ajeno, será sancionado con prisión de tres a seis años.

Espionaje Informático.

Art. 12.- El que indebidamente obtenga datos o información reservada o confidencial contenidas en un sistema que utilice Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, será sancionado con prisión de cinco a ocho años.

Si alguna de las conductas descritas en el inciso anterior se cometieren con el fin de obtener beneficio para sí o para otro, o si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de la información de carácter reservada o confidencial, la sanción será de seis a diez años de prisión.

Hurto por Medios Informáticos.

Art. 13.- El que por medio del uso de las Tecnologías de la Información y la Comunicación, se apodere de bienes o valores tangibles o intangibles de carácter personal o patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de tres a cinco años.

Técnicas de Denegación de Servicio.

Art. 14.- El que de manera intencionada, utilizando las técnicas de la denegación de servicio o prácticas equivalentes que afectaren a los usuarios que tienen pertenencia en el sistema o red afectada, impidiéndoles obtener el servicio, será sancionado con prisión de tres a cinco años.

Desabilitación de Registros.

Art. 15.- Los Administradores de las Plataformas Tecnológicas de instituciones públicas o privadas, que intencionalmente deshabiliten cualquier información o dato contenido en un registro de acceso o uso de los componentes de éstos, será sancionado con prisión de cinco a ocho años.

Manipulación Fraudulenta de Tarjetas Inteligentes o Instrumentos Similares.

Art. 16.- El que intencionalmente y sin la debida autorización por cualquier medio cree, capture, grabe, copie, altere, duplique, clone o elimine, tanto datos informáticos

contenidos en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; como datos informáticos en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será sancionado con prisión de cinco a ocho años.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin o de datos informáticos contenidos en ellos o en un sistema.

Obtención Indebida de Bienes o Servicios por medio de Tarjetas Inteligentes o Medios Similares.

Art. 17.- El que sin autorización utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente las Tecnologías de la Información y la Comunicación para la obtención de cualquier bien o servicio; o para proveer cualquier tipo de pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será sancionado con prisión de tres a ocho años.

Provisión Indebida de Bienes o Servicios.

Art. 18.- El que sin justificación, a traves de un sistema informático utilice tarjetas inteligentes o instrumentos similares destinados a los mismos fines, cuya vigencia haya caducado o haya sido revocada por la institución que la emitió, o que se haya obtenido con el fin de suplantar la identidad contenida en dichas tarjetas inteligentes, será sancionado con prisión de cinco a ocho años.

El que falsifique o altere los datos de las tarjetas inteligentes o instrumentos similares, con el fin de proveer a quien los presente, dinero, bienes o servicios, o cualquier otro objeto de valor económico, la sanción aumentará hasta una tercera parte del máximo de la pena prevista en el inciso anterior.

Alteración, Daño a la Integridad y Disponibilidad de los Datos.

Art. 19.- El que intencionalmente, por cualquier medio destruya, altere, inutilice o dañe de cualquier otro modo los datos en cuanto a su integridad, disponibilidad y confidencialidad en cualquiera de sus estados de procesamiento, transmisión o almacenamiento, programas, documentos electrónicos ajenos, contenidos en redes relacionados a sitios web, páginas de soporte o sistemas informáticos, será sancionado con prisión de tres a seis años.

CAPÍTULO III
DELITOS INFORMÁTICOS RELACIONADOS CON EL CONTENIDO DE LOS DATOS.

Interferencia de Datos.

Art. 20.- El que interfiera, obstruya o interrumpa el uso legítimo de datos o los produce nocivos e ineficaces para alterar o destruir los datos de un tercero, será sancionado con prisión de tres a seis años.

Si alguna de las conductas descritas en el inciso anterior recae sobre datos, documentos, programas o sistemas informáticos públicos o sobre datos destinados a la prestación de servicios de salud, de comunicaciones, sistemas bancarios, entidades financieras, de provisión y transporte de energía, de medios de transporte u otro servicio público, la sanción de prisión será de cinco a ocho años.

Interceptación de Trasmisiones entre Sistemas de las Tecnologías de la Información y la Comunicación.

Art. 21.- La persona que sin justificación intercepte por medios técnológicos cualquier transmisión hacia, desde o dentro de un sistema informático que no está disponible al público; o las emisiones electromagnéticas que están llevando datos informáticos de un sistema informático, será sancionada con prisión de tres a diez años.

Hurto de Identidad.

Art. 22.- El que se apoderare de la identidad de una persona natural o jurídica por medio de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de tres a cinco años.

Si con la conducta descrita en el inciso anterior se daña, extorsiona, defrauda, injuria o amenaza a otra persona para obtener beneficios para si mismo o para terceros y el apoderamiento recae sobre datos personales sensibles, será sancionado con prisión de cinco a ocho años.

Divulgación No Autorizada.

Art. 23.- El que sin autorización da a conocer un código o contraseña de acceso o cualquier otro medio de acceder a cualquier programa o datos almacenados en un equipo o dispositivo tecnológico, con el fin de lucrarse para si mismo, para un tercero o

para cometer un delito o para causar daño, será sancionado con prisión de cinco a ocho años.

Igual sanción tendrá el que sin autorización revele o difunda los datos o información contenidos en un sistema informático que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, con el fin de obtener algún tipo de beneficio para sí o para otro.

Si alguna de las conductas descritas en los incisos anteriores pusieren en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado, será sancionado con prisión de seis a doce años.

Difusión de Información Perjudicial.

Art. 24.- El que haciendo uso de las Tecnologías de la Información y la Comunicación, difunda información,imágenes, audios, videos o cualquier medio cuyo contenido cause perjuicio o dañe la dignidad, el honor, ponga en peligro la integridad física o moral de una persona, será sancionado con prisión de tres a cinco años.

Utilización de Datos Personales.

Art. 25.- El que sin autorización utilice datos personales a través del uso de las Tecnologías de la Información y la Comunicación, violando sistemas de confidencialidad y seguridad de datos, insertando o modificando los datos en perjuicio de un tercero, será sancionado con prisión de cuatro a seis años.

La sanción aumentará hasta en una tercera parte del máximo de la pena prevista en el inciso anterior a quien proporcione o revele a otro, información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar.

Obtención y Transferencia de Información de Carácter Confidencial.

Art. 26.- El que deliberadamente obtenga y transfiera información de carácter confidencial y que mediante el uso de esa información vulnere un sistema o datos informáticos apoyándose en cualquier clase de las Tecnologías de la Información y la Comunicación, incluidas las emisiones electromagnéticas, será sancionado con prisión de cinco a ocho años.

Revelación Indebida de Datos o Información de Carácter Personal.

Art. 27.- El que sin el consentimiento del titular de la información de carácter personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean estos en imágenes, video, texto, audio o en general, obtenidos por alguno de los medios indicados en los artículos precedentes, será sancionado con prisión de tres a cinco años.

Si alguna de las conductas descritas en el inciso anterior, se hubiese realizado con ánimo de lucro o la comisión de otro delito en perjuicio de un tercero, será sancionado con prisión de cuatro a ocho años.

Se impondrá el límite máximo de la pena del inciso anterior, aumentado hasta en una tercera parte, si alguna de las conductas descritas en el inciso primero del presente artículo, recae sobre datos personales sensibles.

Acoso a través de Tecnologías de la Información y la Comunicación.

Art. 28.- El que realice conducta sexual indeseada por quien la recibe, que implique frases, señas u otra conducta inequívoca de naturaleza o contenido sexual, por medio de las redes sociales o cualquier otro tipo de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de tres a cinco años.

CAPÍTULO IV
DELITOS INFORMÁTICOS CONTRA NIÑAS, NIÑOS Y ADOLESCENTES O PERSONAS CON DISCAPACIDAD.

Pornografía a través del Uso de Tecnologías de Información y la Comunicación.

Art. 29.- El que por cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación fabrique, transfiriera, difunda, distribuya, alquile, venda, ofrezca, produzca, ejecute, exhiba o muestre material pornográfico o de contenido sexual entre niñas, niños y adolescentes o personas con discapacidad, será sancionado con prisión de cuatro a ocho años.

El que no advierta de forma visible, para que el usuario restrinja el acceso a niñas, niños y adolescentes o personas con discapacidad, será sancionado con prisión de tres a cinco años.

Utilización de Niñas, Niños y Adolescentes o Personas con Discapacidad en Pornografía a través del Uso de las Tecnologías de la Información y la Comunicación.

Art. 30.- El que por cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación produzca, reproduzca, distribuya, publique, importe, exporte, ofrezca, financie, venda, comercie o difunda de cualquier forma, imágenes o exhiba en actividades sexuales, eróticas o inequívocas de naturaleza sexual, explícitas o no, reales o simuladas, o utilice la voz de niñas, niños y adolescentes o personas con discapacidad, será sancionado con prisión de seis a doce años.

El que por medio de las Tecnologías de la Información y la Comunicación organize o participe en espectáculos, en los que se hace participar a las personas señaladas en el inciso anterior, en acciones pornográficas o eróticas, será sancionado con prisión de cuatro a ocho años.

Adquisición o Posesión de Material Pornográfico de Niñas, Niños y Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación.

Art. 31.- El que adquiera para sí o para un tercero a través de cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación, material pornográfico en el que se haya utilizado a una niña, niño y adolescente o persona con discapacidad, o su imagen para su producción, será sancionado con prisión de tres a cinco años.

Igual sanción se aplicará al que posea en dispositivos de almacenamiento de datos informáticos o a través de cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación, material pornográfico en el que se haya utilizado a una niña, niño y adolescente o persona con discapacidad, o su imagen para su producción.

Corrupción de Niñas, Niños y Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación.

Art. 32.- El que mantenga promueva o facilite la corrupción de una niña, niño y adolescente o persona con discapacidad con fines eróticos, pornográficos u obscenos, por medio de las redes sociales o de las Tecnologías de la Información y la Comunicación, aunque la niña, niño y adolescente o persona con discapacidad lo consienta, será sancionado con prisión de seis a doce años.

Esta misma sanción tendrá, quien haga propuestas explícitas para sostener encuentros de carácter sexual o erótico, o para la producción de pornografía a través de las redes sociales o cualquier otro medio de las Tecnologías de la Información y la Comunicación para sí, para otro o para grupos, con una niña, niño y adolescente o persona con discapacidad.

Acoso a Niñas, Niños y Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación.

Art. 33.- El que realice conducta que implique frases, señas u otra acción inequívoca de naturaleza o contenido sexual contra una niña, niño y adolescente o persona con discapacidad, por medio de las redes sociales o cualquier otro medio de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de cuatro a ocho años.

Condiciones Agravantes Comunes.

Art. 34.- Los delitos referidose en el presente Capitulo, serán sancionados con la pena máxima correspondiente, aumentada hasta en una tercera parte del máximo establecido de la pena y la inhabilitación del ejercicio de su profesión durante el tiempo que dure la condena, si cualquiera de las acciones descritas fuera realizada por:

a) Ascendientes, descendientes, hermanos, adoptantes, adoptados, cónyuges, conviviente y familiares hasta el cuarto grado de consanguinidad y segundo de afinidad;

b) Funcionarios, empleados públicos y municipales, autoridad pública y agente de autoridad;

c) La persona encargada de la tutela, protección o vigilancia de la víctima; y,

d) Toda persona que prevaliéndose de la superioridad originada por relaciones de confianza, doméstica, educativa, de trabajo o cualquier otra relación.

CAPÍTULO V
DELITOS CONTRA EL ORDEN ECONÓMICO.

Aprovechamiento Indebido de la Propiedad Intelectual.

Art. 35.- El que sin autorización de su propietario plagie, reproduzca, modifique, copie, distribuya o divulgue en todo o en parte una obra del intelecto que haya obtenido indebidamente mediante el acceso a cualquier sistema. que utilice de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de tres a cinco años.

En la misma sanción incurrirá, el que a escala comercial inporte, exporte o almacene ejemplares de las obras a las que se hace referencia en el inciso anterior, sin la debida autorización.

La pena se agravará con prisión de seis a ocho años, cuando se comentan las conductas descritas en el inciso primero del presente artículo, cuando se haya obtenido una ventaja comercial o ganancia económica privada.

Oferta Engañosa.

Art. 36.- El que sin autorización y a nombre de un tercero comercialice bienes o servicios mediante el uso de las Tecnologías de la Información y la Comunicación, haga alegaciones falsas, difunda ofertas o atribuya características inciertas vinculadas a un producto o servicio para los consumidores, será sancionado con prisión de tres a cinco años.

TÍTULO III
DISPOSICIONES FINALES.

Otras Responsabilidades.

Art. 37.- Las sanciones previstas en la presente Ley, serán aplicables sin perjuicio de otras responsabilidades penales, civiles o administrativas en que se incurra.

Vigencia.

Art. 38.- El presente Decreto entrará en vigencia ocho días después de su publicación en el Diario Oficial.

DADO EN EL SALÓN AZUL DEL PALACIO LEGISLATIVO: San Salvador, a los ____ días del mes de _____ del año dos mil quince.

RARC/***

POLICÍA NACIONAL CIVIL
EL SALVADOR
Servicio, Orden, Seguridad

Seleccionar idioma

PNC refleja más de cien denuncias por delitos cibernéticos

Galería de Fotos

Anterior Siguiente

EQUIDAD E IGUALDAD DE

En el combate a los delitos cibernéticos.

El director de la Policía Nacional Civil (PNC) comisionado Mauricio Ramírez Landaverde, dijo hoy que en el año 2014 la institución reflejó cerca de un centenar de denuncias por delitos cibernéticos, al tiempo que afirmó que desde 1999 se viene trabajando en el tema, con UNICEF, específicamente para abordar la persecución y prevención de la pornografía infantil.

El jefe de policía sostuvo que con la firma del memorando de entendimiento firmado hoy con la oficina de Naciones Unidas contra la droga y le delito para Centroamérica y el caribe(UNOCDC-ROPAN) vendrá a fortalecer y especializar al grupo de investigadores , quienes ya pronto conformaran una unidad especializada para darle el status correspondiente aseveró el Comisionado Ramírez Landaverde.

De las cien denuncias o casos que se conocen, en su mayoría están vinculados a delitos contra la libertad sexual, acoso sexual, pornografía infantil, trata de personas y otros amenazas, extorsiones , estafas entre otros, señaló el comisionado Landaverde.

Enlaces Externos

- Inspectoría PNC
- Policía Turismo
- Misiones de Paz
- Ameripol

Lo que se busca es que sus miembros adquieran las capacidades necesarias para la prevención y un combate más efectivo de los delitos informáticos, para que aborden la informática forense, el manejo de las evidencias digitales, el uso de software especializados, la recuperación de información en computadoras, teléfonos móviles y otros dispositivos.

Según explicó el comisionado Landaverde el tipo de delitos cibernéticos que se cometen en nuestro país están relacionados a las estafas, delitos contra la vida y la integridad sexual principalmente.

A nivel regional delitos cibernéticos.

El representante regional de la oficina de Naciones Unidas contra la droga y el delito para Centroamérica y el Caribe (UNODC-ROPAN) Amado Philip de Andrés, dijo que muchos de los países que tienen las tazas de crecimiento por encima del 3% son más proclives a tener mayor incidencia de delitos cibernéticos

ZONA1

¿DÓNDE ESTOY? | REPORTAJES

Junio 19, 2014

Le roban una foto desnuda, la suben a la red y su caso queda impune

La intimidad de Catalina, una joven salvadoreña, quedó expuesta en internet luego de que imágenes en las que aparecía con poca ropa fueran hurtadas de su laptop. Pensó en demandar, pero la poca respuesta institucional, sumando amenazas que recibió, frustraron su intento de hacer justicia.

D1 diario1.com
Julia Gavarrete

Foto D1.

La soledad la desorientaba y provocaba que sus nervios se dispararan sin control. Empapada de desánimo y decepción, sentía que su vida no tenía brújula. Catalina apenas digería que un pequeño descuido -o quizás un error que pudo haber evitado- provocara que unas fotografías, tomadas cinco años atrás, fueran filtradas de pronto en el inmenso mar cibernético al que cualquiera tiene libre acceso de navegar.

Su cuerpo estaba al descubierto y expuesto a los ojos de quien la buscara. Catalina

Exhibición de alto costo

En abril el video de una madre azotando a su hija se hizo viral en internet. Los medios y los mismos usuarios de YouTube compartían el momento en el que una menor de 12 años era castigada por compartir imágenes con poca ropa en su perfil de Facebook. La adolescente, originaria de Trinidad y Tobago, fue castigada a golpe de un cincho por una madre llena de furia e indignación.

La incontrolable señora repetía que así aprendería a no nutrir una página con imágenes en ropa interior y mucho menos a decir que tenía 21 años. La joven pedía clemencia, pero la madre le decía, soltando un cinchazo, que "acá tendría su like". El video terminó compartido en la red por la misma familia de la menor. Si hizo conciencia o no en su hija, fue el tipo de castigo lo que desprendió una avalancha de críticas en contra de la menor, quien llegó a ser calificada hasta de exhibicionista.

En Facebook la divulgación de contenido, bajo autorización o no, se ha vuelto frecuente. Fotografía de mujeres desnudas o con poca ropa son compartidas sin control alguno, sobre todo cuando la empresa estadounidense se guarda el derecho de publicar el contenido si lo considera o no inapropiado.

La Pagina
Más rápido y veraz

Sujeto que difundió imágenes íntimas de su novia fue condenado a 15 años de prisión

La acción fue en represalia porque la joven, que en ese momento tenía 19 años, decidió cortar la relación sentimental que sostuvieron por varios meses.

ÚLTIMA ACTUALIZACIÓN: 30 DE ABRIL DE 2015 23:35 | POR JOSÉ NAPOLEÓN MORALES

El juzgado Sexto de Sentencia de San Salvador ordenó 15 años de prisión contra Carlos Guillermo Centeno Avelar por haber difundido en las redes sociales fotos íntimas de su novia.

Centeno Avelar, de 41 años, publicó las fotos y videos de su novia en los momentos en que sostenía relaciones sexuales con él.

La acción fue en represalia porque la joven, que en ese momento tenía 19 años, decidió cortar la relación sentimental que sostuvieron por varios meses.

Según el requerimiento fiscal, las imágenes que se difundieron en las redes sociales corresponden al año 2012, cuando la ofendida tenía 17 años. Por esta razón fue acusado de estupro, difusión de información y por expresiones de violencia contra la mujer.

Según la Fiscalía, cuando la joven puso fin al noviazgo el imputado decidió publicar el material y lo envió a los contactos de ella, debido a que tenía acceso a todas sus cuentas en redes sociales

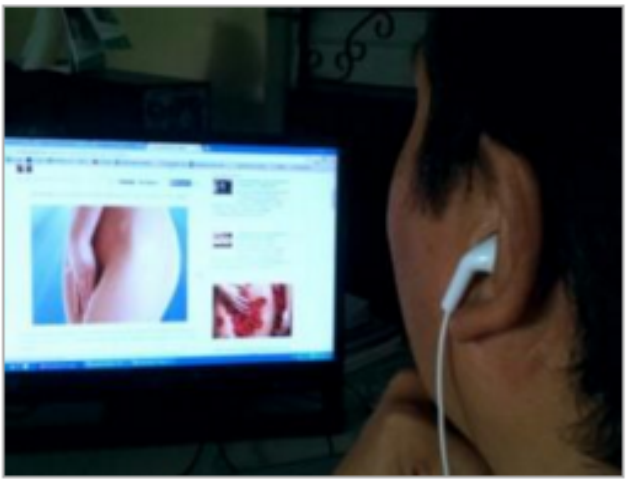
Las imágenes llegaron a la cuenta del padre de su exnovia y, tras ser increpada, ésta dijo que el único hombre con quien había sostenido relaciones sexuales fue con su exnovio.

Al ser detenido, las autoridades localizaron en la computadora de Centeno Avelar las fotos

Capturan a salvadoreño por difundir fotos y videos íntimos de su novia en redes sociales

El hombre de 40 años subió las fotografías y videos de momentos "íntimos" con su novia, 20 años menor que él, porque esta decidió poner fin a la relación que tenían.

ÚLTIMA ACTUALIZACIÓN: 22 DE JULIO DE 2014 19:37 | POR CARMEN RODRÍGUEZ



Un hombre de 40 años que subió fotos y videos íntimos de su exnovia fue detenido hoy por las autoridades. Según la denuncia de la joven de 19 años, el despecho del sujeto lo motivó a publicar las fotos en todas sus cuentas de redes sociales.

Por el caso, Carlos Guillermo Centeno Avelar enfrentará cargos por los delitos de estupro, difusión de información y expresiones de violencia contra la mujer en perjuicio de su exnovia.

De acuerdo al informe fiscal, la joven era menor de edad cuando se tomaron las fotografías y se grabaron los videos. Las imágenes fueron captadas en febrero de 2012, cuando la muchacha tenía 17 años.

Segun la Fiscalía, al ver que la mujer puso fin a la relación de noviazgo que tenían, en abril de este año, Centeno decidió publicar el material y enviarlo a los contactos de la mujer, aprovechando que tenía acceso a todas las cuentas de redes sociales de la joven.

SUJETO QUE FILTRÓ VIDEO DE SEXO CON SU NOVIA DE LA UCA PODRÍA PAGAR CON 10 AÑOS DE CÁRCEL

Un sujeto grabó un video que fue subido a un sitio web pornográfico de Estados Unidos, en donde aparece teniendo relaciones sexuales con su novia estudiante de la UCA.

En el video de más de cinco minutos, el joven trata a la estudiante con palabras obscenas quien aunque sabía que estaba siendo grabada, nunca se imaginó que las escenas se subirían a un sitio pornográfico internacional.

El sitio No Más Violencia afirmó que "anda circulando un paquete de fotos y videos de una chica de la UCA teniendo sexo y siendo grabada por su pareja".

"Las autoridades de la universidad ya están tratando el caso y esperan que las autoridades salvadoreñas hagan pronta justicia en el caso", aseguró una fuente universitaria a revista Portadas TV. Según la versión de algunos estudiantes entrevistados, la estudiante es una de las más destacadas de su carrera.

"En esa misma pista anda circulando que quién subió este material fue el mismo tipo por venganza, la cual fue declarada abiertamente tras su ruptura", afirma el sitio. Sea cual sea el motivo de la ruptura, haya sido culpa de ella o no, este tipo de delitos son castigados con cárcel según en Código Penal de 3 a 5 años.

El sujeto también podría ser condenado por violar la Ley Especial Integral para Una Vida Libre de Violencia contra las Mujeres, que también da una pena máxima de hasta cinco años.

Si se suman ambas penas con tipificaciones de delitos distintos, la pena a pagar por quien subió o grabó sin consentimiento el video, sería de 10 años.

"Si es verdad lo de la venganza, este tipejo asesinó emocional, familiar, social, académica, profesionalmente y mucho más a una persona. Pocas palabras hay para describir a este criminal emocional, basta con ver sus publicaciones en sus redes, ataca a los homosexuales, a las clases sociales bajas y denigra a las mujeres", afirma el sitio.

Mauricio Béjar Jaddalah
Jul 5, 2015 at 5:32pm

Como que no fuera suficiente que tu ex pareja te haya transmitido un hongo, te venís a dar cuenta que también roló por buena parte de los habitantes del Municipio de San Salvador y Municipios aledaños estando con vos... uno nunca termina de conocer a las personas.

9 likes 4 comments

Like Comment Share

Mauricio Béjar Jaddalah
July 3 at 11:47pm

Si van a tener amigos gay que sean como Michel Foucault, no algún gay socialité sin cerebro, si es que ustedes dicen tener cerebro.

2 Likes · 1 Comment

Share

Mauricio Béjar Jaddalah
July 3 at 11:18pm

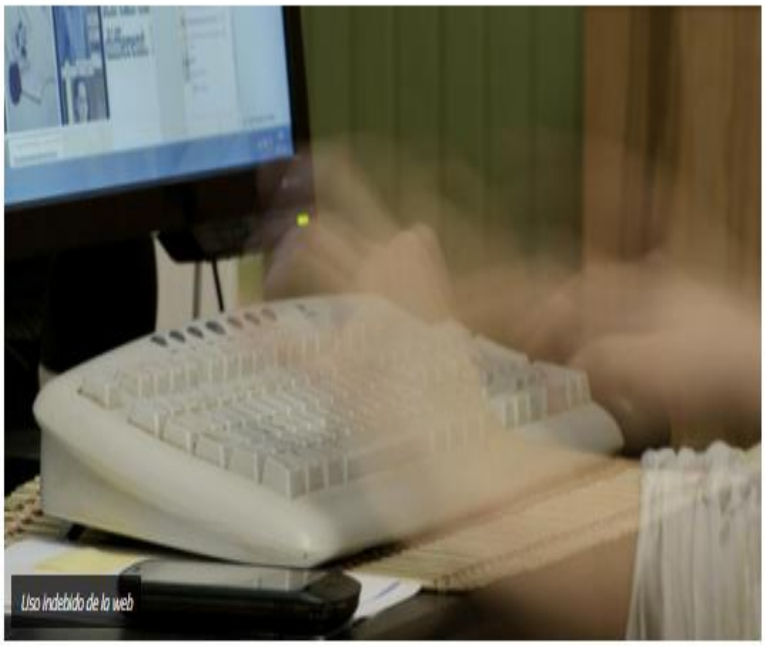
Ahí andan anhelando ir Viernes y Sábados al Club Árabe, a Circo, a Chafa, entre otros. Imbéciles igualados e igualadas, deberían de saber que esos lugares se hicieron para disfrute de la burguesía y entre más "gusanos" como ustedes lleguen, menos la burguesía los va a frecuentar. Por favor ubíquense en su clase social.

11 Likes · 2 Comments

Share

EXPOSICIÓN DE LA INTIMIDAD EN REDES SOCIALES. INTIMIDAD, PRIVACIDAD Y HONOR

BY EDITORIAL - 2 FEBRERO, 2015



Uso indebido de la web

California, un hombre fue condenado a un año de prisión luego que publicara fotografías de su exnovia semidesnuda en la cuenta de Facebook de la empresa donde la mujer trabaja, en el perfil de su empleador, sentencia lograda como resultado de la aprobación, el treinta de septiembre del dos mil catorce, de un nuevo paquete normativo comúnmente llamado "ley contra la porno venganza", la cual regula la prohibición de la difusión de las fotografías tomadas por la propia víctima, atendiendo a su derecho a la privacidad. Un modo de operar, se da mediante la publicación en portales creados específicamente para este fin, de fotografías de desnudos, semidesnudos o con carácter sexual de una persona con la que se ha tenido una disputa, habitualmente una expareja, típicamente por venganza.

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

DEPARTAMENTO DE CIENCIAS JURIDICAS

DISEÑO DE ENTREVISTA ESTRUCTURADA A PROFUNDIDAD PARA REALIZAR AL JEFE DE LA FISCALIA GENERAL DE LA REPUBLICA REGIONAL SANTA ANA.

1- **¿Desde hace cuanto tiempo labora usted para la Fiscalía General de la República**
2- **¿Podría describirnos usted el cargo que realiza para la institución?**
3- **Podría decirnos ¿cuál es el área donde usted se desenvuelve en la institución?**
4- **Partiendo de su experiencia y conocimiento podría usted decirnos ¿qué es para usted un ciberdelito?**
5- **De acuerdo a su conocimiento y al cargo que desempeña conoce algún tipo de conductas lesivas al honor y la intimidad cometidas a través de redes sociales.**
6- **Con la experiencia que su cargo le ha generado ¿Cuál ley se aplica a todas aquellas conductas que lesionan el honor y la intimidad, de las personas y son cometidas a través de internet?**
7- **En la calidad que usted actúa cual es el procedimiento que la Fiscalía tiene para indagar el cometimiento de un posible delito cometido utilizando como medio el internet.**

8- **En su Calidad: de Jefe de la Fiscalía Regional Santa Ana ¿Cuáles creen que son las medidas que la institución debe considerar para el conocimiento a futuro de conductas lesivas cuyo medio de cometimiento sea internet?**

9- **De acuerdo a su conocimiento y su función ¿cuál es el medio idóneo para probar la realización de una conducta lesiva cometida a través de internet?**

10- **Podría decirnos si la institución para la que usted labora cuenta con los recursos y medios técnicos necesarios para conocer de este tipo de conductas lesivas.**

11- **Desde el cargo que usted desempeña cree usted que el factor cultura de la población del departamento de Santa Ana, ha sido un obstáculo, para tener conocimiento de casos de realización de conductas lesivas cometidas a través de internet especialmente a través de redes sociales.**

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

DEPARTAMENTO DE CIENCIAS JURIDICAS

DISEÑO DE ENTREVISTA ESTRUCTURADA A PROFUNDIDAD PARA REALIZAR EN LA PROCURADURIA GENERAL DE LA REPUBLICA REGIONAL SANTA ANA.

.

1- **¿Desde hace cuanto tiempo labora usted para la Procuraduría General de la República**
2- **¿Podría describirnos usted el cargo que desempeña para la institución?**
3- **¿Podría decirnos cuál es el área específica donde usted labora en la institución en referencia?**
4- **Partiendo de su experiencia y conocimiento podría decirnos ¿si se han presentado personas a esta institución acusadas de cometer un Ciberdelito?**
5- **De acuerdo a su conocimiento y a la labor que desempeña ¿ha defendido algún tipo de conducta lesiva al honor y la intimidad cometidas a través de redes sociales?**
6- **Con la experiencia que su cargo le ha generado si tuviera la oportunidad de defender una conducta de este tipo ¿Qué ley ocuparía como fundamento para realizar la defensa?**

7- **En su Calidad de procurador ¿Cuáles creen que son las medidas que la institución debería implementar para el conocimiento a futuro de las conductas lesivas cuyo medio de cometimiento sea el internet?**
8- **De acuerdo a su conocimiento y práctica ¿cuál es el medio idóneo para desvirtuar la realización de una conducta lesiva cometida a través de internet?**
9- **Podría decirnos ¿si la institución para la que usted labora cuenta con los recursos y medios técnicos necesarios para investigar y conocer este tipo de conductas lesivas?**
10- **En su calidad de representante de la procuraduría General de la República Regional Santa Ana ¿Que reformas recomendaría en la legislación Penal vigente, en lo relativo a los Ciberdelitos?**
11- **Desde el cargo que usted desempeña cree usted que el factor cultura de la población del departamento de Santa Ana, ha sido un obstáculo, para que la Procuraduría tenga conocimiento de casos de realización de conductas lesivas cometidas a través de internet especialmente a través de redes sociales.**

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

DEPARTAMENTO DE CIENCIAS JURIDICAS

DISEÑO DE ENTREVISTA ESTRUCTURADA A PROFUNDIDAD PARA REALIZAR AL JUEZ DEL TRIBUNAL PRIMERO DE SENTENCIA DE SANTA ANA.

1- **Podría decirnos ¿cuál es el nombre de la institución para la que usted labora?**
2- **¿Podría describir usted la función que desempeña la institución en la que usted labora?**
3- **¿Describa de manera específica cuales son las funciones que realiza dentro de la institución que representa?**
4- **¿Desde hace cuanto tiempo usted labora para esta institución?**
5- **Partiendo de su experiencia y conocimiento podría explicarnos si conoce usted delitos cibernéticos o ciberdelitos?**
6- **Según su experiencia podría decirnos si conoce leyes utilizadas para regular los ciberdelitos en la actualidad.**
7- **Según su conocimiento ¿Cuál es el criterio profesional que usted tiene en lo relativo a las conductas lesivas, usando como medio el internet específicamente las relativas al honor y la intimidad?**
8- **En su calidad de Juez ¿cuál es el papel que debería desempeñar el Estado respecto a las conductas lesivas cometidas a través de internet?**
9- **Según su experiencia podría Describir, si existen disposiciones legales a reformar de la legislación vigente para para poder sancionar las conductas**

lesivas utilizando como medio para la realización el internet específicamente las redes sociales.

10-Considerando su conocimiento y experiencia ¿cree usted necesaria la creación de un cuerpo normativo especial que regule las conductas realizadas a través de internet?

11-Desde el cargoque usted desempeña, el factor cultural y educacional de la población del Departamento de Santa Ana es un obstáculo para el conocimiento de las conductas lesivas cometidas a través de internet especialmente a través de redes sociales.