

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES
ESCUELA DE CIENCIAS JURÍDICAS



ALCANCES Y LIMITANTES DEL ARTÍCULO 26 DE LA LEY ESPECIAL
CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS, EN RELACIÓN A
LA REVELACIÓN INDEBIDA DE DATOS O INFORMACIÓN DE CARÁCTER
PERSONAL DE LAS MUJERES EN EL SALVADOR

TRABAJO DE GRADO PARA OBTENER EL TÍTULO DE LICENCIADO (A)
EN CIENCIAS JURÍDICAS

PRESENTADO POR:

HERNÁNDEZ DE LIMA, CONSUELO CAROLINA
PÉREZ ARABIA, DIANA MARGARITA
SERRANO ORELLANA, FLOR DE MARÍA

DOCENTE ASESOR:

MSC. ALEJANDRO BICMAR CUBÍAS RAMÍREZ

CIUDAD UNIVERSITARIA, SAN SALVADOR, MAYO DE 2020

TRIBUNAL CALIFICADOR

LIC. FRANCISCO OPORTO

PRESIDENTE

DRA. SANDRA CAROLINA RENDÓN RIVERA

SECRETARIO

MSC. ALEJANDRO BICMAR CUBÍAS RAMÍREZ

VOCAL

UNIVERSIDAD DE EL SALVADOR

Msc. Roger Armando Arias Alvarado

RECTOR

PhD. Raúl Ernesto Azcúnaga López

VICERRECTOR ACADEMICO

Ing. Juan Rosa Quintanilla

VICERRECTOR ADMINISTRATIVO

Ing. Francisco Antonio Alarcón

SECRETARIO GENERAL

Lic. Rafael Humberto Peña Marín

FISCAL GENERAL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

Dra. Evelyn Beatriz Farfán Mata

DECANA

Dr. Edgardo Herrera Medrano Pacheco

VICEDECANO

Licda. Digna Reyna Contreras de Cornejo

SECRETARIA

Msc. Hugo Dagoberto Pineda

DIRECTOR DE ESCUELA DE CIENCIAS JURIDICAS

Licda. Diana del Carmen Merino de Sorto

DIRECTORA GENERAL DE PROCESOS DE GRADUACIÓN

Msc. María Magdalena Morales

COORDINADORA DE PROCESO DE GRADUCACIÓN DE LA ESCUELA DE
CIENCIAS JURÍDICAS

Dedicatoria

Al dueño de mi vida, Dios todo poderoso y su madre inmaculada por nunca abandonarme a lo largo de mi carrera y cargarme cuando ya no tenía fuerzas para seguir, a ellos los dueños de todo lo que soy y lo que tengo gracias por tener misericordia de mí y amarme sin condición.

A mi amada mamá por ser el ejemplo de mujer que ha sido, por enseñarme a luchar por mis sueños pero sobre todo por siempre creer en mí, por sus oraciones y consejos por todos los sacrificios que hizo para verme llegar a la meta, gracias vieja por nunca tirar la toalla, este logro es suyo, la amo mamá, a mi papá por ser mi mentor en esta bella profesión y siempre apoyarme cuando lo necesite.

A mi amado esposo gracias por apoyarme, por creer en mí aun cuando yo dude, gracias por tu comprensión, por tu amor y paciencia, gracias por darme ánimo y no permitir que me diera por vencida cuando las cosas se pusieron difíciles, gracias por tus oraciones, este logro también es tuyo, te amo.

A mi amado hermano por siempre contar con su apoyo y por estar con migo en las buenas y en las malas, te amo hermano, a mis compañeras de tesis por la amistad que me han brindado todos estos años, ha sido un privilegio trabajar con ustedes, gracias por su paciencia y su cariño.

A nuestro apreciado asesor por todos sus consejos y dedicación, por su tiempo y orientación brindada muchas gracias e infinitas bendiciones, a mi alma mater la Universidad de El Salvador por darme la oportunidad de formarme como profesional.

Consuelo Carolina Hernández de Lima

Dedicatoria

Agradezco a Jesús de Nazaret y a la Virgencita María por sus milagros en mi vida y todas las bendiciones en esta etapa, por todas las personas que han estado apoyándome en este proceso académico principalmente a mi madre Margarita por su amor y apoyo incondicional, a mi padre Ángel por su lucha constante, a mis amados hermanos Ruth, Beatriz, Enmanuel, y a mis abuelos que están en una mejor vida y los que aún están conmigo por sus consejos y ejemplo.

A todas aquellas personas que de una u otra manera me inspiran catedráticos, maestros, a todos mis amigos y amigas que alivian mi vida a mis compañeras y amigas de tesis gracias por su paciencia, cariño a nuestro asesor Lic. Bicmar Cubias por guiarnos para poder culminar esta carrera, a la Universidad de El Salvador por formarme para ser una profesional integral.

Diana Margarita Pérez Arabia

Dedicatoria

Le dedico este logro primeramente a Dios, por ser el dador de la vida, el proveedor de sabiduría y salud para poder culminar mi carrera satisfactoriamente, por darme paciencia, fortaleza y su protección en el transcurso de este largo camino, gracias por poner a buenos amigos compañeros y a cada docente y profesor en el recorrido de todo mi estudio.

A mi padre Luis Serrano, por ser siempre el pilar de la casa, un hombre trabajador, responsable, mi ejemplo a seguir, por brindarme lo necesario para mis estudios, por sus consejos, sus oraciones diarias, su apoyo incondicional y sobre todo gracias papi por arriesgar y creer siempre en mí.

A mi querida madre Reina de Serrano, por aconsejarme, cuidarme desde pequeña, regañarme, guiarme por el camino del bien y por ser siempre mi soporte. A mi hermano Alfredo Serrano por sus consejos, regaños, ánimos y apoyo durante toda mi carrera. A mis amadas abuelitas Juanita Serrano y Emma García Orellana y a toda mi familia y amigos/as que creyeron en mí.

Agradezco a mis compañeras de tesis Diana y Consuelo por soportarme hasta la etapa final de este proceso y por la bella amistad que hemos construido y conservado. Asimismo agradezco a nuestro asesor Lic. Bicmar Cubias por la paciencia, por el tiempo brindado al momento de realizar nuestro trabajo de grado. Gracias a la Universidad de El Salvador por darme la oportunidad de iniciar y por fin culminar mi carrera con mucho esfuerzo.

Josué 1:9

Flor de María Serrano Orellana

ÍNDICE DE CONTENIDO

RESUMEN.....	i
LISTA DE SIGLAS Y ABREVIATURAS.....	ii
INTRODUCCIÓN	v
CAPITULO I	
EVOLUCIÓN HISTÓRICA DE LA INFORMÁTICA, LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN, Y DE LOS DELITOS INFORMÁTICOS Y CONEXOS.....	1
1.1 Antecedentes históricos de la informática a nivel mundial	2
1.2 Generaciones de las computadoras	3
1.2.1 Primera generación, 1951 a 1958 bulbos al vacío	3
1.2.2 Segunda generación, 1959-1964 el invento de transistores.....	4
1.2.3 Tercera generación, 1964-1971 evolución del circuito integrado.....	5
1.2.4 Cuarta generación, 1971 a 1981 invento del microprocesador y el chips de memoria.....	5
1.2.5 Quinta generación, 1982 a la actualidad, desarrollo del <i>software</i>	7
1.3 Surgimiento de las tecnologías de la información y la comunicación.....	8
1.4 Antecedentes históricos del internet a nivel mundial	10
1.4.1 Surgimiento del internet	11
1.4.2 Surgimiento de las redes sociales.....	12
1.5 Antecedente del internet en el Salvador	13
1.6 Antecedentes históricos de los delitos informáticos.....	15
1.6.1 Orígenes del término delito informático.....	18
1.6.2 Antecedente de los delitos informáticos en el Salvador	19
CAPITULO II	
GENERALIDADES DE LOS DELITOS INFORMÁTICOS Y CONEXOS, EN RELACIÓN A LA REVELACIÓN INDEBIDA DE DATOS O INFORMACIÓN DE CARÁCTER PERSONAL DE LAS MUJERES	22
2.1 Definiciones del delito Informático	23
2.2 Características del delito informático.....	25
2.3 Clasificación del delito informático.....	26
2.4 Tipos de delitos informáticos	28

2.5 Datos personales o información de carácter personal de las mujeres	29
2.5.1 Clasificación de los datos personales de las mujeres	30
2.5.2 Tipos de datos personales de las mujeres	32
2.5.3 Revelación indebida de datos personales	34
2.6 Catálogo de derechos de las mujeres en El Salvador	36
2.7 Derechos vulnerados en el delito informático de la revelación indebida de datos o información de carácter personal de las mujeres.....	37
2.7.1 Habeas Data o Derecho a la protección de datos personales.....	37
2.7.2 Derecho a la privacidad	39
2.7.3 Derecho a la identidad	40
2.7.4 Derecho a la propia imagen	40
2.7.5 Derecho a la intimidad	41
2.8 Tipos y Modalidades de violencia contra las mujeres	44
2.9 El internet y las redes sociales como instrumento del delito informático de la revelación indebida de datos o información de carácter personal de las mujeres	47
2.9.1 Los riesgos al utilizar y subir información de carácter personal al internet	49
2.9.2 La violencia de género en las redes sociales	50

CAPITULO III

ANÁLISIS Y REGULACIÓN JURÍDICA DEL DELITO INFORMÁTICO DE LA REVELACIÓN INDEBIDA DE DATOS O INFORMACIÓN DE CARÁCTER PERSONAL.....	53
3.1 Normativa Primaria que regula el derecho a la intimidad de las personas	54
3.1.1 Constitución de la Republica de El Salvador	54
3.2 Instrumentos Internacionales que regulan el derecho a la intimidad de las personas	56
3.2.1 Declaración Americana de los Derechos y Deberes del Hombre	56
3.2.2 Declaración Universal de Derechos Humanos	57
3.2.4 Convenio Internacional de Telecomunicaciones	59
3.2.5 Reglas de Brasilia Sobre Acceso a la Justicia de las Personas en Condición de Vulnerabilidad	60
3.3 Normativa secundaria que regula el derecho a la intimidad de las personas y su relación con el tema de investigación	62

3.3.1 Código Penal de El Salvador	62
3.3.2 Ley de Reparación por Daño Moral	67
3.3.3 Ley de Protección al Consumidor	69
3.3.4 Ley Especial Integral Para Una Vida Libre de Violencia Para las Mujeres.....	70
3.3.5 Ley de Acceso a la Información pública	72
3.3.6 Ley Especial Contra los Delitos Informáticos y Conexos.....	72
3.4 Elementos del tipo penal del Artículo 26.....	74
3.4.1 Bien jurídico	74
3.4.2 Elementos objetivos.....	75
3.4.3 Elementos subjetivos	81
3.5 Noticia sobre revelación indebida de datos o información de carácter personal	81
3.6 Proyecto de Ley de Protección de Datos Personales	83
3.7 Análisis de sentencias.....	84
3.7.1 Análisis de sentencia nacional sobre el delito de revelación indebida de datos o información de carácter personal, regulado en el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos	84
3.7.2 Análisis de sentencia internacional con numero de referencia CFP 12474 – 2017 – 44 – CA5, Buenos Aires, Argentina.....	89
3.8 Alcances y Limitantes del artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos.....	91
3.8.1 Alcances	91
3.8.2 Limitantes	93
CONCLUSIONES.....	96
FUENTES DE INFORMACIÓN.....	98

RESUMEN

La evolución de las computadoras responde a dos aspectos muy importantes, un aspecto histórico y un aspecto social, las tecnologías de la información y la comunicación, se desarrollan a partir de los avances científicos producidos en los ámbitos de la informática y las telecomunicaciones y el internet es indispensable para el desarrollo de una sociedad, debido a que el internet es simplemente la interconexión de redes informáticas que permite a los ordenadores o computadoras conectadas comunicarse directamente, aunque se utiliza en múltiples tareas, surge también la preocupación del uso que determinadas personas o instituciones puedan hacer de los datos personales privados y datos sensibles que estén almacenados en distintas bases de datos informáticos y cuyo control se escapa.

Se analiza jurídicamente el delito informático cuando se hace uso de las tecnologías de la información y la comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la manipulación y revelación indebida de datos o información de carácter personal, con énfasis en las mujeres como víctimas del delito, previsto y sancionado en el artículo 26 de la Ley Especial Contra Los Delitos Informáticos y Conexos.

Dicha Ley protege los bienes jurídicos de conductas ilícitas cometidas por medio de las tecnologías informáticas y tecnologías de la comunicación, así como prevenir y sancionar los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su estructura o cualquiera de sus componentes, o los delitos cometidos mediante la utilización de dichas tecnologías que afecten intereses relacionados con la identidad, propiedad, intimidad e imagen.

LISTA DE SIGLAS Y ABREVIATURAS

SIGLAS

ADN: Ácido Desoxirribonucleico

AFIP: Administración Federal de Ingresos Públicos

AIAMP: Asociación Iberoamericana de Ministerios Públicos

AIDEF: Asociación Interamericana de defensorías públicas

ANTEL: Asociación Nacional de Telecomunicaciones

ARPA: Agencia de Investigaciones de Proyectos Avanzados (Advanced Researchs Projects Agency)

ARPANET: Red de la Agencia de Proyectos de Investigación Avanzados (Advanced Research Projects Agency NETWORK)

BASIC: Código de instrucciones simbólicas para todo uso para principiantes (Beginner's All purpose Symbolic Instruction Code)

CEDAW: Convención sobre la Eliminación de toda forma de Discriminación contra la Mujer

CONACYT: Consejo Nacional de Ciencia y Tecnología

DARPA: Agencia de Investigaciones de Proyectos Avanzados de Defensa

(Defense Advanced Researchs Projects Agency)

FIO: Federación Iberoamericana de Ombudsman

FUSADES: Fundación Salvadoreña para el Desarrollo Económico y Social

IAIP: Instituto de Acceso a la Información Pública

IANA: Autoridad de Número Asignados de Internet (Internet Assigned Numbers Authority)

IBM: Máquina de negocios internacionales (International Business Machines)

InterNIC: Centro de Información de la Red Internet (Internet Network Information Center)

IP: Protocolo de internet

KGB: Comité de la Seguridad del Estado (Komitet Gosudarstvennoaja Bezopasnosty)

LAN: Redes de área local (Local area Networks)

NSF: Fundación Nacional de Ciencia (National Science Foundation)

NSFNET: Red de la Fundación Nacional para la Ciencia (National Science Foundation Network)

OCDE: Organización de Cooperación y Desarrollo Económico.

PC-CY: Comité Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras

SVNet: Autoridad internet en El Salvador

TCP: Protocolo de control de transmisión

UCA: Universidad Centroamericana

UES: Universidad de El Salvador

UIBA: Unión Iberoamericana de Colegios y Agrupaciones de Abogados

WAN: Redes de área amplia (Wide Area Networks)

WWW: (World Wide Web)

ABREVIATURAS

A.C. Antes de Cristo

Ed. Editorial/editor

Trad. Traductor/traducido

n. número

INTRODUCCIÓN

En el presente trabajo de investigación se evidencia que las tecnologías de la información y la comunicación, día a día están cambiando a una velocidad increíble y cada vez se acerca y se accede a nuevas tecnologías, es por eso que es importante saber cómo utilizarla y proteger los datos que se almacenan en los dispositivos informáticos, así como nuestra información de carácter privado y personal, ya que la mayoría de personas actualmente tiene acceso a la tecnología y esta puede ser beneficiosa para el desarrollo económico, cultural y social de la población de un país, pero también puede ser utilizada para dañar o atacar aquellos valores más importantes en los usuarios de estas tecnologías y así cometer delitos a través de ellas.

En la actualidad los sistemas informáticos en El Salvador forman parte de la vida cotidiana de los individuos utilizándolos para diversos fines, sean estos sociales, comerciales, laborales, culturales y políticos, sin embargo la facilidad de acceso a estos sistemas informáticos trae aparejado el difícil control para el sistema judicial, esto ha dado paso a nuevas formas de vulnerar garantías constitucionales y derechos de las mujeres por medio de los llamados delitos informáticos.

Lo anteriormente expuesto conlleva a la necesidad de realizar un análisis histórico, doctrinario y jurídico de los delitos informáticos y sobre la nueva Ley Especial Contra los Delitos Informáticos y Conexos, en relación a la revelación indebida de datos o información de carácter personal, esto enfocado a las mujeres de El Salvador, para el conocimiento general de las personas usuarias, estudiantes e instituciones que utilizan los medios tecnológicos y así se logre proteger los datos personales que pueden ser vulnerados a través de las nuevas tecnologías.

La escasa investigación de los elementos y características que comprenden este tipo de delitos, dificulta su estudio, al mismo tiempo la identificación de las conductas delictivas reguladas en dicha Ley, siendo objeto de protección los bienes jurídicos de aquellas conductas cometidas por medio de las tecnologías de la información y la comunicación enfocados a garantizar y proteger el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública orientados a la protección de los derechos constitucionales, la integridad, privacidad, dignidad, a la discriminación y hacia la violencia en contra de las mujeres de El Salvador, la siguiente investigación se abordara en tres capítulos los cuales quedan resumidos de la siguiente forma:

En el capítulo uno se detalla la evolución histórica de la informática, el origen y la evolución de las computadoras, en un sentido general, así como el surgimiento de las tecnologías de la información y comunicación, el apareamiento del internet y las redes sociales, el origen y la evolución de los de los delitos informáticos a través del tiempo, tanto a nivel mundial como a nivel nacional.

Posteriormente en el capítulo dos, se concibe desde un aspecto doctrinario las generalidades de los delitos informáticos, así como sus variadas y diferentes definiciones de cada uno de los autores, sus características, clasificación y tipos, la revelación indebida de los datos personales, su clasificación y tipos de datos privados y además los derechos vulnerados de las mujeres en este tipo de delitos, así mismo se aborda de manera breve, como el internet y las redes sociales son instrumentos para el cometimiento del delito informático de la revelación indebida de datos personales, los riesgos al subir información de carácter personal al internet y la violencia de género en las redes sociales.

En el análisis y regulación jurídica que se realiza en el capítulo tres se relacionan normas jurídicas jerárquicamente y su aplicabilidad y relación de estas con el tema de investigación, es decir, de la Constitución de la Republica, Instrumentos Internacionales que regulan el derecho a la intimidad de las personas, leyes secundarias y jurisprudencia, así como el análisis de los delitos informáticos cometidos en relación con el contenido de los datos, la revelación indebida de los datos personales, de la Ley Especial Contra los Delitos Informáticos y la protección del derecho a la intimidad, honor, imagen, protección de datos personales y datos sensibles y los distintos derechos protegidos de las mujeres en El Salvador mediante las distintas leyes relacionadas.

Finalmente se establecen los alcances y limitantes del artículo 26 y de la misma Ley Especial Contra los Delitos Informáticos, obtenidos de la investigación, debido a que la ley es nueva y pocas personas tienen el conocimiento de ella, además de la mayor influencia de usuarios a nivel mundial y nacional de los sistemas informáticos, redes sociales y tecnologías de la información, que conlleva a la inseguridad sobre protección de los derechos de las mujeres y los datos almacenados en soportes informáticos.

CAPITULO I

EVOLUCIÓN HISTÓRICA DE LA INFORMÁTICA, LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN, Y DE LOS DELITOS INFORMÁTICOS Y CONEXOS

El propósito del presente capítulo es desarrollar una línea histórica sobre el origen y la evolución de los delitos informáticos a través del tiempo, tanto a nivel mundial como a nivel nacional, así como una breve reseña del surgimiento y evolución del internet, y el surgimiento de las nuevas tecnologías que se están desarrollando e introduciendo en el mundo de hoy. La evolución de las computadoras se puede decir que responde a dos aspectos un aspecto histórico y un aspecto social, con el pasar de los años fue haciéndose más evidente la necesidad de crear maquinas que hicieran menos complicado el trabajo del hombre.

En la actualidad el uso de las computadoras y del internet es indispensable para el desarrollo de una sociedad y aunque se utiliza día a día en múltiples tareas poco es el conocimiento que tienen las personas sobre el surgimiento de los mismos, y dado que el tema de estudio que se aborda en el presente trabajo se relaciona con el uso de las computadoras y del internet es necesario realizar una línea histórica sobre el surgimiento de la misma.

Las computadoras en su mayoría eran sistemas grandes que fueron evolucionando en el transcurso de los años y con costos económicos elevados esto hacía que los únicos que podían tener acceso a una de estas eran las corporaciones grandes, universidades y agencias del gobierno para el almacenamiento de datos así se da paso una a periodos importantes del desarrollo de las computadoras y de los sistemas informáticos.

Desde los orígenes de las computadoras estas han pasado por varias fases o etapas siendo cada una más desarrollada que la anterior, la mayoría de autores clasifican estas etapas o fases en generaciones es así que en el presente capítulo se habla de computadoras de primera generación, de segunda generación y así hasta llegar a la quinta generación.

La evolución de las computadoras conlleva también mayor inversión económica por parte de los países, puesto que significa un mayor avance tecnológico para las sociedades y en consecuencia mayor desarrollo social, económico y tecnológico, la evolución de las computadoras no solo ha significado un enorme avance técnico para la humanidad y una herramienta indispensable para el trabajo del hombre sino también un instrumento que ha dinamizado la economía a nivel mundial.

1.1 Antecedentes históricos de la informática a nivel mundial

De acuerdo con la historia y la antigüedad, el hombre ha tratado de reducir al máximo su trabajo y dinamizar la producción, para ello es que se han inventado las herramientas y las máquinas, con la ayuda de estos dispositivos el hombre disminuye la necesidad de esfuerzo físico con el desarrollo de estos, esto si bien ha ayudado a que el trabajo sea más rápido también ha reducido el empleo para el ser humano, el ingenio humano se dedicó a sustituir también la inteligencia aplicada a tareas rutinarias, la automática es precisamente la ciencia que trata de la sustitución del operador humano por un operador artificial en la ejecución de una tarea de esta forma se necesita menos personal obteniendo mismos resultados¹.

¹ Athina Vanessa García Mejía, Víctor Andrés González Guzmán, "El intrusismo informático y la utilización del Derecho Penal como mecanismo de tutela del derecho a la intimidad" (Tesis de Licenciatura: Universidad de El Salvador, 2017), 14.

La informática puede considerarse como la ciencia y la tecnología aplicada a la automatización del razonamiento y del tratamiento de la información, se establece que las raíces de la informática se encuentran en primer lugar en el desarrollo de métodos, herramientas y maquinas, para facilitar la realización de cálculos de forma eficiente y precisa y en segundo lugar la sistematización del razonamiento, como paso previo a su automatización y a la búsqueda de modelos formales de cálculo², por otra parte, se caracteriza a la informática como un producto de la cibernética, asimismo como un proceso científico relacionado con el tratamiento automatizado de la información en un plano interdisciplinario³.

Al establecer los inicios de la informática en el transcurso de la historia, es preciso y oportuno hablar sobre el principio de las computadoras y su desarrollo en las tecnologías ya que sin estas no podría existir la primera, existen numerosas opiniones sobre si el surgimiento de las computadoras realmente favorece a las sociedades o si por el contrario afecta el desarrollo de las mismas, la realidad es que la sociedad actual tiene una relación de dependencia con las computadoras en lo laboral, social, educativo y demás⁴.

1.2 Generaciones de las computadoras

1.2.1 Primera generación, 1951 a 1958 bulbos al vacío

Con esta primera generación inicia la vida de las computadoras en el mundo,

² Alberto Prieto Espinoza, *Introducción a la informática*, 3° ed. (Madrid: McGraw-Hill Interamericana de España, 2002), 56.

³ Leo Bladimir Benavides Salamanca, Marlon Ibán Hernández Anzora, Kenia Katy León Ardón, "La Penalización De Los Delitos Informáticos En El Salvador" (Tesis para optar al Título de: Licenciado en Ciencias Jurídicas, Universidad de El Salvador, 2004), 2.

⁴ Guillermo Levine, *Computación y programación moderna*, (México: Pearson Educación, 2001), 34.

en la historia de las computadoras en la primera generación se emplearon bulbos para ejecutar la información, los operadores integraban los datos y programas en código especial por medio de tarjetas perforadas; el almacenamiento interno se lograba con un tambor que giraba instantáneamente, sobre el cual un aparato de lectura y escritura instalaba marcas magnéticas, esas computadoras eran mucho más grandes y generaban más calor que los modelos modernos.

Las computadoras de la primera generación fueron, como su nombre lo dice las primeras computadoras que existieron, mucho más complejas que las computadoras actuales y mucho más grandes.

1.2.2 Segunda generación, 1959-1964 el invento de transistores

En este periodo el invento del transistor⁵ hizo viable una nueva generación de computadoras, más veloces, más livianas y con menores necesidades de ventilación, sin embargo el precio seguía siendo una parte significativa del presupuesto de una compañía, las computadoras de la segunda generación utilizaban redes de núcleos magnéticos en lugar de tambores giratorios, para el almacenamiento primario, estos núcleos contenían pequeños anillos de material magnético, conectados entre sí, en los cuales podían almacenarse datos e instrucciones.

Las computadoras de la segunda generación, tuvieron un avance significativo en relación a las computadoras de la primera generación, no era suficiente, aunque claro está que son las mejoras que tuvo, hizo su manejo

⁵ El transistor es un componente electrónico construido por materiales semiconductores que prácticamente revoluciono todos los aparatos electrónicos sin excepción alguna, Frank Mecafenix. *¿Qué es un transistor y cómo funciona?* (8 de agosto, 2019), <https://www.ingmecafenix.com/electronica/el-transistor/>

mucho menos complejo y lo más importante minimizo un poco los costos para poder acceder a una computadora⁶.

1.2.3 Tercera generación, 1964-1971 evolución del circuito integrado

La evolución de los circuitos integrados⁷ trajo el desarrollo de la tercera generación de las computadoras, en las cuales se instalaban un sin número de componentes electrónicos, en una integración en miniatura, lo que las hacía de menor tamaño, más veloces, generaban menos calor y eran energicamente más eficientes⁸, los circuitos integrados permitieron a los fabricantes de computadoras incrementar la flexibilidad de los programas, y estandarizar sus modelos.

1.2.4 Cuarta generación, 1971 a 1981 invento del microprocesador y el chips de memoria

La invención de los microprocesadores o simplemente procesador al circuito integrado de un sistema informático, para la ejecución de programas, es un gran progreso de la microelectrónica, los cuales consisten en circuitos integrados de alta densidad y con una rapidez impresionante, las microcomputadoras con base en estos circuitos son considerablemente pequeñas y baratas, por lo que su uso se extiende al mercado industrial, surgen las computadoras personales que han conseguido proporciones

⁶ Athina Vanessa García Mejía, Víctor Andrés González Guzmán, "El intrusismo informático y la utilización del Derecho Penal como mecanismo de tutela del derecho a la intimidad" (Tesis de Licenciatura: Universidad de El Salvador, 2017),44

⁷ El circuito integrado es un pequeño cristal de silicio semiconductor, llamado microcircuito, que contiene los componentes electrónicos para las compuertas digitales. Las diversas compuertas se conectan dentro del microcircuito para formar los circuitos requeridos. M. Morris Mano, *Arquitectura de computadoras*, (Universidad Estatal de California, Los Ángeles, tercera edición).

⁸ *Ibíd.* P.23.

enormes y que han influido en la sociedad en general sobre la llamada evolución de la Informática⁹.

Las diversas críticas al método de cálculo de las macrocomputadoras concluyeron en 1975, cuando una empresa poco conocida de Nuevo México impulso al mercado el Altair, que fue el primer equipo informático, este equipo apenas se podía llamar ordenador y había que añadirle muchos más componentes para conseguir un sistema de uso práctico sin embargo, el anuncio de Altair desencadenó una explosión de energía creativa que para el año de 1977 había producido sistemas capaces de ejecutar tareas útiles y que empleaban chips de silicio avanzados tanto para el procesador como para la memoria.

La versión de BASIC¹⁰, es un tipo de lenguaje de programación, la versión se debe a un pequeño equipo dirigido por Bill Gates, quien había dejado sus estudios en Harvard y se había trasladado a Nuevo México con el fin de desarrollar *software* para Altair, con ello se logró arrebatarse a la Máquina de Negocios Internacionales (IBM) la dirección sobre el sector informático, sin embargo, a ninguno de los gigantes que se enfrentaron a IBM les fue particularmente bien es una reconocida empresa multinacional estadounidense de tecnología y consultoría, durante la siguiente década¹¹.

⁹Comienza con la explosión de los chips y el hardware, cuyo crecimiento condujo al florecimiento del software y los equipamientos de telecomunicaciones, seguidos por la explosión del internet y así sucesivamente. Carlota Pérez, *Revoluciones tecnológicas y capital financiero*, (México: Polaris, 2003), 43.

¹⁰ BASIC significa código de instrucciones simbólicas para el uso de principiantes, y sus siglas en inglés *Beginner's All purpose Symbolic Instruction Code*, fue inventado en el Dartmouth College en el año de 1964, fue el primer producto comercializado por Microsoft Corporation. Faith Davies. https://www.techlandia.com/definicion-del-lenguaje-computacion-basic-hechos_47795/.

¹¹ Ceruzzi, P. E. *Breve Historia de la Computación*, (Madrid: FCE, openmind BBVA, 2018), <https://www.bbvaopenmind.com/articulos/historia-de-la-informatica/>.

1.2.5 Quinta generación, 1982 a la actualidad, desarrollo del *software*

En el desarrollo avanzado de la microelectrónica se perfeccionó el *software* y los sistemas con que se manipulan las computadoras, dejando el progreso que se tenía hasta la cuarta generación en relación al *hardware*¹², hoy se habla ya de computadoras cuánticas, inteligencia artificial, robótica, sistemas expertos, redes de comunicación, entre otros.

La quinta generación de computadoras, es la que existe en la actualidad, se puede observar que ha tenido un gran avance en cuanto la tecnología de las computadora desde la primera generación¹³.

Con el avance de las computadoras y la aplicación de estas a las telecomunicaciones, fue indispensable la creación de un dispositivo que facilitara el tráfico de información, para lograr que la distancia no creara inconveniente a efecto de transferir grandes cantidades de información, siendo así que en un primer momento se creó una red para fines militares denominada Agencia de Investigaciones de Proyectos Avanzados (ARPA)¹⁴.

La Agencia de Investigaciones de Proyectos Avanzados (ARPA) fue creada como respuesta de la necesidad de esta organización de buscar mejores

¹² Conjunto de componentes que tienen una naturaleza física y por tanto material para atender a las actividades de recogida, procesamiento y comunicación del sistema, es uno de los elementos más importantes del sistema y sobre el que se apoya gran parte del sistema de información. Carmen de Pablos, *Informática y comunicaciones en la empresa*, (Madrid: ESIC, 2004), 48.

¹³ La existencia de *software*; fue en esta quinta generación en que las computadoras tuvieron aplicación en las telecomunicaciones y fue así que se pudo compartir información sin importar la distancia que separe a las personas y es hasta en este momento en que surge el problema que es objeto de esta investigación, la revelación indebida de información y debido a esto empezaron a surgir mecanismos para proteger la información de las personas.

¹⁴ También conocida por Agencia de Proyectos Avanzados de Investigación para la Defensa (DARPA, por sus siglas en inglés), creada en 1957, en el Departamento de Defensa de EE. UU, para invertir en investigaciones de alto riesgo.

maneras de usar los computadores de ese momento, pero enfrentados a la dificultad que los principales investigadores y laboratorios, ansiaban tener sus propios computadores, lo que no solo era más oneroso, sino que provocaba una duplicación de esfuerzos y recursos, idea que produjo el avance denominado internet¹⁵.

1.3 Surgimiento de las tecnologías de la información y la comunicación

Las tecnologías de la información y la comunicación (TIC), son aquellos recursos, herramientas, programas para procesar y administrar información se desarrollan a partir de los avances científicos producidos en los ámbitos de la informática y las telecomunicaciones¹⁶, las TIC son el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos¹⁷.

La revolución electrónica iniciada en la década de los 70 constituye el punto de partida para el desarrollo creciente de la era digital, los avances científicos en el campo de la electrónica tuvieron dos consecuencias inmediatas: la caída instantánea de los precios de las materias primas y la preponderancia de las tecnologías de la información que combinaban esencialmente la electrónica y el *software*, pero las investigaciones desarrolladas a principios de los años 80 han permitido la tendencia de la electrónica, la informática y las telecomunicaciones posibilitando la interconexión entre redes, es de esta

¹⁵ Ibíd. P. 11.

¹⁶ Definición general de las Tics, es la combinación entre edición y modificación de la información a través de las diferentes herramientas de informática y la divulgación de la información a través de los diferentes medios de comunicación existentes. Isaac Julio. *Herramientas Informáticas y su diferencia con las TICS* (Septiembre 18, 2015), <https://grupo4herramientasinformatica.blogspot.com/2015/09/herramientas-informaticas-y-su.html>

¹⁷ Consuelo Belloch Orti. *Las tecnologías de la información y comunicación* (Universidad de Valencia, consultado 13 de octubre de 2019), <https://www.uv.es/~bellohc/pdf/pwtic1.pdf>.

forma, que las TIC se han convertido en un sector estratégico para la nueva economía¹⁸.

La informática se acuñó en Francia, en el año de 1962, como acrónimo de *informatique*, de esta manera se formó la conjunción de las palabras *information* y *automatique*, para dar idea de la automatización de la información que se consigue con los sistemas computacionales, la teoría de la información ha venido avanzando gracias al desarrollo de las técnicas de codificación binaria y la invención de una algebra lógica, del matemático y filósofo británico George Boole, se establece que el inventor del código binario fue el filósofo inglés Francis Bacon, quien discutió un sistema según el cual las letras del alfabeto podrían reducirse a secuencias de dígitos binario¹⁹.

Las telecomunicaciones surgen a raíz de la invención del telégrafo en el año 1833 y el posterior extensión de redes telegráficas por la geografía nacional, que en España se desarrolla entre los años 1850 y 1900 actualmente estamos acostumbrados a coexistir con todo tipo de servicios que nos facilitan la comunicación entre personas, son el intercambio de información a distancias considerables por medios electrónicos y se refiere a todos los tipos de transmisión de voz, datos y video, pero la experiencia con estos sistemas es relativamente reciente, igualmente a lo largo de la historia las señales han ido evolucionando en cuanto a su variedad y complejidad, para ajustarse en satisfacer las necesidades de comunicación del hombre en la sociedad²⁰.

¹⁸ Francy Milena Bonilla. *Origen, historia y evolución de las TIC* (15 oct, 2019), <https://sites.google.com/site/ticsyopal5/assignments>.

¹⁹ William Darío Ávila Díaz, "Hacia una reflexión histórica de las TIC", *Hallazgos*, Vol. 10 núm. 19 (Bogotá Colombia, 2013): 218, 222.

²⁰ Francy Milena Bonilla. *Origen, historia y evolución de las TIC* (15 oct, 2019), <https://www.sites.google.com/site/ticsyopal5/assignments>.

Esta evolución a la que se refiere el párrafo anterior sobre las comunicaciones entre personas se ha beneficiado en gran medida de los avances tecnológicos experimentados en todas las épocas, que han ido suprimiendo las barreras que tradicionalmente han limitado la interactividad entre las personas, asimismo el uso de nuevos tipos de señales y el desarrollo de nuevos medios de transmisión adaptados a las crecientes necesidades de comunicación han sido fenómenos paralelos al desarrollo de la historia²¹.

1.4 Antecedentes históricos del internet a nivel mundial

El antecedente de la creación del Internet, para comunicarse digitalmente era por medio del telégrafo este se inventó en el año de 1840, emitía señales eléctricas que viajaban por cables conectados entre un origen y un destino, se utilizaba el código Morse para interpretar la información consecuentemente para interconectar las minicomputadoras²² y permitir una transferencia rápida de la información entre ellas, muchas empresas comenzaron a instalar Redes de Área Local (LAN, por sus siglas en inglés de *local area Networks*)²³.

El Internet surgió en el año de 1962, introduciendo una serie de notas escritas por Joseph Carl Robnett Licklider, también conocido como J.C.R. Licklider, quien consecutivamente se convirtió en el jefe del programa de

²¹ El término comunicación proviene de la palabra latina *communicare*, que significa transmitir o compartir algo, poner en común a dos o más personas conectadas entre sí, mediante relaciones e influencias de símbolos y sistemas de mensajes.

²² Las minicomputadoras son computadoras multi-usuario, pero con menos capacidad que las computadoras mainframe. Estos tipos de computadoras aparecieron en los años de 1960 cuando los circuitos integrados de grande escala hicieron posible la fabricación de una computadora mucho más barata que las computadoras mainframe existentes, debido a que la tecnología LAN es barata y fácil de instalar.

²³ Douglas E. Comer, *El Libro del internet*, trad. Hugo Alberto Acuña Soto y Roberto L. Escalona, 2ª Ed. (México: Prentice Hall, 1998), 50.

investigación de computación de la Agencia de Investigación Avanzada de Proyectos del Departamento de Defensa de los Estados Unidos (DARPA) institución que dio desarrollo al Internet y cuyo intención principal era la investigación y desarrollo de protocolos de comunicación²⁴.

1.4.1 Surgimiento del internet

El Internet se originó hace ya varias décadas, debido al esfuerzo de interconectar la Red de la Agencia de Proyectos de Investigación Avanzada o como se conoce ARPANET del Departamento de Defensa Estadounidense con varias redes vinculadas por medio de satélite y de radio en el modelo ARPANET la comunicación ocurre entre una computadora fuente y un destino por lo tanto debe afirmar que la comunicación entre ellas se lleve a cabo. Otras redes como conmutadores de paquetes llamados mensajes de interfaz que utilizaban paquetes de radio y satélites se conectaron a ARPANET utilizando la tecnología interconectada por DARPA²⁵.

La definición de Internet es simplemente la interconexión de redes informáticas que permite a los ordenadores o computadoras conectadas comunicarse directamente, es decir cada ordenador de la red puede conectarse a cualquier otro ordenador de la red, el *software* de las computadoras forma parte importante de la tecnología que hace posible la interconexión de redes²⁶, el Protocolo de Control de Transmisión (TCP) se refiere a un importante protocolo de Internet que es responsable de la

²⁴ Aníbal Alejandro Pardini, *Derecho de Internet*, (Buenos Aires, Argentina: La Rocca, 2002), 43.

²⁵ Athina Vanessa García Mejía, Víctor Andrés González Guzmán, "El intrusismo informático y la utilización del Derecho Penal como mecanismo de tutela del derecho a la intimidad". (Tesis de Licenciatura: Universidad de El Salvador, 2017), 19.

²⁶ Douglas E. Comer, *El Libro del internet*, trad. por Hugo Alberto Acuña Soto y Roberto L. Escalona, 2ª Ed. (México: Prentice Hall, 1998), 55. Sin Software, los ordenadores serían inútiles, y es desarrollado mediante el uso de distintos lenguajes de programación.

transmisión o transferencia de paquetes de datos a través de redes y a través del Internet²⁷.

La Fundación Nacional de Ciencia (*National Science Foundation* en inglés o NSF), entidad gubernamental de los Estados Unidos para el desarrollo de la ciencia se hizo cargo de la red, conectando las redes que luego darían lugar a la red de redes que hoy llamamos Internet, en el año de 1990 el Internet comenzó a llegar a la población en general, fue en ese año que el ingeniero inglés Tim Bernes Lee desarrolla la *World Wide Web* (WWW)²⁸ permitiendo el uso de una interfaz gráfica y la creación de sitios más dinámicos y visualmente interesantes.

1.4.2 Surgimiento de las redes sociales

Las redes sociales en el contexto digital se refiere a las plataformas que permiten la interacciones entre personas o empresas, la primera red social surgió en el año de 1997 llamada sixdegrees la cual fue el primer servicio que permitía crear un perfil en la web además agrupaba los contactos directos e intercambiaban mensajes con ellos, posteriormente en el años de 1999 se creó liveJournal.com es cual fue uno de los primeros servicios de redes sociales que ofrecían blogs y diarios en línea en el transcurso de los años se encuentra en 2003 My Space y MSN y Hi5 lograron tener desde 250 millones hasta 100 millones de usuarios con la intención de promover el intercambio de información diversa y compartiendo datos personales²⁹.

²⁷ SPEEDCHECK. *Protocolo de Control de Transmisión y Protocolo de Internet* (TCP/IP), 03 de septiembre 2019 <https://www.speedcheck.org/es/wiki/tcp-ip/>.

²⁸ Es una enorme porción de Internet que incluye gran riqueza de contenido multimedia accesible a través de sencillos programas, consistentes en señalar y hacer clic, llamados navegadores web. George Beekman, *Introducción a la Informática*, 6° ed. (Madrid: Pearson Educación, 2004), 15.

²⁹ Bubot. *Historia de las redes sociales desde 1997 hasta hoy* (16 de julio de 2014), <https://www.bubot.es/historia-de-las-redes-sociales-desde-1997-hasta-hoy/>.

En el mundo globalizado en el que actualmente se vive, el Internet ya forma parte de la vida y las redes sociales es el medio de comunicación e interacción más común entre los individuos en todo el mundo, sin embargo, se debe saber qué tipos de redes sociales existen y para qué sirven, porque no todas las redes sociales tienen los mismos objetivos ni tampoco están dirigidos al mismo público es por eso que cada una cumple una función específica³⁰.

En la actualidad, en pleno siglo XXI el internet tiene una red masiva desarrollada por todo el mundo, en relación a la aparición de las redes sociales³¹ como medio para el cometimiento de delitos informáticos por lo que es muy importante desarrollar su origen debido a que por medio de ellas en la actualidad se comenten la mayoría de delitos informáticos.

1.5 Antecedente del internet en el Salvador

El Salvador emprendió incorporarse al grupo de los países conectados con obstáculos e inconvenientes hasta que en el año de 1994 del mes de septiembre se negoció, ante el IANA (*Internet Assigned Numbers Authority*, en español significa Autoridad Número Asignados de Internet) y el InterNIC (*Internet Network Information Center*, que significa Centro de Información de la Red Internet), correspondientemente un conjunto de direcciones de protocolo de internet (IP) equivalentes a una clase B y la administración del dominio de nivel superior correspondiente al país, El Salvador obtuvo el

³⁰ Alba Caride. *Tipos de redes sociales* (17 de octubre de 2017), [https:// www.hoyreka.com/tipos-redes-sociales/](https://www.hoyreka.com/tipos-redes-sociales/).

³¹ Las redes sociales como Instagram, YouTube, Facebook WhatsApp, Twitter, los usuarios las utilizan para diferentes fines, a través de estas se puede compartir fotos, videos, aficiones, conocer gente, los sitios ofrecen características como actualización automática de la libreta de direcciones, perfiles visibles, la capacidad de crear nuevos enlaces mediante servicios de presentación y otras maneras de conexión social en línea.

dominio “sv” que permitía diferenciar a los sitios web salvadoreños de los demás³².

El Protocolo Internet proporciona un servicio de distribución de paquetes de información orientado a no conexión de manera no fiable. La orientación a no conexión significa que los paquetes de información, que será emitido a la red, son tratados independientemente, pudiendo viajar por diferentes trayectorias para llegar a su destino. Según los códigos de países a El Salvador se le atribuyen el “sv” La ISO 3166 es un estándar internacional para los códigos de país y los códigos para sus subdivisiones. Ha sido publicada por la Organización Internacional de Normalización

En Costa Rica en el año de 1993 fue el primer país centroamericano en conectarse a Internet ante ello, unos meses más tarde El Salvador también daría un paso adelante para seguir dicho ejemplo, en El Salvador existía una empresa estatal que era encargada de la telefonía, llamada ANTEL (Asociación Nacional de Telecomunicaciones)³³.

En el año de 1994 la primera conexión a internet en El Salvador se instaló en el Consejo Nacional de Ciencia y Tecnología (CONACYT), y el ingeniero Rafael Ibarra fue quien hizo la instalación con el apoyo de colegas de Guatemala y Costa Rica, ese mismo mes y año el grupo SVNet fue constituido por la Universidad Centroamericana UCA, CONACYT, UES, la Universidad Don Bosco, FUSADES³⁴ y ANTEL con el fin de administrar

³² Brendan P. Kehoe, Miguel A. Martínez Sarmiento, *Internet del Arte al Zen*, (México: Prentice Hall, 1995), 159..

³³ El Blog de Misael Alemán, *Historia del internet en El Salvador*, 20 de julio de 2017). <https://www.misaelaleman.com/historia-del-internet-en-el-salvador>.

³⁴ FUSADES, *¿Quiénes somos?*, 03 de septiembre 2019, <http://www.fusades.org/fusades/conócenos/acerca-de-fusades-2>. Fundación Salvadoreña para el Desarrollo Económico y Social, FUSADES, es una organización privada de desarrollo, sin fines de lucro.

ambos recursos, formaron la Asociación SVNET el cual es el administrador de nombres de dominio de IP para El Salvador y pretende promover, desarrollar e impulsar toda clase de proyectos relacionados con el campo de la informática, desarrollo de programas y nuevos productos tecnológicos³⁵.

En febrero de 1996 ANTEL completó la instalación de los primeros enlaces dedicados a Internet en territorio salvadoreño, siendo éstos los de la Universidad Centroamericana José Simeón Cañas y el de la Universidad Don Bosco, el siguiente mes vieron los sitios Web de estas dos universidades, así como los de SVNet y la página principal de El Salvador (www.sv), convirtiéndose así en los primeros sitios Web de El Salvador que residían en un servidor ubicado físicamente en El Salvador³⁶.

1.6 Antecedentes históricos de los delitos informáticos

A lo largo de la historia y la evolución de las tecnologías surgen también nuevos fenómenos ilícitos y con la aparición de la computadora personal, móviles y con la expansión del Internet el surgimiento de la *World Wide Web*, (WWW) la capacidad de procesamiento de datos e información y el acceso a miles de personas en un medio interactivo de características globales, amplió a gran manera las posibilidades de comisión de hechos ilícitos e ilegales y del surgimiento de entornos digitales amigables como sus aplicaciones prácticas, en cuanto a su fácil manejo de la información así como las posibilidades del anonimato en las comunicaciones³⁷.

³⁵ Rafael Antonio Ibarra Hernández. *Internet en El Salvador*, (27 de abril 2002), <https://www.nsrc.org/regions/CENTRAM/SV/Internet-SV-04-2002.PDF>.

³⁶ El Blog de Misael Alemán, *Historia del internet en El Salvador*, 20 de julio de 2017). <https://www.misaelaleman.com/historia-del-internet-en-el-salvador>.

³⁷ Gustavo Sain, Revista Pensamiento Penal. "Evolución histórica de los delitos informáticos", (2015): 1. http://www.pensamiento penal.com.ar/system/files/2015/04/doctrina_40877.pdf.

Durante la década de 1970 se comenzaban a registrar una serie de casos que arrojan pérdidas muy numerosas para los sectores privados, esto fue por el comienzo del desarrollo de delitos económicos tales como el espionaje informático, la piratería de *software*, el sabotaje y la extorsión, dentro de la historia la primera propuesta de legislar el delito informático fue introducida por el Senador Ribicoff en el año de 1977 en el Congreso Federal de Estados Unidos años más tarde en 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) en París, designó un comité de expertos para discutir el crimen relacionado con las computadoras y la necesidad de cambios en los códigos penales³⁸.

Se puede estudiar que a partir de los primeros años de la década de 1980, los delitos informáticos adquieren una importante notoriedad debido al alto aumento de fraudes para el resultado de los fraudes, los casos típicos se realizaban mediante la manipulación de uso de tarjetas de débito en cajeros automáticos, fundamentalmente a través de la vulneración de las bandas magnética y el tratamiento de la problemática por parte de organismos internacionales, fue a fines de esa década que comenzaron a aparecer contenidos ilícitos y nocivos en las redes tales como amenazas contra las personas incitación al odio y el intercambio de material de pornografía infantil, tanto así como actos de violencia y discriminación racista por parte de grupos extremistas³⁹.

En el año de 1989 el Consejo de Europa convocó a otro comité de expertos que en la recomendación número 9 adoptada el 13 de septiembre de 1989 presenta una lista mínima de los delitos sobre los que debía necesariamente

³⁸ *Ibíd.* P.35.

³⁹ Gustavo Sain, Revista Pensamiento Penal. “Evolución histórica de los delitos informáticos”, (2015): 3. <http://www.pensamientopenal.com.ar/system/files/2015/04/doctrina40877.pdf>.

legislarse en cada país miembro, más una lista opcional⁴⁰ las nuevas técnicas de *hacking* manipulaban sistemas de vuelo o sistemas hospitalarios y de salud definidos como ataques contra la vida, estos hechos aumentaron significativamente a la par del incremento de usuarios de las red haciéndose evidente a nivel gubernamental en 1989, cuando la justicia alemana identificó a *hackers*⁴¹ que utilizaban las redes de datos internacionales para el acceso a información privilegiada de Estados Unidos y Gran Bretaña para vender la información a la KGB⁴².

En el año de 1996 el Comité Europeo para los problemas criminales decidió establecer un nuevo comité de expertos para que se abordara el tema de los delitos informáticos dicho Comité Especial de Expertos sobre Delitos relacionados con el empleo de computadoras, inicio su labor en abril de 1997 y efectuó negociaciones con respecto al borrador de un convenio internacional en materia de delitos informáticos.

En los años de 1997 al 2000 el Comité Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras, sus siglas PC-CY, inició su labor en abril de 1997 y efectuó negociaciones con respecto al borrador de un convenio internacional en materia de delitos informáticos Budapest, definido como primer tratado internacional sobre delitos cometidos a través

⁴⁰ 1990 el tema fue discutido en el Décimo Tercer Congreso Internacional de la Académica de Derecho Comparado en Montreal y en el Octavo Congreso Criminal de las Naciones Unidas celebrado en La Habana el mismo año, en 1992 en la Conferencia de Wurzburg Alemania y en 1995 el Consejo de Europa adopta otra recomendación concerniente a los problemas de derecho procesal conectados con la información tecnológica. *Ibíd.* P. 36.

⁴¹ Hacking es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo. Blog LemonHead, web de Duiops, (Consultado 13 de agosto de 2019), <https://www.duiops.net/hacking/hacking-cracking.htm>.

⁴² Las iniciales de KGB (Siglas de *Komitet Gosudarstrennoaja Bezopasnosty*), que significa Comité de la Seguridad del Estado: es una Organización de la antigua Unión Soviética dedicada al espionaje y contraespionaje.

de Internet y otras redes informáticas, que se ocupa especialmente de las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de la red. También contiene una serie de poderes y procedimientos, como la búsqueda de redes informáticas y la interceptación.

1.6.1 Orígenes del término delito informático

Entre los orígenes del termino delito informático empezó con el nombre de delito cibernético y luego con la aparición del correo electrónico a finales de los años ochenta posteriormente con el avance de los navegadores web en los años noventa el delito cibernético se empezó a expandir a principios del 2000 cuando las redes sociales cobraron vidas y las personas subían toda la información que podían en una base de datos del perfil, se creó una inundación de información personal y así mismo el aumento del robo de identidad⁴³.

Se puede establecer que para la comisión de las conductas delictivas denominadas delitos informáticos, es indispensable el uso de la computadora y del manejo del internet, sin embargo en la actualidad no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir no existe un concepto propio⁴⁴.

La expresión delito informático se afianzo a finales de los años 90, a medida que el Internet se esparció por toda Norteamérica, después de una reunión

⁴³ Paola Rinaldi. *Origen y evolución del delito cibernético*, (abril 27 de 2017), <https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/>

⁴⁴ *Ibíd.* P.38. la diversidad de términos que se encuentran son: Delitos Electrónicos, Delito cibernético, Cibercrimenes, Cibercrimitos, entre otros, por lo que no se establece con que termino se empezó a catalogar este delito.

en Lyon, Francia, se fundó un subgrupo del grupo de naciones que conforman el denominado “G8” con el objetivo de estudiar los problemas emergentes de criminalidad que eran propiciados por lo que migraron a la Internet⁴⁵.

1.6.2 Antecedente de los delitos informáticos en el Salvador

A lo largo de la historia se han desarrollado medios masivos de comunicación veloz, económicos, idóneos para enviar y recibir todo tipo de mensajes de texto, correos de voz, fotografías, archivos de sonidos, gráficos e información en grandes volúmenes⁴⁶, en los últimos años el país ha experimentado una mayor cobertura de Internet y con ello los ciudadanos emplean con mayor intensidad las TIC. Aunque existen algunas contradicciones respecto a las estadísticas de cobertura como por ejemplo Internet *World Stats* registra que el país alcanza el 50.4% de cobertura de Internet.

Por su parte el foro económico mundial en su informe global de tecnologías de la información registra que el uso individual de Internet en El Salvador alcanza el 29.7%, lo cierto es que a partir del crecimiento del uso de las TIC se incrementan también los delitos cometidos a través de éstas⁴⁷.

⁴⁵ Gonzo Stelgon. *Historia de Delitos informáticos* (18 de noviembre de 2008), <http://gonzo.stelgon.blogspot.com/2008/11/historia-de-delitos-informaticos.html>.

⁴⁶ Athina Vanessa, García Mejía, Víctor Andrés González Guzmán, “El intrusismo informático y la utilización del derecho penal como mecanismo de tutela del derecho a la intimidad” (tesis para optar al título de Licenciado en Ciencias Jurídicas, Universidad de El Salvador, 2017), 39

⁴⁷ Carlos Molina Medrano. *A un año de la aprobación de la Ley de Delitos Informáticos en El Salvador: retos y desafíos* (Unidad de Informática y Comunicaciones, Universidad Luterana Salvadoreña, 23 de febrero 2017) <https://www.uls.edu.sv/sitioweb/component/k2/item/551-a-un-ano-de-la-aprobacion-de-la-ley-de-delitos-informaticos-en-el-salvador-retos-y-desafios>.

Se puede destacar el aumento del uso del internet y por ello el aumento de los delitos cometidos a través de los medios tecnológicos y por ello que los datos de toda persona deben ser objeto de protección ante las tecnologías, para que estos puedan ser tratados o elaborados y finalmente ser convertidos en información y en consecuencia solo ser utilizados para los fines y por las personas correspondientes.⁴⁸

Las nuevas tecnologías digitales producen relevantes efectos sobre las categorías jurídicas tradicionales relacionadas directamente con la información y la comunicación⁴⁹, es por ello que los delitos informáticos están presentes en la actualidad en nuestro país y se pueden cometer por el simple hecho que se tenga acceso a un medio virtual y electrónico esto conlleva a que la información que se publica en redes sociales, perfiles, correos entre otros, en consecuencia se puede llegar a vulnerar este tipo de acceso a la privacidad de una persona⁵⁰.

Se analiza que cuando se usan los servicios y aplicaciones online es muy habitual que se utilice información personal, tanto propia como de terceros, para que las personas se puedan relacionar, comprar, o planificar distintas actividades.

En la actualidad con mucha facilidad y rapidez se difunde información, fotografías, vídeos o audios, por ejemplo, en las redes sociales o a través de los servicios de mensajería instantánea o del correo electrónico, que afectan a personas a las que no se ha pedido permiso para hacerlo.

⁴⁸ María Estela Raffino, (10 de enero de 2019). <https://concepto.de/base-de-datos/#ixzz5yWNXjvuS>.

⁴⁹ Ignacio Flores Prada, *Criminalidad informativa, aspectos sustantivos y procesales*. (Valencia, España: Tirant lo Blanch, 2012), 23.

⁵⁰ Daniel Calderón <https://es.calameo.com/books/00548365172880153bba7>.

En El Salvador se lleva a cabo la investigación de los delitos informáticos a través de la Policía Nacional Civil desde el año 2005, en el año 2011 se reestructura como grupo de investigación de los delitos informáticos, y posteriormente en el año 2015 se creó la Unidad de delitos especiales para la investigación de Cibercrimenes, actualmente la Policía Nacional Civil tiene una división central de investigación y una Unidad de investigación de delitos informáticos⁵¹.

⁵¹ Entrevista con el Jefe de la Unidad de Investigación de delitos informáticos, Policía Nacional Civil de El Salvador.

CAPITULO II

GENERALIDADES DE LOS DELITOS INFORMÁTICOS Y CONEXOS, EN RELACIÓN A LA REVELACIÓN INDEBIDA DE DATOS O INFORMACIÓN DE CARÁCTER PERSONAL DE LAS MUJERES

El presente capítulo aborda el estudio y análisis de los delitos informáticos y conexos desde la perspectiva doctrinaria ya que en una sociedad informatizada donde los sistemas de información computarizada nos ayudan a realizar investigaciones educativas, culturales, laborales, de conocimiento general y hasta socializar con diferentes personas en redes sociales.

Con los ordenadores surgen también la preocupación ante el uso que determinadas personas o instituciones puedan hacer de la gran masa de datos sobre las personas cuyo control se escapa, así se define al delito informático como cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin, el cual se identifica una diversidad de características donde se pueden vulnerar la privacidad de las personas con la revelación de información o datos, imágenes, videos, audios, textos, y su realización en el tiempo y espacio por medio tangibles o intangibles en diferentes sistemas informáticos y de difícil comprobación.

Refiriéndose a los diferentes tipos de delitos informáticos se analizara algunos enfocados en la revelación indebida de datos de carácter personal, confidencialidad, la integridad y privacidad, cuando los medios de almacenamiento de datos informáticos es donde se encuentra la información personal de los usuarios de carácter persona y privado se comprenderá cada uno de ellos.

Las redes sociales es aquella estructura basada en el internet con el objetivo de interactuar y crear relaciones con otras personas ya sean de amistad, laborales, familiares o amorosas, el cual cada individuo publica información que quieren dar a conocer no obstante está expuesta a cierto determinado público de elección del usuario la puede poner público o con restricciones, de esto se deriva la vulnerabilidad de la información expuesta a otros.

2.1 Definiciones del delito Informático

Para el análisis del delito informático se aclara que los expertos han discutido acerca de lo que constituye un delito informático entre los diversos autores no se ha establecido una definición de delito informático que sea válida en el plano mundial, lo común ha sido que se utilicen definiciones funcionales ya que esto implica actividades criminales de carácter tradicional como fraudes, falsificaciones⁵² y perjuicios que en general son motivo de sanción penal, vulnerando los derechos del titular por medio del *hardware* o *software*⁵³ de las cuales se citan las siguientes definiciones:

El delito informático es la realización de una acción que reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo empleando un elemento informativo o telemático contra los derechos y libertades de los ciudadanos⁵⁴, es decir todo delito informático que atenta la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos.

⁵² Naciones Unidas, "Revista internacional de política criminal" Manual de las Naciones Unidas sobre prevención y control de delitos informáticos, n. 43 y 44 (1994), 5.

⁵³ Miguel Ángel Davara Rodríguez, *Manual de Derecho Informático*, 8ª ed. (España: Aranzadi, 2006), 358.

⁵⁴ Consejo de la Judicatura, Órgano doctrinario e informativo del H. Tribunal Superior de Justicia del Estado de Veracruz-Llave, "Revista Jurídica Veracruzana", n. 93 (2011): 63.

Se define a los delitos electrónicos o informáticos en un sentido amplio, como cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones⁵⁵ desempeñando un papel ya sea como método, medio o fin.

Los delitos informáticos son aquellos que se proporcionan con la ayuda de la informática o de técnicas conexas⁵⁶, es decir que los delitos informáticos están estrictamente relacionados con los sistemas de la informática para su realización.

El delito informático, en forma típica y atípica, entendiendo por la primera a las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y por las segundas a las actitudes ilícitas en que se tienen a las computadoras como instrumento o fin⁵⁷.

El departamento de investigación de la Universidad de México, establece que los delitos informáticos son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático, por otra parte, la Organización para la Cooperación Económica y el Desarrollo (OCED) lo define como cualquier

⁵⁵ María de la Luz Lima, *Delitos Electrónicos*, Academia mexicana de ciencias penales, (México: Porrúa, 1984), 100.

⁵⁶ Nidia Callegari, "Delitos informáticos y legislación", (Revista de la facultad de derecho y ciencias políticas de la Universidad Pontificia Bolivariana, Medellín Colombia 1985), 115. El especialista en esta materia definió al delito informático analizándolo como aquellas conductas típicas antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin, siendo este el más completo al definir, Julio Téllez Valdés.

⁵⁷ Leo Vladimir Benavides Salamanca, Marlon Iban Hernández Anzora, Kenia Kati León Ardon, "La penalización de los delitos informáticos en El Salvador" (tesis para optar al título de Licenciado en Ciencias Jurídicas, Universidad de El Salvador, 2005), 4.

conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos⁵⁸.

Los delitos informáticos en general se pueden establecer que son todos aquellos delitos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo por la utilización indebida de los medios informáticos⁵⁹.

2.2 Características del delito informático

En forma general las principales características que revisten los delitos informáticos son: Conductas criminógenas de cuello blanco, acciones ocupacionales que muchas veces se realizan cuando el sujeto se encuentra trabajando, acciones de oportunidad, en cuanto a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico⁶⁰, provocan serias pérdidas económicas, ofrecen facilidades de tiempo y espacio ya que en milésimas de segundos y sin una necesaria presencia física pueden llegar a consumarse, son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de conocimiento del Derecho.

Siguiendo con las diferentes características; presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico, ofrecen

⁵⁸ *Ibíd.* P.39.

⁵⁹ Consejo de la Judicatura, Órgano doctrinario e informativo del H. Tribunal Superior de Justicia del Estado de Veracruz-Llave, "Revista Jurídica Veracruzana", n. 93 (2011), 64.

⁶⁰ La teoría de Sutherland sobre el delito de cuello blanco trata uno de los problemas de tendencia creciente en la sociedad actual, la reacción social es mínima o nula. Javier Sanz. *La escena del crimen, delitos de cuello blanco, teoría criminológica* (consultada 20 de agosto de 2019), https://www.laescenadelcrimen.com/crimen/delitos_cuello_blanco_sutherland/

facilidades para su comisión a los menores de edad, tienden a proliferar cada vez más por lo que requieren una urgente regulación por el momento siguen siendo ilícitos e impunes ante la ley⁶¹.

La rapidez y acercamiento, en tiempo y espacio esta característica dificulta en múltiples ocasiones, la localización de la actividad y su realización con los hechos, llegando incluso a ocultar al verdadero impulsor y al que realiza la acción, es posible modificar un programa, una actividad ilícita en beneficio del autor dejándola como se encontraba en otro sentido el vincular a la persona que ha cometido el hecho con el mismo la falta de especialización en esta materia, la tercera característica es la facilidad de borrar las pruebas, esto hace prácticamente imposible detectar la acción cometida la facilidad que proviene la flexibilidad y dinámica propia del procesamiento informático, que impide detectar una determinada actividad o proceso con posterioridad⁶².

2.3 Clasificación del delito informático

Los delitos informáticos han sido objeto de variadas clasificaciones y se han tenido en cuenta a estos efectos; el perjuicio causado, el papel que la computadora desempeña en la realización del mismo, el modo de actuar del sujeto el tipo penal en que se encuadren los delitos, Clase de actividad que implique según los datos involucrados⁶³.

Se clasifican los delitos informáticos o electrónicos en tres categorías, de acuerdo a como utilizan la tecnología electrónica; Como método: cuando los

⁶¹ *Ibíd.*

⁶² Miguel Ángel Davara Rodríguez, *Manual de Derecho Informático*, 7º ed. (Madrid: Aranzadi, 2005), 368.

⁶³ *Ibíd.* P.44.

individuos utilizan métodos electrónicos para llegar a un resultado ilícito⁶⁴ como medio: en donde para realizar un delito utilizan una computadora como medio o símbolo; como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla⁶⁵.

Según el convenio de la ciberdelincuencia del uno de noviembre de 2001, que fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de Canadá, Japón y China como estados observadores plantea la siguiente clasificación en cuatro grupos: delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. El acceso, la interceptación, la interferencia de los sistemas y datos informáticos y datos personales de una persona no autorizada, se está produciendo cada vez más en soportes informáticos, delitos informáticos de falsificación y fraude informático, delitos relacionados con el contenido y delitos relacionados con infracciones de la propiedad intelectual y derechos conexos⁶⁶.

Se puede establecer que la seguridad informática, también conocida como ciberseguridad o seguridad de tecnología de la información, está relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras, para ello existen una serie de

⁶⁴ María de la Luz Lima La clasificación de los delitos electrónicos de esta autora son tres como método, medio y como fin es decir para llegar el resultado ilícito se necesita de un medio electrónico realizando conductas ilícitas y provocar un daño a una personas o varias

⁶⁵ *Ibíd.* P. 45

⁶⁶ División Computer Forensic, *Delitos Informáticos, tipos de delitos informáticos* (10 de agosto, 2019), [https:// www. Delitos informaticos .info/delitos _ informaticos /tipos _delitos.html](https://www.Delitosinformaticos.info/delitos_informaticos_tipos_delitos.html)

estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

Se considera más clara y acertada la siguiente clasificación que realiza Jover Padró y los agrupa en cinco apartados: el fraude informático, los documentos informáticos y sus falsedades, del sabotaje informático, las defraudaciones a la propiedad intelectual, y de los ataques contra el derecho a la intimidad⁶⁷.

2.4 Tipos de delitos informáticos

Las Naciones Unidas reconoce cuatro tipos de delitos informáticos los cuales son: los fraudes cometidos mediante manipulación de computadoras, falsificaciones informáticas, daños o modificaciones de programas o datos computarizados y el acceso no autorizado a servicios y sistemas informáticos⁶⁸.

Entre otra tipología se mencionan: las estafas informáticas, los delitos informáticos de daño, las defraudaciones de las telecomunicaciones y los ciberdelitos contra la intimidad; estos consisten cuando una persona instala en un *software* un determinado dispositivo para acceder a la información personal sin autorización de su titular⁶⁹.

En nuestra normativa, la Ley especial contra los delitos informáticos y conexos establece los siguientes tipos: delitos contra los sistemas

⁶⁷ Miguel Ángel Davara Rodríguez, *Manual de Derecho Informático*, 7° ed. (Madrid: Aranzadi, 2005), 374

⁶⁸ Andres Hall. *Tipos de delitos* (Argentina, consultado 19 de noviembre de 2019), http://www.forodeseguridad.com/artic/discipl/disc_4016.htm.

⁶⁹ Sistemius, despacho de abogados tecnológicos de Santiago de Compostela. *Ciberdelincuencia: los 4 delitos informáticos más comunes, tipos de ciberdelitos* (España, 2 de diciembre 2018), <https://www.sistemius.com/ciberdelincuencia-4-tipos-de-delitos-informaticos.html>.

tecnológicos de información, delitos meramente informáticos, delitos informáticos relacionados con el contenido de los datos, delitos informáticos contra niños y niñas y adolescentes o personas con discapacidad, y delito contra el orden económico.

2.5 Datos personales o información de carácter personal de las mujeres

Un dato personal tiene mucha importancia para poder lograr identificar a una persona, en nuestro caso a poder identificar una mujer, en la determinación de las características o su comportamiento y adquiere relevancia por esa capacidad identificadora pero también porque se logra influir en la forma en que pueden ser tratados y evaluados⁷⁰, así los datos personales es toda aquella información asociada a una persona que permite la identificación por documentos de identidad, como el estado civil, edad, residencia, profesión.

Un dato es cualquier información que permite identificar a una persona física o la haga identificable⁷¹, por otra parte un dato privado o secreto se puede definir como hechos o noticias de la vida de una persona y estos deben permanecer ignorados, lo íntimo es el ámbito de la vida personal o familiar que se desea que nadie se intervenga, dentro de lo privado es lo que afecta el ámbito de la persona en singular como el honor imagen y nombre⁷², por lo cual estos datos son los que nuestra investigación hace referencia a la protección y a la no revelación de estos sin el consentimiento de su titular.

⁷⁰ Alfredo Chirino. *Manual operativo de protección de datos en El Salvador*, (2015), 28 http://sia.eurosocial-ii.eu/files/docs/1432887451-DT_26_Chirino.pdf. En este tipo de delitos informáticos se encuentra clasificado y enmarcado el delito de la revelación indebida de datos o información de carácter personal, artículo 26, el cual es el tema de estudio que más adelante se analizara.

⁷¹ Protección de datos. *Tipos de datos personales* (Rubí – Barcelona, 15 de noviembre de 2018), <https://www.protecciondatos.org/tipos-de-datos-personales/>.

⁷² Carlos Barriuso Ruiz, *Interpretación del derecho y la informática*, (Madrid 1996), 146.

2.5.1 Clasificación de los datos personales de las mujeres

Existen muchos datos personales que todo ser humano posee, por el simple hecho de ser persona estos datos son recogidos y abarcados en varias clasificaciones o categorías, a continuación se detallan algunas de las clasificaciones, analizando dentro de ellas todos los datos personales.

Datos Identificativos son también denominados como información de identificación personal, estos datos como su nombre lo indica pueden identificar a un individuo específico⁷³ son cualquier información que puede ser utilizada para distinguir a una persona de otra y que puede ser usada para quitarle su anonimato.

Se pueden establecer como datos identificativos de las mujeres, los siguientes: los nombres, apellidos, la fecha y lugar de nacimiento, edad, estado civil, firma, nacionalidad, sexo, datos familiares, número de Documento Único de Identidad, Número de Identificación Tributaria, número de afiliación de seguro social, domicilio, teléfono, entre otros como correo electrónico, fotografías⁷⁴, audios de voz, estos datos son también catalogados como datos personales identificativos⁷⁵.

Toda persona tiene derecho a un nombre propio y a los apellidos de sus padres, o al de uno de ellos dentro del alcance del derecho existen dos órdenes de intereses a considerar primero el social relativo al registro por

⁷³ Margaret Rouse. *Información de identificación personal* (2014), <https://searchdatacenter.techtarget.com/es/definición/información-de-identificación-personal-PII>

⁷⁴ María Estela Raffino. *La fotografía* (Argentina, Publicado 5 de diciembre de 2018), <https://concepto.de/fotografia/>.

⁷⁵ Consultoría de Protección de datos. *Tipos de datos personales* (Rubí – Barcelona, 15 de noviembre de 2018), <https://www.protecciondatos.org/tipos-de-datos-personales/>

parte del Estado de las personas naturales como medio para su identificación social que se puede interpretar como interés público cuya proyección va más allá del mero dato formal y se refiere a la persona considerada tanto de modo individual como social al que se puede interpretar como de interés humano particular⁷⁶.

Asimismo las características físicas de las mujeres como el tipo de sangre, ADN es un ácido nucleico responsable de codificar toda la información genética que compone a un organismo viviente, huella digital, altura, peso, discapacidades, color de piel, iris, cabello y señales particulares son también catalogados como datos de identificación personal⁷⁷.

Los datos laborales de las mujeres son: el puesto o cargo que ocupan, lugar de trabajo, empleador, correo electrónico institucional, teléfono del trabajo, información de trabajos anteriores, sanciones, licencias, seguridad social, aportes, historial de la empresa o institución⁷⁸.

Los datos sociales son útiles para las empresas y la red social es un canal de distribución de contenidos, tienen una noción de situación social se vincula a la posición que ocupa una persona en la sociedad como alta, media en otras palabras la idea hace referencia al estado del sujeto respecto al contexto o al entorno en el que se mueve, estos pueden ser la información de las

⁷⁶ Ayelen Casella y Leonardo Toia. *Derecho al nombre* (Argentina 2012), <http://www.derecho.uba.ar/publicaciones/libros/pdf/la-cadh-y-su-proyeccion-en-el-derecho-argentino/018-casella-toia-nombre-la-cadh-y-su-proyeccion-en-el-da.pdf>

⁷⁷ PRODATO Protección de datos personales. *¿Qué tipo de datos personales hay? Categorías de datos* (México, junio 30, 2011), <https://prodato.mx/2011/06/30/%C2%BFque-tipo-de-datos-personales-hay/>

⁷⁸ Consultores Certificados de primer nivel, expertos en Protección de Datos Personales & Privacy Compliance, HABEAS DAT. *Preguntas Frecuentes: ¿Qué tipo de datos personas hay?* (Servicios en protección de datos personales en Argentina, Colombia, Perú y México, fecha de consulta de página agosto 10, 2019) www.habeasdat.com/faq.html

propiedades de las personas, formas de vida, inscripciones en foros, clubes o asociaciones.

Algunos datos de las mujeres de carácter ideológico, como las creencias religiosas, afiliación política, sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, son considerados como datos personales sensibles, de los que más adelante, en los tipos de datos se estudiarán⁷⁹.

2.5.2 Tipos de datos personales de las mujeres

Existen además algunos tipos de datos personales sobre los cuales puede darse un tratamiento de recolección o administración, estos tipos de datos determina el grado de protección sobre los mismos los cuales son: datos personales íntimos o privados, datos personales sensibles, los cuales tienen relevancia en la investigación y sobre los cuales recae su protección en el delito informático investigado, datos personales semiprivados y datos personales públicos⁸⁰.

Dato personal íntimo o privado es aquel que por su naturaleza íntima o reservada sólo es relevante para el titular de la información, es la información privada concerniente a la mujer, identificada o identificable, o identificativos, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, y número de teléfono, dicha información no debe ser observada o tener acceso indebido por ningún órgano público o privado a excepción que esté

⁷⁹ Consultoría de Protección de datos. *Tipos de datos personales* (Rubí – Barcelona, 15 de noviembre de 2018), <https://www.protecciondatos.org/tipos-de-datos-personales/>

⁸⁰ Industria y comercio Superintendencia. *Protección de datos personales: Aspectos prácticos sobre el derecho de Habeas Data*. (2017), 6. https://protecdatalatam.com/wp-content/uploads/2017/07/Aspectos_Derecho_de_Habeas_Data.pdf

autorizado por el titular, ya que este tiene derecho a controlar su información que la hace parte de su vida privada⁸¹.

Se considera como datos sensibles de las mujeres, aquellos que corresponden a una persona en lo referente al credo, el origen racial, étnico, las convicciones en especial las políticas y religiosas, la pertenencia a un sindicato o partido político, las circunstancias penales, comportamiento sexual y condiciones de salud física y mental, sin embargo los datos considerados neutros ya sea personales públicos privados, se pueden convertir en datos personales sensibles⁸² que afectan la esfera más íntima del ser humano y su divulgación indebida puede ocasionar daño al honor y la intimidad de las personas además se requieren mayor protección y un tratamiento de protección especial.

Estos datos anteriormente referidos, especialmente protege 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 por la Ley de acceso a la información pública vigente en el país y la Ley Especial Contra los Delitos Informáticos y Conexos⁸³ en estudio, así mismo se constituye un principio muy importante que nadie está obligado a proporcionar datos como: origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, Ideas filosóficas, preferencia sexual y datos biométricos.

⁸¹ Natalia Hernández Lotero. *Clasificación de los datos personales e implicaciones legales* (Bolivia, fecha de consulta 13 de noviembre de 2019), <https://repository.upb.edu.co/bitstream/handle/20.500.11912/3595/Clasificaci%C3%B3n%20de%20los%20datos%20personales%20e%20implicaciones%20legales.pdf?sequence=1>.

⁸² María Elena Orellana de Gutiérrez, "Habeas Data" (Tesis de licenciatura: Universidad Salvadoreña Alberto Masferrer, 1994), Monografía proporcionada por Biblioteca de la Corte Suprema de Justicia.

⁸³ Ley especial contra los delitos informáticos y conexos (Aprobada por Decreto Legislativo N° 260, D. O. N° 40, Tomo N° 410, 26 de febrero de 2016), Art 3 m y n

El dato personal semiprivado es aquel dato que no tiene naturaleza íntima reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general⁸⁴ estos datos aun cuando tienen un carácter privado solo le interesa al titular y un determinado grupo de personas las cuales pueden consultar la información mediante una autorización, estos pueden ser financieros, crediticios, dirección, teléfono y correo electrónico⁸⁵.

2.5.3 Revelación indebida de datos personales

El termino revelación tiene su origen etimológico en el vocablo latino *revelatio*,⁸⁶ se trata del acto y el resultado de revelar, por otra parte el vocablo indebido viene etimológicamente del latín *indebitus* que significa lo que no se debe hacer o contar se refiere a contar algo que era secreto, oculto, escondido y separado del conocimiento de los demás, ese secreto por lo tanto es ignorado por la mayoría de las personas excepto por aquellas a quienes se les ha compartido, el revelar puede asociarse a describir, divulgar o a informar algo que no se sabía y que no se debía de divulgar.

Una definición del verbo revelar es descubrir o manifestar lo ignorado o secreto, sin embargo este tipo de delito informático tiene dos verbos relacionados; el verbo de difundir que es propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas, e información privada, como algunos

⁸⁴ Natalia Hernández Lotero. *Clasificación de los datos personales e implicaciones legales* (Bolivia, fecha de consulta 13 de noviembre de 2019), <https://repository.upb.edu.co/bitstream/handle/20.500.11912/3595/clasificasi%C3%B3n%20de%20los%20datos%20personales%20e%20implicaciones%20legales.pdf?sequence=1>

⁸⁵ Industria y comercio Superintendencia. *Protección de datos personales: Aspectos prácticos sobre el derecho de Habeas Data*. (2017), 7. https://protecdatalatam.com/wp-content/uploads/2017/07/Aspectos_Derecho_de_Habeas_Data.pdf

⁸⁶ Julián Pérez Porto y María Merino. *Definición de revelación* (Publicado: 2014. Actualizado: 2016), <https://definicion.de/revelacion/>.

personales y el verbo de ceder, que es dar, transferir o traspasar a alguien una cosa, acción, derecho o información⁸⁷.

Se puede establecer del párrafo anterior, que el término revelación es el descubrimiento o la simple manifestación de algo que es secreto y que no se debe revelar, por lo que debe permanecer en lo oculto o desconocido de las demás personas como lo son algunos de los datos personales que de cada ser humano posee, por lo que se deben de proteger y que cada individuo es responsable de guardarlos y mantenerlos en secreto o bien el manifestarlos, expresarlos o divulgarlos a terceros con su consentimiento a través de los distintos nuevos medios tecnológicos.

Existe un peligro real para aquellas personas que tienen almacenados datos personales en un archivo y es necesario estructurar una normativa específica orientada a la protección de la información personal⁸⁸ en relación a que la sociedad actual ha crecido y evolucionado en los últimos años así también se han desarrollado muchos avances tecnológicos, es por ello que se requiere un tratamiento automatizado de los datos⁸⁹.

La evolución a la que se hace referencia anteriormente es producto de la crisis de la representativa división entre lo público y lo privado se habla así de derechos y libertades de tercera generación, conocidos como derechos de solidaridad o de los pueblos contempla cuestiones que traspasa los límites de lo nacional como el derecho a la paz y un medio ambiente sano y entre

⁸⁷ FGR y UNODC. *Análisis jurídico de los delitos contenidos en los capítulos I II III y V del Título segundo de la Ley especial contra los delitos informáticos y conexos* (El Salvador, 2018), <http://escuela.fgr.gob.sv/wp-content/uploads/leyes-nuevas/analisis-juridico-de-la-ley-especial-contra-los-delitos-informaticos-y-conexos-COMPLETO-CAP-I-II-III-V.pdf>.

⁸⁸ Renato Javier Jijena Leiva, *Chile La Protección Penal de la Intimidación y el Delito Informático*, (Chile: Editorial Jurídica de Chile, 1992), 30.

⁸⁹ Carlos Barriuso Ruiz, *Interpretación del derecho y la informática*, (Madrid 1996), 146.

algunos ejemplos de estos derechos son: derecho a la cooperación internacional y regional, derecho a la justicia internacional y el uso de los avances de las ciencias y la tecnología relacionándolo a la protección de datos, que vienen a construir nuevas garantías del individuo frente a la contaminación de las libertades en la nueva sociedad tecnológica⁹⁰.

2.6 Catálogo de derechos de las mujeres en El Salvador

La ley especial integral para una vida libre de violencia para las mujeres, establece el derecho de las mujeres a una vida libre de violencia, el cual 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 subordinación⁹¹.

Igualmente se refiere al goce, ejercicio y protección de los derechos humanos y las libertades consagradas en la Constitución y en los Instrumentos Nacionales e Internacionales⁹², incluidos los siguientes derechos:

1. Que se respete su vida y su integridad física, psíquica y moral
2. Que se respete la dignidad inherente a su persona y se le brinde protección a su familia
3. La libertad a la seguridad personal
4. No ser sometida a tortura o tratos humillantes
5. La igualdad de protección ante la ley y de la ley

⁹⁰ Fermín Morales Prats, *La protección del derecho a la intimidad de las personas (fichero de datos)*, (Madrid, 1997), 47.

⁹¹ Ley especial integral para una vida libre de violencia para las mujeres (Aprobada por Decreto Legislativo N° 520, D. O. N° 2, Tomo N° 390, 04 de enero de 2012), Art 2 1-9

⁹² Como el 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.

6. Un recurso sencillo y rápido ante los tribunales competentes que la amparen frente a hechos que violen sus derechos⁹³
7. La libertad de asociación
8. Profesar la religión y las creencias
9. Participar en los asuntos públicos incluyendo cargos públicos

2.7 Derechos vulnerados en el delito informático de la revelación indebida de datos o información de carácter personal de las mujeres

2.7.1 Habeas Data o Derecho a la protección de datos personales

El derecho de habeas data o protección de datos personales consiste en la facultad de conocer, actualizar, rectificar y eliminar la información que se haya recogido de las personas en archivos y bases de datos⁹⁴, así también la facultad que tienen las personas de velar porque la información personal otorgada a terceros recolectada en base de datos o archivos sea tratada apropiadamente⁹⁵.

La protección de datos se refiere a las prácticas, salvaguardas y principios fundamentales puestos en ejercicio para proteger al individuo contra el uso indebido de los datos personales por parte de entidades públicas o privadas y asegurar que el titular de la información se mantenga en control de ella, y así evitar el cometimiento de delitos informáticos.

⁹³ Al ser víctimas de delitos, las mujeres tienen derecho a que se les proteja por medio de las leyes y los debidos procedimientos para poder llevar a cabo los hechos delictivos a sus consecuencias y poder así interponer penas a los agresores.

⁹⁴ Sala de lo Constitucional, *Sentencia de Amparo, referencia: 118-2002* (El Salvador: Corte Suprema de Justicia 2004).

⁹⁵ Industria y comercio Superintendencia. *Protección de datos personales: Aspectos prácticos sobre el derecho de Habeas Data*. (2017), 6. https://protecdatalatam.com/wp-content/uploads/2017/07/Aspectos_Derecho_de_Habeas_Data.pdf

A través del hábeas data se persiguen los objetivos siguientes: el derecho de acceso a la información, debido a que es la pieza central que consiste en el derecho de toda persona a conocer los datos que se encuentran registrados en relación a ella en un registro o fichero y el derecho a la actualización de la información, derecho a la rectificación de la información, derecho a la exclusión, derecho a la confidencialidad, este consiste en la pretensión de que ciertos datos relativos a un individuo permanezcan reservados y que no puedan suministrarse a terceros⁹⁶.

Compartir información personal puede implicar beneficios sociales, culturales, políticos, económicos, educativos, pero en algunos casos incluso es necesario hacerlo para cumplir con las tareas cotidianas y para mantenerse en contacto en la sociedad moderna y relaciones personales, pero esto implica un riesgo inminente, la información personal revela mucho acerca de la misma, de sus pensamientos, gustos y de su vida en general.

Un tercero que ingrese ilegítimamente en un banco de datos⁹⁷ realiza una acción tan reprochable contra el titular de esos datos como quien allana un domicilio sin orden judicial, perturbando en tal grado el derecho a la intimidad, esto es así incluso aunque los datos no sean reservados ya que implica divulgar circunstancias que el interesado puede tener interés en que no se difundan más allá de un círculo determinado, cosa diferente es que el titular de la información de su consentimiento para que se divulgue⁹⁸.

⁹⁶ María Elena Orellana de Gutiérrez, "Habeas Data" (Tesis de licenciatura: Universidad Salvadoreña Alberto Masferrer, 1994), 63.

⁹⁷ Banco de datos es el conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. La mayoría de las bases de datos se encuentran en formatos digitales. Josefina López Herrera, *Programación en Tiempo Real y Bases de Datos: Un Enfoque Práctico*, Universidad Politécnica de Catalunya, (Barcelona, España: Iniciativa Digital Politécnica, 2011). 18.

⁹⁸ *Ibíd.*

El derecho a la protección de datos personales, está integrado por una serie de prerrogativas, principios y procedimientos para el tratamiento de información que concierne a las personas físicas no sólo por parte del Estado o los entes públicos, sino también, por parte de terceros o personas de derecho privado⁹⁹.

2.7.2 Derecho a la privacidad

El concepto de privacidad deriva de la palabra inglesa *privacy* que no tiene una traducción concreta al castellano, pero que alude a un cierto aislamiento de los ciudadanos y a una expectativa de no ser arrastrados a la publicidad dentro del concepto de privacidad existe la necesidad o relación con el termino intimidad que se puede decir que son términos inherentes a la persona humana y que el respeto a la vida privada permitirá que la personalidad del ser humano se desarrolle libremente, de esta forma, la protección a la vida privada se constituye en un criterio de carácter democrático de toda sociedad, se trata sin duda de un concepto que tiene que ver con la naturaleza anglosajona, pero que ha sido conectada muchas veces también con el problema práctico de la protección de las personas frente al abuso de sus datos personales¹⁰⁰.

El respeto a la vida privada y a la intimidad tanto personal como familiar se constituye en un valor fundamental del ser humano, razón por la cual el derecho ha considerado importante tutelarlos y dictar medidas para evitar su violación así como para intentar subsanar los daños ocasionados, de esta manera, surge el llamado derecho a la privacidad, a la vida privada o

⁹⁹ Alfredo Chirino. *Manual operativo de protección de datos en el salvador*, (2015), 30. http://sia.eurosocial-ii.eu/files/docs/1432887451-DT_26_Chirino.pdf

¹⁰⁰ *Ibíd.*

simplemente derecho a la intimidad como un derecho humano fundamental por virtud del cual se tiene la facultad de excluir o negar a las demás personas del conocimiento de ciertos aspectos de la vida de cada persona¹⁰¹.

2.7.3 Derecho a la identidad

El derecho a la identidad es uno de los derechos fundamentales de todo ser humano y es necesario para poder beneficiarse de los otros derechos fundamentales, este derecho está relacionado de igual manera con los derechos a un nombre y un apellido desde su nacimiento el niño y niña tiene derecho a tener un nombre y un apellido a ser registrado inmediatamente¹⁰² después de su nacimiento ya que los padres tienen la obligación de informar el nombre, el apellido y la fecha de nacimiento del recién nacido¹⁰³.

2.7.4 Derecho a la propia imagen

El derecho a la propia imagen atribuye a su titular la potestad para disponer de su imagen física imposibilitando su difusión salvo que exprese su propio consentimiento, es decir la facultad de decidir cuándo a su figura puede ser reproducida por un tercero y cuando no pero los avances tecnológicos permiten mil maneras de reproducir la imagen de una persona sin que ésta pueda llegar a percibirse, razón por la cual la defensa de forma autónoma de

¹⁰¹ Cuauhtémoc M. *El derecho a la intimidad, al honor y a la propia imagen* (revista jurídica IUS, Universidad Latina de América), <http://www.unla.mx/lusunla3/reflexion/derecho%20a%20la%20intimidad.htm>.

¹⁰² Su registro permitirá al niño preservar sus orígenes, es decir, las relaciones de parentesco que lo unen a sus padres biológicos.

¹⁰³ Rosa María Sánchez, Miriam Gutiérrez. *Derecho a una identidad*. <https://www.humanium.org/es/derecho-identidad/>.

este derecho de la personalidad diferenciándolo del derecho al honor y del derecho a la intimidad, ilegítimas sobre la vida de la persona¹⁰⁴.

El derecho a la propia imagen es conforme la jurisprudencia española como aquella facultad exclusiva del interesado a difundir o publicar su propia imagen y por ende su derecho a evitar su reproducción en cuanto se trate de un derecho de la personalidad¹⁰⁵, por otra parte es un derecho de la personalidad, con un contenido propio, específico y diferenciado de los demás, derivado de la dignidad humana y dirigido a proteger la dimensión moral de las personas.

Atribuye a su titular un derecho a determinar la información gráfica generada por sus rasgos físicos personales que puede tener difusión pública (vertiente positiva del derecho). La facultad otorgada por este derecho, en tanto que derecho fundamental, consiste en esencia en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad: informativa, comercial, científica, cultural, perseguida por quien la capta o difunde. (Vertiente negativa del derecho)¹⁰⁶.

2.7.5 Derecho a la intimidad

Algunos autores piensan que la intimidad, es una necesidad humana y un derecho innato del hombre por lo que es soberano y anterior a su regulación

¹⁰⁴ Marc Carrillo *El derecho a la propia imagen*. 15 Marzo 20103. https://elpais.com/diario/2003/03/15/catalunya/1047694043_850215.html.

¹⁰⁵ María Elena Orellana de Gutiérrez, "Habeas Data" (Tesis de licenciatura: Universidad Salvadoreña Alberto Masferrer, 1994)

¹⁰⁶ Guías Jurídicas Wolters Kluver. *Derecho a la propia imagen* (Consultado 19 mayo 2020), <https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEA MtMSbF1jTAAAkMjU1MjE7Wy1KLizPw8WyMDQ3MDcyMDkEBmWqVLfnJIZUGqbVpiTnEqA JohrjY1AAAAWKE>.

positiva, si bien la idea de intimidad implica una gran diversidad de perfiles y criterios en ocasiones confusos difíciles de precisar lo cual lleva a la conclusión de que no existe una definición particular válida en torno a la cual haya unanimidad, igualmente el concepto es más indeterminado y dependiente del medio social y cultural¹⁰⁷ .

Cuando se habla de intimidad normalmente se hace referencia a la intimidad individual, el más íntimo, descubriendo que su origen proviene del adverbio intus, traducido por entre o hacia adentro y que es utilizada, en un inicio para referirse al ámbito más profundo, inherente y reservado de la personalidad del ser humano. no obstante también el núcleo familiar como institución goza del derecho a la Intimidad, es decir, el derecho es comprendido en cuanto a miembros de una familia y no en cuanto a personas en sí o individuales, es así que el derecho a la Intimidad se amplía no sólo a los aspectos de la vida propia personal, sino también a determinados aspectos de otras personas con las que se tenga una personal y estrecha vinculación familiar ¹⁰⁸ .

El concepto de intimidad es asumido por la mayoría de los autores como sinónimo de privacidad o de vida privada, por lo tanto comprende los diversos actos, situaciones y circunstancias que por su carácter personalísimo no deben estar expuestos a la curiosidad y a la divulgación, sino salvaguardados de la injerencia extraña¹⁰⁹, la necesidad a la intimidad es inherente a la persona humana para su desarrollo y personalidad.

¹⁰⁷ Athina Vanessa García Mejía et al, “El intrusismo informático y la utilización del Derecho Penal como mecanismo de tutela del derecho a la intimidad”. (Tesis de Licenciatura: Universidad de El Salvador, 2017). El origen de la palabra intimidad se encuentra en intimus, la cual se traduce del latín por íntimo, Norberto González Caytano, *El deber del respeto a la intimidad*, (España: S.A. EUNSA ediciones Universidad de Navarra, 1990).104.

¹⁰⁸ Ana Laura Cabezuelo Arenas, *Derecho de Intimidad*, (Valencia: tirant lo Blanch, 1998).

¹⁰⁹ Mario Madrid Malo Garizabal, *Derechos Fundamentales*, 2º ed. (Bogotá, Colombia: 3R Editores, 1997), 38.

El elemento intimidad es intensamente complejo de ahí el conflicto de precisar su naturaleza jurídica, pero el autor relaciona su naturaleza como psicosocial porque se considera un bien moral de la espiritualidad de cada ser humano potestad que tiene de suprimir a los demás de su esfera íntima o compartirla con cierto grupo de personas que él considere de su confianza, sin embargo para este autor también pertenece a la clase de derecho personalísimo por ser éste inherente al desarrollo del ser humano, al ofrecerle la decisión de proteger para sí todos los hechos, pensamientos, emociones y sentimientos que la persona decida no compartir con el resto de la sociedad ¹¹⁰.

Para que sea considerado derecho fundamental debe cumplir con las siguientes características: debe de ser protegido por la constitución, de allí que toda norma que los vulnere es inconstitucional y por lo tanto nula por regla general debe poseer protección judicial en todos los sentidos, así la observancia de éstos se hallan completamente vigilada por los tribunales y establecen la organización de una sociedad, es decir estos tienen límites¹¹¹.

El respeto a la intimidad tanto personal como familiar se compone en un valor fundamental del ser humano, razón por la cual el derecho ha considerado transcendental tutelado y dictar medidas para evitar su violación así como para intentar subsanar los daños ocasionados, de esta manera, surgen el llamado derecho a la intimidad, como un derecho humano fundamental por virtud del cual, se tiene la facultad de excluir o negar a las demás personas del conocimiento de ciertos aspectos de la vida personal, aspectos que las sociedades deben velar por proteger.

¹¹⁰ Luis Fariñas Matoni, *El Derecho a la Intimidad*, (España: Trívium, 1983), 208.

¹¹¹ Robert Alexi, *Los Derechos Fundamentales en el Estado Democrático de Derecho*, en Neoconstitucionalismo, (Madrid: Trotta, 2003). 32.

2.8 Tipos y Modalidades de violencia contra las mujeres

El Tipo de 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 económicas¹¹².

El Tipo de Violencia Femenicida 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 mujeres¹¹³.

El Tipo de 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.

El Tipo de 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,

¹¹² Ley especial contra los delitos informáticos y conexos (Aprobada por Decreto Legislativo N° 260, D. O. N° 40, Tomo N° 410, 26 de febrero de 2016), Art 9 a, b, c, d, e, f, g

¹¹³ En este tipo de violencia se puede establecer que la revelación de datos personales en las mujeres no solo atenta contra el derecho de protección de sus datos, sino que en este apartado se abarcan la violencia de todos los derechos humanos de las mujeres, tanto en el ámbito público como privado.

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, este tipo de violencia contra las mujeres no tiene por qué alcanzar el hostigamiento o la humillación, sino que puede manifestarse como acoso, restricción, humillación, manipulación o aislamiento, produciendo daños emocionales y perjudicando un desarrollo personal hasta problemas emocionales y psicológicos muy graves que han llevado a muchas mujeres al suicidio..

El Tipo de Violencia Sexual es toda conducta que amenace o vulnere el derecho de la mujer a decidir voluntariamente su vida sexual¹¹⁴, 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.

El Tipo de 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 sociedad¹¹⁵.

La Modalidad de Violencia Comunitaria se refiere a toda acción u omisión abusiva que a partir de actos individuales o colectivos que transgreden los derechos fundamentales de la mujer y propician su denigración,

¹¹⁴ Ayuda en acción. *Blog Mujer. tipos de Violencia contra las mujeres* (05 de julio de 2018), <https://www.ayudaenaccion.org/ong/blog/mujer/tipos-violencia-mujeres/>.

¹¹⁵ Mujer Coomeva. *Violencia contra las mujeres* (fecha de consulta: 19 mayo 2020), <http://www.coomeva.com/publicaciones.php?id=45139>.

discriminación, marginación o exclusión¹¹⁶, y la mayoría de mujeres es víctima de esta modalidad de violencia con la ayuda de las tecnologías de la información y las redes sociales.

La Modalidad de 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.

La Modalidad de Violencia Laboral¹¹⁷ se establece que son las 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 trabajo¹¹⁸, existen forma de violencia, la interna es la que se da en el lugar de trabajo es la que tiene entre los trabajadores, incluidos directores y supervisores, la segunda es la violencia externa es aquella que tiene lugar entre los trabajadores, y otra persona presente en el lugar de trabajo se refiere a la violencia ejercida contra una empleada por parte de la clientela.

¹¹⁶ Ley especial contra los delitos informáticos y conexos (Aprobada por Decreto Legislativo N° 260, D. O. N° 40, Tomo N° 410, 26 de febrero de 2016),

¹¹⁷ Ley especial integral para una vida libre de violencia para las mujeres (Aprobada por Decreto Legislativo N° 520, D. O. N° 2, Tomo N° 390, 04 de enero de 2012), Art. 10

¹¹⁸ La modalidad de violencia en las mujeres en relación al artículo 26 de la ley especial de delitos informáticos se puede observar en la violencia comunitaria en los actos individuales y colectivos que trasgreden sus derechos fundamentales, y en la violencia institucional la cual es toda acción abusiva de cualquier servidor público en relación a la divulgación de datos personales resguardados o proporcionados en las instituciones públicas.

2.9 El internet y las redes sociales como instrumento del delito informático de la revelación indebida de datos o información de carácter personal de las mujeres

La expansión del internet ha desarrollado un incremento del número y clase de servicios que están disponibles a través de la red como el acceso a toda clase de información y documentación en cualquier lugar del mundo así como la posibilidad de comunicarse con un número ilimitado de personas en cualquier país en el que se encuentren, el acceso a nuevas formas de ocio y la posibilidad de adquirir servicios o bienes de cualquier clase a través del comercio electrónico¹¹⁹.

En el mundo de las tecnologías en el proceso de producción ya sea turístico, deportivo, comercial, educativo, social, financiero, político en estos se utilizan actualmente computadoras y el internet algunos autores lo llaman como la era de la informática donde todas las personas están conectadas en la nueva sociedad digital¹²⁰.

El masivo acceso al internet ha permitido ampliar el conocimiento de los personas, tanto en adultos, jóvenes y hasta niños con el permiso y supervisión de los padres, esto a través de las tecnologías de la información y comunicación generando espacios de intercambio y aprendizaje, en donde se comparten contenidos que han desarrollado una capacidad de control y movilización¹²¹.

¹¹⁹ Ana Garriga Domínguez, *Nuevas tecnologías y derechos humanos. Algunas consideraciones sobre los derechos humanos en internet*, (Valencia: Tirant lo Blanch, 2014), 87

¹²⁰ Jorge Eduardo Buompadre, *Violencia de género en la era digital. Modalidades mediante el uso de la tecnología*, (Buenos Aires, Bogotá: Astrea, 2016), 2.

¹²¹ Florencia Barindelli, Carlos G. Gregorio, *Datos personales y libertad de expresión en las redes sociales digitales*, (Argentina: AD-HOC, 2010), 9.

Las tecnologías de la información y la comunicación ofrecen la posibilidad de intervenir y participar en un nuevo espacio público, el internet genera un ámbito vivo y nuevo sin fronteras, se crea un verdadero intercambio entre las personas que acceden a la red.

La web 2.0 ha dado lugar a un gran número de comunidades de usuarios, agrupados alrededor de una plataforma común, es en ese contexto que han surgido las redes sociales, no obstante esta idea no es tan actual¹²², que el origen del concepto de red social puede encontrarse en la teoría denominada de los seis grados, esta teoría fue enunciada originalmente por Karinthy en 1929, en la que establecía que cualquier persona puede interactuar con cualquier otra en el mundo a través de un máximo de seis conexiones, de este modo el número de conocidos crecía numerosamente con el número de conexiones en la cadena¹²³.

Las red social es aquel conjunto de personas que tienen vínculos entre sí, las redes sociales son estructuras formadas en internet por personas u organizaciones que se conectan, están creadas para el intercambio de información han respaldado un nivel de divulgación de información personal incluidas las grandes cantidades de contenido, datos, fotografías y videos de los usuarios que comparten en estas redes así como de terceros, sin ningún precedente, por otra parte existen auténticos programas rastreadores o espías utilizados para la protección y lucha de delincuencia cibernética en las cuales no se respetan los derechos humanos¹²⁴.

¹²² Barriuso Ruiz C., *Las redes sociales y la protección de datos*, Anuario Facultad de Derecho, Universidad de Alcalá II (Alcalá 2009), 301

¹²³ Albert Agustinoy Guilayn, Jorge Monclus Ruiz, *Aspectos legales de las redes sociales*, 2º ed. (Madrid España: Bosch, 2019), 19.

¹²⁴ Ana Garriga Domínguez, *Nuevas tecnologías y derechos humanos. Algunas consideraciones sobre los derechos humanos en internet*, (Valencia, 2014), 89

Se establece que las redes sociales son servicios entre las plataformas web que permiten al usuario realizar las acciones de construir un perfil público o semipúblico dentro de un sistema limitado, permite unir una lista de otros usuarios con los que se comparte conexión y visualizar o rastrear una lista de contactos elaborados por otros usuarios dentro de sistema.

Las redes sociales como formas de interacción social entre personas de distintos intereses y a su vez las define como un intercambio dinámico entre todo tipo de personas, grupos e instituciones en contextos de complejidad generando interacciones con diferentes tipos de usuarios llevando a la creación de una comunidad digital sean sociales, culturales, económicas, políticas, deportivas, ideológicas, íntimas y cualquier otras relaciones de interés de los usuarios¹²⁵.

2.9.1 Los riesgos al utilizar y subir información de carácter personal al internet

La percepción de los riesgos a los que las mujeres están expuestas en el internet, está determinada a la práctica o del manejo de las redes sociales y las nuevas tecnologías existentes en el mundo digital, los siguientes casos son algunas situaciones consideradas como peligrosas en el internet¹²⁶.

El elemento esencial del que se nutren las redes sociales son los contenidos de los datos personales de sus usuarios que ponen a disposición del resto de miembros de la red, como los textos referidos a circunstancias propias del usuario fotos, videos familiares o con amigos, son elementos habituales en

¹²⁵ Sergio Balardini, *Datos personales y libertad de expresión en las redes sociales digitales*, (Argentina) 86.

¹²⁶ Laura León Kanashiro, *Datos personales y libertad de expresión en las redes sociales digitales*, (Argentina) 45.

este tipo de redes, permitiendo una identificación de la persona hasta obtener un perfil muy detallado de su personalidad, aficiones, formación, trabajo y hasta la residencia¹²⁷.

El primer caso que se ha analizado, es el alcance que puede tener una foto íntima compartida con alguien, se debe tener en cuenta que al compartir esta imagen, la situación puede volverse perjudicial, debido a que con ese contenido la otra persona cuenta con la posibilidad de hacer chantaje y aprovechar el miedo que puede generar en la víctima, el que alguien pudiera ver este contenido¹²⁸ lo peor de estas situaciones es que todo queda en el aire, las personas o mujeres que se ven envueltas en esta situación no acuden a nadie y por tanto no existe ninguna denuncia ni rastro de los agresores, los hechos se quedan impunes.

El internet posee tanto contenidos constructivos como perjudiciales, dentro de los perjudiciales para las mujeres, que es lo que se está estudiando, se puede mencionar la información que degrada a la mujer y el uso de violencia contra ella, ya sea sexual o/y física¹²⁹ a través de las redes y utilizando su información personal.

2.9.2 La violencia de género en las redes sociales

La violencia de género es un fenómeno global, y es cualquier acto violento o de agresión manifestados de diferentes maneras en constante crecimiento y que se ha extendido en todos los aspectos de la sociedad, su estructura

¹²⁷ Ibid.

¹²⁸ Damián Montero. *Violencia de género en redes sociales, un peligro silencioso*, (Europa, 2019), <https://www.hacerfamilia.com/actualidad/violencia-genero-redes-sociales-peligro-silencioso-20170422173729.html>

¹²⁹ Ibid.

representa uno de los problemas más graves y complejos que enfrenta la sociedad actual a través de las nuevas tecnologías de comunicación¹³⁰.

Se puede establecer que la violencia de género contra las mujeres es una expresión de las relaciones desiguales de poder entre hombres y mujeres está basada en la construcción social, cultural e histórica de la superioridad de un género sobre otro, es decir de los hombres sobre las mujeres se encuentra como conductas inferioridad, desvalorizarlas de manera general encontrar defectos en sus actuaciones¹³¹.

Se adopta la definición de violencia contra la mujer establecida por la CEDAW y la Convención de Belem Do Pará: como cualquier acción o conducta, dirigida contra la mujer basada en su género, sea porque es mujer o que la afecta en forma desproporcionada en grado de amenaza o efectiva, que tenga o pueda tener como resultado muerte, daño, lesiones, trastornos del desarrollo, privaciones o sufrimiento físico, sexual, psicológico o patrimonial a la mujer, tanto en el ámbito público como privado¹³².

El control hacia las mujeres a través de aplicaciones como *Whatsapp*, *Instagram*, *Facebook* y los comentarios manifestados en las redes pueden convertirse en un tipo de violencia psicológica en el que las mujeres más jóvenes se ven inmersas sin ni siquiera detectar que están siendo objeto de maltrato, estas agresiones *on line* pueden convertirse en los primeros pasos

¹³⁰ Jorge Eduardo Buompadre, *Violencia de género en la era digital. Modalidades mediante el uso de la tecnología*, (Buenos Aires- Bogotá- Porto Alegre, 2016), 39.

¹³¹ Rebeca Arias Flores, Helene Van Acker, Arianna Calza Bini, Programa de las naciones unidas para el desarrollo. Informe "Violencia de género en El Salvador", (El Salvador, Mayo 2000), 23.

¹³² Instituto Salvadoreño para el desarrollo de la mujer, *Segundo Informe Nacional sobre la situación de violencia contra las mujeres en El Salvador* (El Salvador, 2010) 19. La Convención sobre la Eliminación de toda forma de Discriminación contra la Mujer.(CEDAW son sus siglas en inglés)

hacia la violencia física, la ciberviolencia de género hace por sí sola tanto daño, más que el físico, ya que traspasa el ámbito privado y por otra entran en juego dos factores propios de las redes sociales, como son la viralidad y la perpetuidad de los mensajes¹³³, la violencia contra las mujeres se extiende también a través de los chats, el cual es muy utilizado por las mujeres adolescentes y estas pueden ser víctimas de violencia por este medio¹³⁴.

No es difícil encontrar en internet muchas fotos e imágenes de mujeres, en donde se puede establecer las múltiples formas de violencia contra ellas, imágenes altamente racistas y sexistas que representan una distorsión de lo que las mujeres son las imágenes de fotografías de mujeres que son subidas a las redes, la violencia de género contra las mujeres, real o virtual, no es un problema de las mujeres sino de la cultura masculina/patriarcal, es un problema social de los hombres contra las mujeres¹³⁵.

¹³³ Miryam García en Zinetik Consultores. *Violencia de género en redes sociales* (8 noviembre 2019), <https://zinetik.com/violencia-de-genero/>. La Ciberviolencia de género es aquella violencia desarrollada frente a la mujer que se sustancia en el mundo virtual, utilizando las nuevas tecnologías como medio para ejercer daño o dominio

¹³⁴ María Cruz Rubio Liniers, *Medios de comunicación y violencia contra las mujeres, Internet y la violencia contra las mujeres* (Sevilla, 2003), 205.

¹³⁵ Ana Elena Obando, *Medios de comunicación y violencia contra las mujeres, Violencia contra las mujeres y nuevas tecnologías: un repaso al "mundo virtual"*, (Sevilla, 2003), 181.

CAPITULO III

ANÁLISIS Y REGULACIÓN JURÍDICA DEL DELITO INFORMÁTICO DE LA REVELACIÓN INDEBIDA DE DATOS O INFORMACIÓN DE CARÁCTER PERSONAL

El objetivo que se pretende alcanzar con el desarrollo del presente capítulo es realizar un análisis jurídico sobre el delito de revelación indebida de datos o información de carácter personal, con énfasis en las mujeres como víctimas de dicho delito, previsto y sancionado en el artículo 26 de la Ley Especial Contra Los Delitos Informáticos y Conexos.

Dicha Ley protege los bienes jurídicos de conductas ilícitas cometidas por medio de las tecnologías informáticas y tecnologías de la comunicación, así como prevenir y sancionar los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su estructura o cualquiera de sus componentes, o los delitos cometidos mediante la utilización de dichas tecnologías que afecten intereses relacionados con la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas.

La Ley Especial Contra Los Delitos Informáticos y Conexos, tiene aplicación en los hechos punibles cometidos totalmente o parcialmente en el territorio de El Salvador o en los lugares que se encuentren sometidos a su jurisdicción, también tiene aplicación a las personas naturales o jurídicas ya sean nacionales o extranjeras que cometan delitos que afecten bienes jurídicos del Estado salvadoreño, de sus habitantes, o protegidos por pactos o tratados internacionales que hayan sido ratificados por El Salvador, o en los casos que la ejecución del hecho delictivo se haya iniciado en territorio

extranjero pero que se consumó en territorio salvadoreño o si se realizara utilizando tecnologías de la información y comunicación que estuvieran instaladas en el territorio salvadoreño y el responsable no haya sido juzgado por tal delito por los tribunales extranjeros o no se le haya impuesto una condena.

En este capítulo se estudiarán tanto las normas nacionales que regulan la protección de la información de carácter personal, como las normas internacionales a las que El Salvador se ha suscrito y ratificado, se realiza un estudio de derecho comparado de legislaciones internacionales que poseen normas similares a las nuestras que regulan este tipo de delitos, para evidenciar las diferencias y similitudes que puedan existir entre unas y otras.

Se presente jurisprudencia nacional sobre el delito de revelación indebida de datos o información de carácter personal y jurisprudencia internacional relacionada con el delito en cuestión, realizando un breve análisis sobre ambas sentencias.

3.1 Normativa Primaria que regula el derecho a la intimidad de las personas

3.1.1 Constitución de la Republica de El Salvador

La actual Constitución de la República de El Salvador¹³⁶, constituye la norma primordial y suprema, lo anteriormente está consagrado en el artículo 246 inc. 2 de la Constitución de El Salvador, que señala: *“la Constitución prevalecerá sobre todas las leyes y reglamentos”*, asimismo los artículos 144

¹³⁶ Constitución de la Republica de El Salvador (Asamblea Constituyente de El Salvador, Aprobada bajo Decreto Constituyente N° 38, en el D. O. N° 234, Tomo N° 281, del dieciséis de diciembre de 1983), Art. 246 inc 2, 144 y 145.

y 145 de la Constitución, señalan que los tratados internacionales celebrados por El Salvador con otros Estados o con organismos internacionales son leyes de la República al entrar en vigencia, pero cuando estos entren en conflicto con otras leyes prevalecerá el tratado, sin que perturbe, limite o afecte por ningún motivo las disposiciones instituidas en la constitución.

Bajo esa perspectiva la Intimidad como todo derecho esencial contiene seguridad constitucional, es así, que el artículo 2 inciso segundo de la Constitución establece que: “*se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*”¹³⁷, según constituye dicha norma, de igual manera se establece en el artículo 6 de la Constitución, el derecho a la libertad de expresión, siempre y cuando esta no lesione bienes jurídicos susceptibles como el orden público, la moral, el honor, ni la vida privada de los demás¹³⁸.

La Constitución tiene como objeto defender la intimidad de las personas físicas, a través de la defensa de sus diferentes manifestaciones como lo son la inviolabilidad de la morada, la inviolabilidad de la correspondencia y la no interferencia o intervención de las telecomunicaciones, el artículo 20 establece que “*La morada es inviolable y sólo podrá ingresarse a ella por consentimiento de la persona que la habita, por mandato judicial, por flagrante delito o peligro inminente de su perpetración, o por grave riesgo de las personas*” en relación al artículo 188 C.P. Allanamiento de Morada. Así

¹³⁷ El derecho a la intimidad personal supone reservar para si un determinado ambiente o sector, donde la intromisión de extraños perjudicaría la autonomía de la libertad para determinar su conducta. Cámara de lo Contencioso Administrativo, *Sentencia, Referencia 00036-18-ST-COPC-CAM* (El Salvador: Corte Suprema de Justicia, 2018).

¹³⁸ El derecho a la intimidad es un derecho fundamental en la vida de toda sociedad y uno de los derechos en los que se centra esta investigación, como todo derecho fundamental se puede evidenciar que tiene su fundamento en la Constitución de la Republica, la intimidad ha sido últimamente vulnerada debido a la gran cantidad de avances tecnológicos.

mismo el artículo 24 inc 1 establece la inviolabilidad de la correspondencia de toda clase, el inc 2 “*se prohíbe la interferencia y la intervención de las telecomunicaciones,*” salvo judicialmente, de forma escrita y motivada¹³⁹.

Se debe contar con herramientas legales que garanticen la protección de la información personal y datos personales de los habitantes, y a la vez ejercer con mayor claridad los mecanismos como el *habeas data*¹⁴⁰, por tales efectos la defensa de datos personales se encontrara dispersa en una serie de normativas que toman en cuenta factores como los siguientes: privacidad e intimidad personal en las tecnologías de la información y comunicaciones, aprobación en la transferencia de la información personal, regulación de datos personales en base de datos y centros de distribución, seguridad de la información personal.

3.2 Instrumentos Internacionales que regulan el derecho a la intimidad de las personas

3.2.1 Declaración Americana de los Derechos y Deberes del Hombre

Ratificada por El Salvador el 20 de junio del año de 1978¹⁴¹, este instrumento fue aprobado el 3 de Mayo de 1948, por la Organización de los Estados Americanos, fue el primer acuerdo internacional de derechos humanos, en el inciso primero de su considerando, explica que esta fue fundada teniendo en cuenta que los pueblos americanos han dignificado la persona humana y que sus constituciones nacionales reconocen que las instituciones jurídicas y

¹³⁹ Constitución de la Republica de El Salvador (Asamblea Constituyente de El Salvador, Aprobada bajo Decreto Constituyente N° 38, en el D. O. N° 234, Tomo N° 281, del dieciséis de diciembre de 1983), Art. 2, 6, 20, 24 inc 1 y 2.

¹⁴⁰ Enrique Cesar Pérez, Luño Robledo, *El procedimiento de habeas data*, (Madrid España: Dykinson, 2017), 98.

¹⁴¹ Adoptado en San José, Costa Rica, el 22 de noviembre de 1969, en la Conferencia Especializada Interamericana Sobre Derechos Humanos.

políticas, rectoras de la vida en sociedad, tienen como fin primordial la defensa de los derechos fundamentales del hombre y la creación de condiciones que le permitan desarrollarse espiritual, materialmente y alcanzar la felicidad.

En este tratado se regula una lista de derechos, entre ellos el derecho a la vida, la libertad, la seguridad e integridad de la persona, en cuanto al derecho a la intimidad en su artículo V constituye el derecho de protección a la honra, la reputación personal y vida privada familiar¹⁴², al manifestar que: *“toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honor, a su reputación, a su vida privada y familiar”*, en esta declaración, no se encuentra regulado ningún tipo de procedimiento en caso de interpretación o aplicación del instrumento, de modo que será la Organización de Estados Americanos su autoridad de aplicación en caso de controversia¹⁴³.

3.2.2 Declaración Universal de Derechos Humanos

La Asamblea General proclamo la presente Declaración Universal de Derechos Humanos¹⁴⁴ con el ideal de que todos los pueblos y naciones deben esforzarse, a fin de que los individuos y las instituciones, mediante la enseñanza y la educación, respeten a estos derechos y libertades, y

¹⁴² La relación que existe entre la Declaración Americana de los Derechos y Deberes del Hombre y el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos se encuentra en el artículo 5 de dicha declaración en el cual se busca proteger la vida privada de las personas y el derecho a la intimidad, mismas que se protegen en el artículo 26 al imponer una sanción que revelen datos o información de carácter personal.

¹⁴³ Leo Bladimir Benavides Salamanca, Marlon Ibán Hernández Anzora, Kenia Katy León Ardón, “La Penalización De Los Delitos Informáticos En El Salvador” (Tesis de licenciatura: Universidad de El Salvador, 2004).

¹⁴⁴ Adoptada y proclamada por la Asamblea General en su resolución 217 A, del 10 de diciembre de 1948.

aseguren los estados, por medidas progresivas de carácter nacional e internacional, su reconocimiento y aplicación universales y efectivos.

En ese sentido la autoridad de aplicación es la Organización de las Naciones Unidas y por tratarse de una Declaración no está sujeta a ratificación, pero surte efectos a partir del 10 de Diciembre de 1948, en su artículo 12 se encuentra plasmado el reconocimiento al derecho a la intimidad al manifestar lo siguiente: *“Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”*¹⁴⁵.

Así se protege el ámbito de la vida privada y familiar, por medio de la prohibición de las conductas públicas y privadas, que puedan invadirlo, es decir, que este derecho se traduce a estar solo, y no ser conocido por los demás mientras no lo autorice el titular¹⁴⁶, expresando además que la Ley tiene que resguardar contra injerencias o ataques de terceros, es decir, injerencias de extraños a la esfera de su vida individual y familiar, porque se le concede la potestad de excluir a otras personas el conocimiento de aspecto que reserva para sí o para quien el considere pertinente revelar.

La Declaración Universal de Derechos Humanos reconoce el derecho a la intimidad protege la vida privada y familiar de las personas prohibiendo las conductas públicas y privadas que puedan invadir dichas esferas, reconoce el derecho que tienen los individuos de excluir a ciertas personas de su vida

¹⁴⁵ Athina Vanessa García Mejía, Víctor Andrés González Guzmán, “El intrusismo informático y la utilización del Derecho Penal como mecanismo de tutela del derecho a la intimidad”. (Tesis de Licenciatura: Universidad de El Salvador, 2017).

¹⁴⁶ Xavier Pons Rafols, *La Declaración Universal de Derechos Humanos: Comentario artículo por artículo*, (España: Icaria, 1998), 302.

privada y la potestad que tienen los individuos de reservarse para sí o de revelar a ciertas personas su información personal.

3.2.3 Pacto Internacional de Derechos Civiles y Políticos

Este pacto fue ratificado por El Salvador el 23 de Noviembre de 1979¹⁴⁷, reconoce los derechos que se derivan de la dignidad inherente a la persona humana, de todos los miembros de la familia humana y de sus derechos iguales e inalienables, como la libertad, la justicia y la paz en el mundo, así, la Convención mencionada tiene como propósito hacer que reconozcan los estados suscriptores, de los derechos civiles y políticos de sus ciudadanos.

En su parte III, el artículo 17, reconoce en el numeral 1 que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio su correspondencia ni de ataques ilegales a su honra y reputación, reafirmando en el numeral 2 que toda persona tendrá derecho a la protección de la Ley contra esas injerencias o esos ataques, en el caso que se verificaran:

3.2.4 Convenio Internacional de Telecomunicaciones

Ratificado por El Salvador, el 22 de Julio de 1976, su principal objetivo es conservar y extender la cooperación internacional para el perfeccionamiento y el uso racional de toda clase de telecomunicaciones, y a su vez, beneficiar el desarrollo de los medios técnicos y su mayor eficacia a fin de ampliar el rendimiento de los servicios de telecomunicaciones, ampliar su empleo y propagar en lo posible su utilización para el público, el organismo

¹⁴⁷ D.L. N° 27, del 23 de noviembre de 1979, publicado en D.O. N° 218, tomo 265 del 23 de noviembre de 1979.

internacional de origen de este Convenio es la Unión Internacional de Telecomunicaciones¹⁴⁸ y por lo tanto la autoridad de aplicación, con sede es la ciudad de Ginebra.

Se puede establecer en su artículo 32 que se reconoce expresamente el secreto de las telecomunicaciones, con este se intenta resguardar las comunicaciones entre las personas, de cualquier interceptación ilegal de terceros, existiendo la excepción, para su afectación a esta dimensión del derecho a la intimidad¹⁴⁹, cuando la Ley lo disponga¹⁵⁰, este derecho no tiene carácter absoluto porque en el mismo artículo, se reservan el derecho a comunicar esta correspondencia a las autoridades competentes, con el fin de asegurar la aplicación de su legislación interior o la ejecución de los Convenios internacionales de los que son parte, es decir que no se exceptúan de la obligación para colaborar en alguna investigación penal.

3.2.5 Reglas de Brasilia Sobre Acceso a la Justicia de las Personas en Condición de Vulnerabilidad

Las reglas de Brasilia fueron elaboradas con el apoyo del Proyecto Eurosocial Justicia, por un grupo de trabajo constituido en el seno de la Cumbre Judicial Iberoamericana, en el que también han participado la Asociación Iberoamericana de Ministerios Públicos (AIAMP), la Asociación Interamericana de defensorías públicas (AIDEF), la Federación

¹⁴⁸ la Unión Internacional de Telecomunicaciones se basa en el principio de cooperación internacional público privada. [http:// www.exteriores .gob.es/ RepresentacionesPermanentes/ Oficinadelas Naciones Unidas/](http://www.exteriores.gob.es/RepresentacionesPermanentes/Oficinadelas Naciones Unidas/).

¹⁴⁹ En el convenio internacional de telecomunicaciones se reconoce expresamente el secreto en las telecomunicaciones en su artículo 32 a través del cual pretende resguardar las comunicaciones entre las personas protegiéndolas de cualquier interceptación ilegal de terceros, mismo que pretende resguardar el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos.

¹⁵⁰ Javier Díaz Revorio, "El derecho fundamental al secreto de las comunicaciones", Universidad de Castilla, La mancha, 2006, 32.

Iberoamericana de Ombudsman (FIO) y la Unión Iberoamericana de Colegios y Agrupaciones de Abogados (UIBA)¹⁵¹.

Las Reglas de Acceso a la Justicia de las Personas en Condición de Vulnerabilidad han sido aprobadas por El Salvador por la XIV Cumbre Judicial Iberoamericana, que ha tenido lugar en Brasilia durante los días 4 a 6 de marzo de 2008, la Cumbre Judicial Iberoamericana es ante todo una estructura de cooperación, concertación e intercambio de experiencias, que se articula a través de las máximas instancias de los poderes judiciales de la Región Iberoamericana¹⁵².

Las reglas de Brasilia tienen relación con el presente tema de investigación, ya que las mismas buscan garantizar el acceso efectivo a la justicia de las personas en condición de vulnerabilidad, en el capítulo I sección segunda numeral 8, establece que la discriminación que la mujer sufre en determinados ámbitos supone un obstáculo en el acceso a la justicia, y que se considera violencia contra la mujer cualquier acción o conducta, basada en su género, que cause daño o sufrimiento sexual o psicológico a la mujer, tanto en el ámbito público como en el privado, mediante el empleo de violencia física o psíquica.

Lo anteriormente se relaciona con el tema de estudio ya que al revelar, difundir o ceder en todo o en parte información, datos o material sexual explícito de las mujeres sin su consentimiento tal y como lo regula el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos, se está violentando a la mujer al causarle un daño psicológico.

¹⁵¹ *Reglas de Brasilia Sobre Acceso a la Justicia de las Personas en Condición de Vulnerabilidad*. <https://acnur.org>.

¹⁵² <https://www.cumbrejudicial.org>

3.3 Normativa secundaria que regula el derecho a la intimidad de las personas y su relación con el tema de investigación

3.3.1 Código Penal de El Salvador

El Código Penal¹⁵³, fue creado el 26 de abril de 1997, regula los tipos de delitos, faltas y sus penas, así, el Derecho Penal, se emplea y responde al principio de mínima intervención, que establece que solo debe intervenir en aquellos hechos más graves que infringen los bienes jurídicos más significativos de la sociedad, dejando para otras ramas del derecho, las infracciones que no le interesa proteger.

En cuanto al derecho a la intimidad su defensa se encuentra, en su título VI denominado delitos relativos al honor y la intimidad¹⁵⁴, se establece en su capítulo II los delitos relativos a la intimidad, de los cuales se dispone de una lista de delitos, que afectan el derecho a la intimidad, entre ellos se observa, el delito de violación de comunicaciones privadas regulado en el artículo 184 inc 1, establece lo siguiente: *“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”*¹⁵⁵.

¹⁵³ Código Penal (Aprobado por Decreto Legislativo N° 1030, D.O. N° 105, Tomo N° 335, del 10 de junio de 1997).

¹⁵⁴ Se puede observar que el derecho a la intimidad es tan importante que se encuentra regulado tanto en la Constitución de la Republica como en el Código Penal, realizando un capitulo para regular exclusivamente los delitos relativos a la misma.

¹⁵⁵ El artículo 184 inc. 1 habla de datos reservados ya sean de carácter familiar o personal, es decir hay datos que como se estableció en el capítulo anterior no son datos de carácter reservado y esos no son con los que se constituye el delito en cuestión.

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 multa¹⁵⁶.

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 multa¹⁵⁷

La conducta queda consumada, en el inciso primero, cuando el sujeto activo, realiza el comportamiento con alguna de las finalidades citadas en el artículo, al final del inciso primero se establece la sanción de cincuenta a cien días multas, así mismo se impone al que difundiere o revelare a tercero los datos reservados, la sanción de cien a doscientos días multa, el inciso tercero establece como sanción la pena de multa de treinta a cincuenta días multa a quien se revelare el secreto y lo divulgare, siempre que tenga conocimiento que es producto de una acción constitutiva de delito¹⁵⁸.

El artículo 185 del mismo cuerpo normativo regula el delito de la violación agravada de comunicaciones, que establece: *“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”*.

¹⁵⁶ En el segundo inciso se puede observar como la sanción asciende ya hasta doscientos días multas no solo por apropiarse de la información o datos reservados sino por difundirlos a otras personas.

¹⁵⁷ En este tercer inciso se puede evidenciar como la sanción ya no va dirigida solo a la persona que se apodere de la información o datos reservados y los difunda sino también para la persona o personas que a sabiendas que esos datos fueron obtenidos de manera ilegal los divulgue o revele.

¹⁵⁸ Oscar Carlos Ernesto Aguirre Linares, Jorge Antonio Sevillano Flores, “Desafíos a enfrentar en la aplicación de leyes sobre delitos informáticos en El Salvador” (Tesis de maestría: Universidad Don Bosco de El Salvador, 2015).

Esté tipo penal es una agravante de los hechos descritos en el art 184, en cuanto a la calidad del sujeto activo, siempre que ejecuten las conductas definidas en el artículo 184 y tengan la calidad de sujetos encargados o responsables, además que el secreto este en un fichero¹⁵⁹, soporte informático, se refiere a información secreta o con carácter personal no así a información que sea de carácter público.

El artículo 186 se regula el delito de captación de comunicaciones, de la siguiente forma: *“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”¹⁶⁰.

¹⁵⁹ Es un conjunto de información (fichas o registros) que se refieren a una misma cosa. Carlos de la Puente Viedma, *SPSS/PC+ una guía para la investigación*, (Madrid: Complutense, 2009), 402.

¹⁶⁰ En el segundo inciso del artículo 186 se establece una condición para que la acción sea constitutiva de delito y es que la persona a quien se le revele la información que fue obtenida de forma ilícita la divulgue a sabiendas de la ilicitud de su origen, es decir que si este tercero no divulga dicha información no comete delito alguno.

Al igual que el delito anterior, el bien jurídico protegido por el tipo penal, es la intimidad de las personas, la acción típica se ejecuta al interceptar, impedir o interrumpir una comunicación telegráfica o telefónica o la utilización de medios o artificios tecnológicos de escucha, transmisión o grabación del sonido, de la imagen o de cualquier otra señal de comunicación, es decir que encierra los innovadores avances tecnológicos en comunicación, como el fax, el internet, lo que implica intrusismo informático, también denominado *hacking*¹⁶¹, es decir el acceso sin permiso, a los archivos y bases de datos comprendidos en los sistemas informáticos ajenos, aunque por lo general de grandes empresas o instituciones, al acceder sin permiso a la información que se supone secreta, estando en presencia de intrusismo informático, aunque el tipo penal no lo regula claramente¹⁶².

En la redacción del tipo penal el legislador advirtió el fenómeno de internet y las innovadoras formas de correspondencia y comunicación que existen, al establecer en la descripción “(...) *cualquier otra señal de comunicación.*” y cuando se expresa “(...) *utilizare instrumentos o artificios técnicos.*” Para ejecutar cualquiera de los verbos rectores del tipo penal se puede deducir que el sujeto que quiera obtener dicha información forzosamente tiene que tener conocimientos y herramientas de hacking para ejecutar este tipo de delitos, sin embargo no se necesita una aptitud especial para ejecutar la acción descrita, la infracción queda consumada desde el momento en el que el secreto llega a la persona destinada del sujeto activo y esta lo difunde sin el consentimiento del titular.

¹⁶¹ Hacking es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo. <https://www.duiops.net/hacking/hacking-cracking.htm>

¹⁶² Athina Vanessa García Mejía, Víctor Andrés González Guzmán, “El intrusismo informático y la utilización del Derecho Penal como mecanismo de tutela del derecho a la intimidad”. (Tesis de Licenciatura: Universidad de El Salvador, 2017).

Asimismo establece la sanción de prisión de seis meses a un año y multa de cincuenta a cien días multa, el segundo inciso regula un tipo agravado por difundir o revelar a terceros los datos reservados que hubieren sido descubiertos, para el caso la sanción es de prisión de seis meses a un año y multa de cien a ciento cincuenta días multa¹⁶³.

El inciso tercero del artículo 186, regula con sanción de multa de treinta a cincuenta días, para la divulgación del secreto, por parte de un sujeto diferente al que ejecuto el tipo básico¹⁶⁴, sabiendo del origen ilícito de la información y el inciso final regula la pena de dos a seis años de prisión, al que realice los actos señalados en el primer inciso con la intención de preparar la ejecución de un delito grave, entiéndase por tal los delitos sancionados con pena de prisión cuyo límite máximo exceda de tres años y multa cuyo límite máximo exceda de doscientos días multa, según dispone el artículo 18 del Código Penal.

Además, hay que recalcar que el sujeto activo del delito tiene como propósito, violar la intimidad de otro, ejecutando cualquiera de los verbos rectores mencionados con anterioridad, se entiende por intimidad aquella parte de la vida privada de la persona, que no debe de divulgarse aún tercero, sin el consentimiento expreso del titular,¹⁶⁵ es ahí donde está la clave para que dicha acción constituya o no un delito, en el consentimiento.

¹⁶³ El Estado tiene la obligación y trata de proteger el derecho a la intimidad de las personas regulando este tipo de delitos y no solo regulándolos sino estableciendo una sanción para así evitar el cometimiento de estos hechos delictivos.

¹⁶⁴ Entendiendo que la persona que ejecuta el tipo básico de este delito es quien obtiene la información privada de manera ilícita, por tanto este inciso tercero se refiere a que la información la divulga un sujeto diferente al que la sustrajo.

¹⁶⁵ Si la persona que divulgue la información lo hace con el consentimiento y permiso del titular de esta no incurre en delito alguno, ya que las personas son dueñas de su propia información y pueden disponer hacer con la misma lo que mejor les parezca.

El artículo 190 se refiere al delito de Utilización de la imagen o nombre de otro, por lo que establece: *“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 multas de treinta a cien días multa”*¹⁶⁶, este artículo tiene relación al tema de investigación debido a que la imagen de una persona y sus datos personales deben de ser protegidos y no ser utilizados ni revelados por los medios tecnológicos sin el consentimiento del titular de la información.

Los delitos relativos a la intimidad, definidos en el código penal eran sancionados y regulados por este código cuando no se constaba en el país, una ley especial a la que más adelante se relacionará y se estudiará el delito objeto de la investigación.

3.3.2 Ley de Reparación por Daño Moral

La Ley de Reparación por Daño Moral¹⁶⁷ se relaciona con el inciso tercero del artículo dos de la Constitución en el que *“se establece la indemnización conforme a la Ley, por daños de carácter moral”* y con el derecho al honor, a la intimidad personal y familiar así como también a la propia imagen.

El artículo 3 de la Ley de Reparación por Daño Moral establece las causales para la reparación del daño moral, para efectos de la investigación solo se estudiarán las causales de los literales a y b que establecen respectivamente que cualquier acción u omisión ilícita, intencional o culposa, en los ámbitos civil, mercantil, administrativo, penal o de otra índole que afecte los derechos

¹⁶⁶ Código Penal (Aprobado por Decreto Legislativo N° 1030, D.O. N° 105, Tomo N° 335, del 10 de junio de 1997), Art. 184, 185, 186, 190

¹⁶⁷ Ley de Reparación por Daño Moral (Aprobada por Decreto Legislativo N° 216, D. O. N° 5, Tomo N° 410, del 08 de enero de 2016).

humanos o los derechos de la personalidad de la víctima, o cualquier exceso de los límites de la buena fe en el ejercicio de un derecho legítimo que cause un daño a otro, da lugar a solicitar la reparación del daño moral.

Ambas causales podrán configurarse al tipo penal regulado en el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos, al revelarse, difundirse o cederse en todo o en parte información, datos, imágenes, videos, audio, material sexual explícito u otros, sin el consentimiento del titular de la información¹⁶⁸.

El artículo 9 de la Ley de Reparación de Daño Moral establece que el procedimiento para reclamar la indemnización se tramitara siguiendo el proceso declarativo común que establece el Código Procesal Civil y Mercantil¹⁶⁹, es decir se deberá presentar la demanda que deberá contener según el artículo 10 de dicha Ley la estimación pecuaria de la indemnización por daño moral y la propuesta de medidas de reparación que se considere pertinente, demanda que deberá presentarse en el domicilio del demandado, una vez admitida la demanda se emplaza al demandado para que conteste, posteriormente el juzgado respectivo programara audiencia preparatoria y probatoria, finalmente el Juez respectivo dictara la sentencia respectiva.

El monto de la indemnización económica por daño moral deberá fijarse según el artículo 14 de la Ley de Reparación del Daño Moral atendiendo a criterios de equidad y razonabilidad y tomando en cuenta las condiciones personales del afectado y del responsable, así como las circunstancias del caso y especialmente la gravedad del hecho y la culpa.

¹⁶⁸ El titular de la información es la persona, en este caso la mujer que es la titular de la información que se ha revelado.

¹⁶⁹ Código Procesal Civil y Mercantil (Decreto Legislativo N° 712, D. O. N° 224, Tomo N° 381, del 27 de noviembre de 2008), Libro Segundo, Título Primero, Capítulo Primero.

Cuando se ordene la indemnización económica, según el artículo 17 de la Ley de Reparación del Daño Moral deberá pagarse en moneda de curso legal, de manera excepcional las partes podrán convenir que el monto de la indemnización sea pagado en especies de valor equivalente.

3.3.3 Ley de Protección al Consumidor

La Ley de protección al consumidor¹⁷⁰ es la normativa que limita a las empresas de poder compartir información personal y crediticia del consumidor, ya sea entre proveedores o a través de entidades especializadas en la prestación de servicios de información, sin la debida autorización.

El objeto de esta Ley es proteger los derechos de los consumidores a fin de procurar el equilibrio, certeza y seguridad jurídica en sus relaciones con los proveedores, así mismo tiene por objeto establecer el Sistema Nacional de Protección al Consumidor y la Defensoría del Consumidor como institución encargada de promover y desarrollar la protección de los consumidores, disponiendo su organización, competencia y sus relaciones con los órganos e instituciones del Estado y los particulares.

El artículo 18, literal g) determina que una de las prohibiciones de los proveedores¹⁷¹ es compartir información personal y crediticia del consumidor, ya sea entre proveedores o a través de entidades especializadas en la

¹⁷⁰ Ley de Protección al Consumidor (Decreto Legislativo N° 776, Diario Oficial N° 166, Tomo N° 368, de fecha 08 de septiembre de 2005).

¹⁷¹ Toda persona natural o jurídica, de carácter público o privado que desarrolle actividades de producción, fabricación, importación, suministro, construcción, distribución, alquiler, facilitación, comercialización o contratación de bienes, transformación, almacenamiento, transporte, así como de prestación de servicios a consumidores, mediante el pago de precio, tasa o tarifa. Ley de Protección al Consumidor, artículo 3, literal b.

prestación de servicios de información, sin la debida autorización del consumidor, es en esta disposición que se encuentra la relación con el tema de investigación, pues se refiere a compartir información personal sin la autorización del consumidor, acción que también se regula en el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos.

3.3.4 Ley Especial Integral Para Una Vida Libre de Violencia Para las Mujeres

El objeto de la ley¹⁷² se encuentra descrito en el artículo 1 en el que establece que 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, con el fin de proteger los derechos de las mujeres.

El artículo 8 literal g) de la Ley Especial Integral Para Una Vida Libre de Violencia Para las Mujeres, establece que la 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, tomando en cuenta que la violencia contra la mujer es como la define el mismo artículo en su literal k, 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, lamentablemente en la actualidad la realización de este tipo de acciones se ha normalizado y es cada vez más común la violación a este tipo penal.

¹⁷² Ley Especial Integral Para Una Vida Libre de Violencia Para las Mujeres (Decreto Legislativo N°520, publicado en el Diario Oficial N°2, Tomo 390, de fecha 4 de enero de 2011).

El artículo 9 literal g) de la Ley Especial Integral Para Una Vida Libre de Violencia Para las Mujeres establece la violencia simbólica como un tipo de violencia hacia la mujer, que se refiere a los 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 sociedad¹⁷³.

También existe relación en los artículos 49, 50, 51 de la Ley Especial Integral Para Una Vida Libre de Violencia Para las Mujeres ya que en los mismos se establecen que “quien publicare, distribuyere, enviare, promoviere, facilitare, administrare, financiare u organizare la utilización de mujeres, sin su consentimiento en actos sexuales o eróticos, utilizando medios informáticos o electrónicos será sancionada con prisión de cinco a diez años, así como la difusión ilegal de información personal de la mujer, y la difusión de pornografía, quien publicare, compartiere, enviare o distribuyere material pornográfico por cualquier medio informático o electrónico¹⁷⁴ en el que se utilice la imagen o identidad de la mujer sin su consentimiento, será sancionado con pena de tres a cinco años¹⁷⁵.

El artículo 55 literal a) establece que es expresión de violencia contra la mujer elaborar, publicar, difundir o transmitir por cualquier medio, imágenes o

¹⁷³ Esto se relaciona con el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos, en la revelación, difusión o cesión de todo en parte de los mensajes, valores iconos signos que transmiten y reproducen relaciones de dominación desigualdad y discriminación en las relaciones sociales.

¹⁷⁴ El artículo 25 de la Ley Especial Contra los Delitos Informáticos y Conexos establece en relación con esto que el que deliberadamente obtenga y transfiera información de carácter confidencial apoyándose en cualquier clase de las tecnologías de la comunicación y la información, será sancionado con prisión de cinco a ocho años.

¹⁷⁵ La relación de los artículos y los tipos de delitos expresados contra las mujeres, se encuentra el inciso segundo del artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos se establece que si se difunde material sexual explícito en perjuicio de un tercero sin su consentimiento se sancionara con prisión de cuatro a ocho años.

mensajes visuales, audiovisuales, multimedia o plataformas informáticas con contenido de odio o menosprecio hacia las mujeres, se puede observar la relación con el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos al referirse al verbo rector difundir imágenes, lo cual el inciso primero de dicho artículo lo sanciona con prisión de tres a cinco años.

3.3.5 Ley de Acceso a la Información pública

El objeto de la ley¹⁷⁶ se encuentra en el artículo 1, el cual es el garantizar el derecho de acceso de toda persona a la información pública, a fin de contribuir con la transparencia de las actuaciones de las instituciones del Estado, y en el trato a la protección de los datos personales en posesión de los entes obligados, así como garantizar su exactitud.

La relación de la esta ley con la ley especial contra los delitos informáticos y conexos es la protección de los datos personales privados y los datos personales sensibles los cuales están definidos en el Art. 6 Lit. a y b, los definidos en ambas leyes y relacionados en el tipo de delito investigado.

3.3.6 Ley Especial Contra los Delitos Informáticos y Conexos

El objeto de la ley¹⁷⁷ se encuentra en el artículo 1 y es 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 los cometidos mediante el uso de las tecnologías que afecten intereses

¹⁷⁶ Ley de acceso a la información pública (Aprobada por Decreto Legislativo N° 534, D. O. N° 70, Tomo N° 391, 08 de abril de 2011), Art. 1, 3 h. y Art 6 a y b

¹⁷⁷ Ley Especial Contra los Delitos Informáticos y Conexos (Aprobada por Decreto Legislativo N° 260, D. O. N° 40, Tomo N° 410, 26 de febrero de 2016).

asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas, aunque este tipo de delitos es más frecuentemente cometido en contra de personas naturales .

La ley establece en su capítulo III, los delitos informáticos relacionados con el contenido de los datos personales, teniendo relación con el delito y tema de investigación, los cuales se encuentran regulados en los artículos: artículo 20 referente a la interferencia de datos, artículo 22 del Hurto de identidad, artículo 24 en relación a la utilización de datos personales, y el artículo 26, de la Revelación indebida de datos o información de carácter personal.

El tipo penal regulado en el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos, que es precisamente la disposición que es objeto de estudio de esta investigación, dispone lo siguiente:

Art. 26.- El que sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean éstos en imágenes, video, texto, audio u otros, 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, la comisión de otro delito o se difunda material sexual explícito en perjuicio de un tercero, será sancionado con prisión de cuatro a ocho años¹⁷⁸.

¹⁷⁸ El artículo 26 se refiere específicamente a la acción de difundir la información de carácter privado y personal, la cual anteriormente se explica que información se considera entre estas clasificaciones

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 confidenciales o sensibles definidos en la Ley de Acceso a la Información Pública”¹⁷⁹.

3.4 Elementos del tipo penal del Artículo 26

3.4.1 Bien jurídico

El legislador salvadoreño colocó este tipo penal en el capítulo que ha designado delitos Informáticos relacionados con el contenido de los datos, y es de los tipos penales de la Ley Especial Contra los Delitos Informáticos y Conexos, que menciona en su redacción al contenido de la información (los datos informáticos) como objeto de protección, por lo que se puede señalar que el bien jurídico tutelado en consecuencia, concuerda con lo que se ha asegurado en el artículo 4 de la Ley Especial Contra los Delitos Informáticos y Conexos, en el sentido que se puede iniciar a sostener que se está en presencia de un valor social que requiere la defensa del derecho y en especial del Derecho Penal, que se ha categorizado como la integridad de los sistemas y datos informáticos¹⁸⁰.

Es el contenido de la información de los datos informáticos, sistemas informáticos, información de carácter personal y la información que garantice y proteja el ejercicio de derechos fundamentales como la intimidad, honor,

¹⁷⁹ La definición de lo que son y en lo que consisten los datos sensibles a los que se refiere este artículo se abordan más adelante en este capítulo.

¹⁸⁰ Jorge Alberto Elías Cornejo, Javier Alexander Hernández Hernández, Arnoldo Ernesto Sánchez Gamero, “Desarrollo de un kit de seguridad informática enfocada para la protección de la información computacional tanto en hardware como en software para la Universidad Tecnológica de El Salvador” (Tesis para obtener el grado de técnico: Universidad Tecnológica de El Salvador, 2016).

integridad sexual, e imagen¹⁸¹, no obstante, a lo anterior, se sanciona la difusión o cesión de información de carácter privada y personal es posible vincularlo con el derecho a la intimidad, materializado en el contenido de los datos informáticos, por lo que se puede hablar de un tipo penal pluriofensivo¹⁸².

3.4.2 Elementos objetivos

Sujeto activo

En virtud de la formulación utilizada por el legislador en el artículo 26 inc 1, consistente en *“El que sin el consentimiento del titular de la información de carácter privado y personal”*, se puede concluir que se trata de un delito común, en el cual el sujeto activo no debe contar con ninguna cualidad o calidad especial, por lo que puede ser ejecutado por cualquier persona natural¹⁸³, siempre y cuando pueda saber utilizar, manipular, y tener un conocimiento básico sobre las nuevas tecnologías, poseer un aparato digital, con acceso a internet o redes sociales para poder realizar el cometimiento del delito.

Sujeto pasivo

¹⁸¹ Ley Especial Contra los Delitos Informáticos y Conexos (Aprobada por Decreto Legislativo N° 260, D. O. N° 40, Tomo N° 410, 26 de febrero de 2016), Art. 3 lit b

¹⁸² Los delitos pluriofensivos hacen referencia a la afectación de más de un bien jurídico por un delito de naturaleza unitaria, es toda infracción en que pueda verse afectado más de un objeto de tutela. Javier Guardiola García, *La realización arbitraria del propio derecho*, (Universidad de Valencia, 2003).

¹⁸³ Al tratarse de un delito que no requiere mayores habilidades, cualidades o aptitudes más que tener conocimientos básicos de las tecnologías e instrumentos tecnológicos por parte de los sujetos o sujeto que lo cometa, este se vuelve más difícil y complejo la investigación de este tipo de delitos y con esto el establecimiento de responsabilidades debido q cualquier persona los puede cometer.

Puede ser sujeto pasivo cualquier persona natural o jurídica titular de la información de carácter privada y personal

Conducta típica

La parte objetiva de la conducta típica comprende el que *“sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean éstos en imágenes, video, texto, audio u otros, obtenidos por alguno de los medios indicados en los artículos precedentes”*¹⁸⁴.

Los verbos rectores del tipo penal están conformados por revelar, difundir o ceder en todo o en parte, lo que indica que son conductas alternativas, es decir que no se deben cometer todas para consumar el delito, sino que basta con la ejecución de una de ellas¹⁸⁵, revelar, como ya se ha señalado es revelar o manifestar lo ignorado o secreto; por su parte difundir, es propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas, etc.; y ceder, es dar, transferir o traspasar a alguien una cosa, acción o derecho.

Todas las acciones recaen sobre la información de carácter privado y personal, al respecto, la Ley Especial Contra los Delitos Informáticos y Conexos, tiene una definición de tales conceptos , sin embargo, cuando se

¹⁸⁴ Para que el delito regulado en el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos se tipifique debe cumplir con las acciones requeridas en los verbos rectores ósea debe revelar, difundir o ceder en todo o en parte la información de carácter privado y personal de una persona sin la autorización de la misma.

¹⁸⁵ Aunque los verbos rectores del artículo en cuestión establece tres acciones: revelar, difundir o ceder, no es necesario que se cometan las tres acciones para que se tipifique el delito en cuestión, basta con que se realice una de estas para que dicho delito sea sancionado.

define en el artículo 3 lit m y n de los datos personales y datos personales sensibles¹⁸⁶, hace colecta de información privada y de que esta se refiere a información de las personas, de tal manera que se puede considerar que se trata de términos que en conjunto han sido utilizado como sinónimos, pero a la misma vez se está hablando de datos diferentes de las personas.

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”¹⁸⁷.

Sobre el contenido de la información, el tipo penal además determina los medios sobre los cuales esta se puede haber soportado, al señalar “*sean éstos en imágenes, video, texto, audio u otros*”, vocablos que se explican por sí mismos, salvo la cláusula de apertura “*u otros*”, que admitiría incluir algún otro medio de soporte, haciendo uso de los medios tecnológicos¹⁸⁸.

¹⁸⁶ Ley Especial Contra los Delitos Informáticos y Conexos (Aprobada por Decreto Legislativo N° 260, D. O. N° 40, Tomo N° 410, 26 de febrero de 2016), Art. 3 lit. m, n.

¹⁸⁷ En esta clasificación de datos personales el legislador hace una definición más detallada y profunda en la cual ya se denominan datos personales sensibles, entre los cuales se encuentran datos más privados, más íntimos, más sensibles como el legislador los denomino.

¹⁸⁸ Al tratarse de una Ley que regula delitos de naturaleza informática, podría inferirse que eso “u otros” medios a los que se refiere el artículo tendrían que ser medios o aparatos por los que se haya hecho uso de la red.

El tipo señala además que se trata de la revelación, difusión o cesión de información sin el consentimiento del titular, de tal modo que contar con la aprobación de este, produce la atipicidad de la conducta.

Finalmente, el tipo hace alusión a que la información objeto de la revelación, difusión o cesión, debe haber sido factible para el sujeto activo por alguno de los medios indicados en los artículos precedentes, pero que abre la posibilidad de discutir si en esos casos se está en presencia de un concurso aparente de leyes o alguna de las figuras concursales que regula el Código Penal; sin embargo, también cabe señalar, que comete delito tanto el que accede a la información personal y sensible por alguno de los medios señalados en los artículos precedentes y luego la difunde aquí es donde se puede determinar la clase de concurso, pero también, quien sin intervenir en los otros delitos, accede a la información y sin consentimiento del titular la revela, difunde o cede.

Por ejemplo en el caso que “A”, ejecutando acciones de vulneración de medidas de seguridad concretas de un sistema, programa o datos informáticos, accede a información personal y sensible de “B”, y luego, por un costo que desde el inicio fue su objetivo: ánimo de lucro, se la concede a “C”, quien es quien la revela en una cuenta de redes sociales anónima, la conducta de “A”, podría ser calificada como obtención y transferencia de información de carácter confidencial, sancionada en el artículo 25 de la Ley Especial Contra los Delitos Informáticos y Conexos¹⁸⁹, mientras que la

¹⁸⁹ En los artículos 25 y el artículo 26 ambos de la Ley Especial Contra los Delitos Informáticos y Conexos, el primer artículo sanciona la obtención y transferencia deliberada de información de carácter confidencial obtenida mediante la vulneración de sistemas informáticos mientras que el segundo artículo lo que sanciona es la revelación o difusión en todo o en parte de información de carácter personal y privada sin la autorización del titular.

ejecutada por “C”, que no intervino en la conducta original, se puede calificar conforme al artículo que se comenta¹⁹⁰.

Consumación y tentativa

Por los elementos objetivos del tipo penal, señalados anteriormente, y esencialmente por los verbos rectores se considera que se trata de un delito de mera actividad¹⁹¹, pues solo señala una mera acción, sin resultado separable transitoriamente de la conducta, de tal manera que el delito se consuma con la mera difusión, revelación o cesión de la información.

Es un delito de mera actividad, pues solo señala una acción, sin resultado separable de la conducta, de tal manera que el delito se consuma con la mera revelación, difusión o cesión de la información sin el consentimiento de la persona titular de la información personal.

Conducta agravada

En los incisos segundo y tercero del artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos, se consideran agravadas, es decir que estas acciones se consideran que causan un daño más grave a la víctima y por consiguiente deben tener una pena mayor respecto al inciso primero, las conductas realizadas por el autor, de la siguiente forma:

¹⁹⁰ Fiscalía General de la Republica de El Salvador, escuela de capacitación fiscal, equipo del programa global del ciberdelito, “Análisis jurídico de los delitos contenidos en los capítulos I, II, III, y V del título segundo de la Ley Especial Contra Los Delitos Informáticos y Conexos”, 2018.

¹⁹¹ Los delitos de mera actividad son aquellos en los cuales solo se exige la conducta del autor para la realización del tipo, sin necesidad de un hecho (suceso) distinto a la misma. Juan Luis Modellel González, *Temas Penales*, (Caracas: Universidad Católica Andrés Bello, 2006).

Si alguna de las conductas descritas en el inciso anterior, se hubiese realizado con ánimo de lucro, la comisión de otro delito o se difunda material sexual explícito en perjuicio de un tercero, será sancionado con prisión de cuatro a ocho años¹⁹².

En el caso del inciso segundo, si el sujeto activo actúo con ánimo de lucro, es decir de conseguir un beneficio patrimonial, si lo hizo con la intención de cometer otro delito, que puede estar sancionado en la misma Ley Especial Contra los Delitos Informáticos y Conexos, u otras leyes; y si se refiere a material sexual explícito en perjuicio de un tercero, en este último caso hay que evaluar las relaciones concursales que puedan existir, en el caso que la persona afectada sea mujer¹⁹³, pues en los artículos 50 y 51 de la Ley Especial Integral Para Una Vida Libre de Violencia Para Las Mujeres, se sancionan conductas de la misma naturaleza, las que ya se relacionaron anteriormente.

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 confidenciales o sensibles definidos en la Ley de Acceso a la Información Pública”.

En relación al inciso tercero del artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos, la agravante se refiere a sí la información revelada tienen que ver con los datos personales de carácter confidencial o

¹⁹² Si la información de carácter privado y personal que se difunde, revela o ceda sin el consentimiento del titular de dicha información es de carácter explícitamente sexual o es utilizada para percibir un beneficio económico, la pena de prisión asciende hasta ocho años.

¹⁹³ Este último caso es el que interesa en esta investigación cuando la víctima del delito regulado en el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos es una mujer.

sensible, los cuales se encuentran definidos en la Ley de Acceso a la Información Pública en el artículo 6 literal b).

3.4.3 Elementos subjetivos

Dolo

El elemento subjetivo se determina en el dolo, es decir en el conocimiento y la voluntad de realizar el tipo¹⁹⁴, consentimiento, conocimiento, intención y voluntad de realizar la conducta típica, tener la voluntad e intención de realizar el hecho delictivo, el delito de revelación indebida de datos o información de carácter personal.

El ánimo de lucro

Como pudo observarse, en el inciso segundo se contempla una agravante en virtud de este ánimo especial, entendido como la pretensión del sujeto activo en el sentido de lograr como consecuencia de su acción un beneficio patrimonial¹⁹⁵.

3.5 Noticia sobre revelación indebida de datos o información de carácter personal

En el país existe un caso muy actual y que aún está en vías de investigación que se adecua al tercer inciso del artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos, y es la sospecha de una filtración de datos

¹⁹⁴ En el Derecho Penal la voluntad o intención de provocar un daño en el bien jurídico protegido es importante al momento de tipificar la acción, y para establecer la pena.

¹⁹⁵ *Ibíd.* P.24.

de ciudadanos Salvadoreños¹⁹⁶ por parte del presidente del Instituto de Acceso a la Información Pública, supuestamente entregados a casa presidencial, información que se publicó el pasado 08 de noviembre de 2019.

Se expresa que el Instituto de Acceso a la Información Pública suspendió el envío de información confidencial, pero autorizó a petición de la presidencia el envío de informes estadísticos diarios sobre las solicitudes de información pública, la cual fue autorizada por el entonces presidente del Instituto de Acceso a la Información Pública René Cárcamo, quien presentó su renuncia el pasado 15 de noviembre de 2019, en respuesta a estas publicaciones el Instituto de Acceso a la Información Pública emitió un comunicado en el que negaba haber compartido información confidencial de Ciudadanos con la presidencia y cinco días después de ese comunicado es decir el 13 de noviembre de 2019 la revista Factum publicó una serie de audios en una sesión de pleno del Instituto celebrada el pasado 23 de septiembre de 2019.

El señor Cárcamo aceptó que la institución llamada a ser el árbitro del acceso a la información, envió datos confidenciales a un ente obligado en este caso a la presidencia, tras suspender el envío de información confidencial la Unidad de Tecnología del instituto acató la orden Cárcamo y mandó nuevos informes durante un mes desde el 19 de agosto hasta el 19 de septiembre de 2019 estos informes contenían cinco campos: el número de referencia, tipo de solicitud, fecha de ingreso, estado y fecha de vencimiento, sin embargo posterior a estos envíos la presidencia solicitó que se agregara una columna más a los informes Carpres¹⁹⁷.

¹⁹⁶ La información personal de los ciudadanos que solicitaron información a cualquiera de las 285 instituciones públicas entre el 01 y el 15 de junio del 2019, fecha de la cual estaba recién entrado el gobierno de Nayib Bukele.

¹⁹⁷ Bryan Avelar, "Presidente del IAIP renuncia tras filtración de datos de Ciudadanos a la presidencia," revista Factum, 15 de noviembre de 2019. <http://www.revistafactum.com>.

3.6 Proyecto de Ley de Protección de Datos Personales

Se establece que existen proyectos de ley de protección de datos en El Salvador, los diputados de la fracción del partido ARENA presentaron el lunes 24 de junio de 2019 a la Asamblea Legislativa un proyecto de Ley que busca garantizar la protección de los datos personales de los ciudadanos que hayan sido proporcionados a organismos públicos y privados del país¹⁹⁸, la propuesta de Ley de Protección de Datos Personales establece que los ciudadanos son dueños de la información contenida en las unidades de almacenamiento de estas organizaciones.

El proyecto fue realizado con ayuda de la Cámara Americana de Comercio (Amcham) y la empresa Microsoft, la propuesta establece que la información de las bases de datos debe aprobarse bajo el consentimiento específico, informado y expreso de la persona¹⁹⁹, de igual manera, manifiesta que los datos de la ciudadanía no pueden ser utilizados para fines comerciales como proporcionar productos o con fines lucrativos, sin haberse obtenido antes el permiso requerido.

Según las disposiciones de este proyecto, los responsables de las bases de datos²⁰⁰ deben adoptar las medidas de seguridad, integridad y confidencialidad de los datos para evitar su adulteración, pérdida o uso no autorizado. Además, los encargados serán responsables de notificar a los

¹⁹⁸ Ricardo Posada, "Presentan proyecto de Ley que busca proteger datos personales," Diario El Mundo, 25 de junio de 2019, sección política.

¹⁹⁹ Otro aspecto que está contemplado dentro de la propuesta es que toda persona natural tendrá derecho a solicitar toda la información sobre si misma que haya sido recabada.

²⁰⁰ Se está discutiendo en la Asamblea Legislativa quien será la institución responsable de manejar y salvaguardar estos datos de las personas, existen tres propuestas una de ellas es que lo maneje el Instituto de Acceso a la Información Pública, otra propuesta es que lo maneje la Defensoría del Consumidor o que se cree un institución especializada en el manejo de datos personales.

ciudadanos cuando estos datos se vulneren o se manifiesten violaciones contra lo establecido en la legislación, esto traería beneficios comerciales, pues la Unión Europea ha creado la Ley General de Datos, la cual insta a los estados miembros a priorizar inversiones en los países que tienen vigentes mecanismos de protección de datos.

Julio Martínez, representante de Microsoft para la región centroamericana, aseguro que si la Ley se aprueba en los próximos meses, El Salvador sería el primer país en Centroamérica en contar con ella, dado que, aunque Panamá tiene una legislación similar, aun no se encuentra vigente²⁰¹, el resguardo de datos como el historial médico, el record crediticio, la religión que profesa una persona, entre otro tipo de información personal sensible es el objeto de una nueva normativa que inicio a estudiar la Comisión de Economía de la Asamblea Legislativa²⁰².

3.7 Análisis de sentencias

3.7.1 Análisis de sentencia nacional sobre el delito de revelación indebida de datos o información de carácter personal, regulado en el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos

Sentencia con número de referencia INC – 259 – 17, emitida por la cámara tercera de lo penal de la primera sección del centro, a las quince horas con cincuenta y cinco minutos del trece de octubre de dos mil diecisiete,²⁰³ en la cual la víctima es una mujer, por ser pertinente para esta investigación.

²⁰¹ Laura Flores, Gabriel Campos Madrid, “Proponen una Ley de datos y habeas data,” La Prensa Gráfica, 25 de junio de 2019, sección política.

²⁰² Enrique Miranda, “Asamblea inicia estudio de Ley para proteger datos personales,” El Diario de Hoy, 06 de noviembre de 2019, sección política.

²⁰³ Cámara Tercera de lo Penal de la Primera Sección del Centro, *recurso de apelación*, referencia: INC-259-17 (El Salvador: Corte Suprema de Justicia, 2017).

Relación circunstanciada de los hechos: La señorita “X” se presentó en sede fiscal el día once de septiembre del año dos mil diecisiete, a interponer denuncia en contra del imputado, Carlos Adrián V.R., a quien conoció en una fiesta de *Halloween*, no recordando la fecha pero si en el mes de octubre de dos mil dieciséis, ya que tenían amigos en común, desde ese día empezaron a comunicarse, iniciando una relación sentimental en enero de dos mil diecisiete.

Pero se da el caso que desde ese momento el empezó a presentar escenas de celos, obligándola incluso a borrar amigos de sus redes sociales, revisarle el teléfono, chantajeándola para que hiciera cosas con él, tales como tomarse fotos y subirlas a las redes sociales, dejarse tocar su cuerpo, alegándole que solo con él no quería hacer ese tipo de cosas alegando que él ya sabía que esas cosas la víctima las había hecho con su ex novio, también después de pelearse o después de discutir, el sujeto se hacía la víctima diciéndole que lo disculpara que él era así porque él no tenía dinero o no tenía una mansión como ella, que por su tipo de vida él tenía ese carácter, que él desde pequeño sufrió de *bullying*²⁰⁴, que por eso ella tenía que comprenderlo cuando el actuaba mal y le decía cosas feas.

Una de las ofensas que la víctima más recuerda es que una vez él decía que ella se había metido con hombres que tenían el pene más grande, o que se había metido cosas más grandes a su boca, haciéndole ver como que ella se había metido con un montón de hombres, diciéndole todo lo anterior con el afán de ofenderla, quienes terminaron esa relación sentimental la primera vez el día veintiuno de junio de dos mil diecisiete.

²⁰⁴ El bullying se trata de un acoso sistemático que se produce reiteradamente en el tiempo por parte de uno o varios acosadores a una o varias víctimas, afecta a todas las clases sociales. Ferran Barri Vitero, *Sos bullying*, (España: Monografías escuela española educación al día, 2006).

El día veinticuatro de junio del presente año, la víctima salió a comer con un amigo de ella, subiendo una foto a sus redes sociales sin que realmente evidenciara que en efecto la persona con quien ella había salido era del sexo masculino.

Pero al ver el imputado en dicha foto las bebidas que estaban sobre la mesa, éste asumió que había salido con un hombre, razón por la cual empezó a escribirle y a decirle que ella lo había engañado diciéndole "que ya le hacía falta salir con p(...) nuevos" "que era una m(...)" ese mismo día Carlos Adrián V. le dijo que él le había tomado un video donde ella le está realizando sexo oral, y al mismo tiempo que se lo enviaba por medio de chat (*whatsapp*) le escribía: "hoy si la regaste, hoy es mi turno, te voy a hacer quedar mal con un video que le podría interesar a tu papá o tu mamá, cheras igual vienen y van adiós ave de paso, vos no sos mujer, vos sos una m(...), con esos vídeos te voy a dejar quieta", razón por la cual ella le reclamo preguntándole que porqué lo hizo, porqué la grabó sin su consentimiento.

Después de esto el día domingo el sujeto se disculpó le prometió borrar dicho vídeo para que la víctima lo perdonara por lo que ella regreso con él, pero el imputado seguía celándola por cualquier motivo, pasaba revisándole sus redes sociales de modo que él sabía a quién agregaba, quien le daba "*like*" a sus publicaciones, por todo esto la víctima se molestaba con él, pero no terminaba la relación por temor ya que sí discutían o se peleaban el terminaba siempre acosándola, esperándola afuera de la casa de la víctima para ver con quien salía o con quien llegaba.

El día seis de agosto del presente año, con motivo del cumpleaños de Carlos Adrián V., salieron a celebrar a un bar ubicado en la colonia San Benito y posteriormente en una discoteca ubicada en carretera al Puerto de La

Libertad, ese día Carlos Adrián le hizo otra escena de celos, volviéndole a decir que aún tenía el video en su poder y que se lo iba a mostrar a sus papás, por lo que la víctima molesta le contestó que sus papás podían pagarle a un abogado para meterlo preso por poseer dicho vídeo, al mismo tiempo ella empezó a llamar a la policía, al ver esto Carlos, le pidió que por favor no lo hiciera que pensara en él y su familia, colgándole la llamada, y rogándole de rodillas que lo perdonara, la víctima en ese momento lo dejó en ese lugar (discoteca en el centro comercial La Joya) ahí sin mediar palabra.

El día diez de agosto regresaron a su relación de pareja, empezando nuevamente los pleitos por celos, finalmente el día veinticuatro de agosto del presente año terminaron la relación porque el imputado se molestó pues la víctima agregó a un sujeto a sus redes sociales, diciéndole que lo tenía que borrar porque él se sentía incómodo con eso y si ella quería tenerlo contento lo tenía que hacer, negándose a realizar tal acción, terminando nuevamente con él, pero Carlos Adrián no contento con eso, empezó a acosar a la víctima por medio de las redes sociales, viendo con quien salía, que hacía, llamándole constantemente de diferentes números telefónicos, escribiéndole a las amigas de la víctima.

Fue a la iglesia y a comer con sus amigos de la iglesia, subiendo una foto a sus redes sociales (*Instagram*), foto que fue vista por Carlos Adrián V., quien inició nuevamente el acoso telefónico, diciéndole que aun guardaba el video y mostrándole otro vídeo de ellos teniendo relaciones sexuales, y enviándole una foto a la víctima donde se reflejaba que dicho video se lo había enviado al padre de ella, diciéndole que todo esto lo hacía porque ella ya tenía otra pareja y tal vez así aprendía a no jugar con los hombres, por lo que ella le dijo que iba a tomar las medidas legales pertinentes, que por todos esos hechos se considera ofendida.

Por los hechos anteriormente expuestos, se le atribuyen al imputado en cuestión, una serie de delitos, pero únicamente se analizara en esta ocasión el delito que compete a esta investigación, siendo el delito de revelación indebida de datos o información de carácter personal, previsto y sancionado en el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos, en perjuicio de la libertad sexual, el honor y la intimidad de la víctima²⁰⁵.

Con respecto a este delito la cámara ratifica la apariencia del buen derecho, realizada por el juzgado primero de paz de Santa Tecla, La Libertad, en el sentido que de los elementos iniciales de investigación si acreditan la posible comisión del mismo.

En el caso en cuestión se ve claramente que se cumplen los requisitos para que se configure el delito de revelación indebida de datos o información de carácter personal, previsto y sancionado en el artículo 26 de la Ley Especial Contra Delitos Informáticos y Conexos, pues la víctima no dio su consentimiento en primer lugar para ser filmada y en segundo lugar no dio su consentimiento para que el imputado revelara y difundiera el video por medio del internet.

Al realizar el imputado esta acción ilícita quedo expuesta la imagen y la identidad de la víctima, ya que el daño que el imputado le creo no se revierte con el solo hecho de borrar los videos en los aparatos emisores y

²⁰⁵ En este caso al imputado se le atribuyen los delitos de acoso sexual, expresiones de violencia contra las mujeres y difusión de pornografía, acoso a través de tecnologías de la información y la comunicación, pero al ser el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos el tema de esta investigación solo de este delito se realiza el análisis de esta sentencia.

receptores²⁰⁶, sino que los datos almacenados quedan en los servidores que utilizan estos medios de comunicación; pues se trata de la intimidad de la víctima que está siendo difundida a terceras personas sin su autorización.

3.7.2 Análisis de sentencia internacional con número de referencia CFP 12474 – 2017 – 44 – CA5, Buenos Aires, Argentina

Sentencia de Buenos Aires, Argentina, con número de referencia CFP 12474/2017/44/CA5, el juez procesó con prisión preventiva a Leandro A. Rodríguez, Sebastián H. Karamanian, Martín O., Alejandro Adduci, Daniel Courmanian, Pablo Degano y Marcelo Vecchio. Todos fueron considerados miembros de una asociación ilícita los dos primeros, en carácter de jefes u organizadores, mientras que a Rodríguez, Adduci, Degano y Vecchio se lo hizo con relación a la figura del artículo 157 CP²⁰⁷.

El embargo impuesto a los imputados ascendió a la suma de diez millones de pesos \$10.000.000, en los considerandos de la misma pieza, se consignó que serían mantenidas las inhabilitaciones generales de bienes y congelamientos de cuentas antes dispuestos en la instrucción, que en parte abarcan a los ahora procesados.

En este caso se produjo como lo regula la Ley argentina una filtración de datos sensibles, de la Administración Federal de Ingresos Públicos (AFIP), un grupo de personas en forma organizada, continuada y permanente

²⁰⁶ La Cámara ratificó la resolución emitida por el juzgado primero de paz de Santa Tecla, La Libertad, se decretó la medida cautelar de la detención provisional en contra del imputado, ya que la Cámara considera que si el imputado se beneficia con medidas sustitutivas a la detención provisional, tendría la posibilidad, el tiempo y los medios suficientes para influir a la víctima para destruir evidencias, para brindar información falsa en las investigaciones.

²⁰⁷ Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, referencia: CFP 12474/2017/44/CA5 (Argentina: Corte Suprema de Justicia de la Nación).

operaba filtrando, recibiendo y/o comercializando datos sensibles²⁰⁸ y privados que los ciudadanos proporcionaban a la Administración Federal de Ingresos Públicos y que, por Ley, eran secretos.

Para ello, funcionarios públicos con acceso directo a ese tipo de información habrían con arreglo a ese acuerdo preconcebido recibido, en forma periódica, importantes sumas dinero a cambio de infringir sus deberes.

La Administración Federal de Ingresos Públicos almacena información personal, patrimonial, societaria, laboral, entre otras de las personas físicas y jurídicas que operan en el sistema de recaudación, estos datos, por Ley, son secretos y las razones son obvias: su sensibilidad, su carácter privado en la mayoría de los casos y las consecuencias negativas para los ciudadanos que puede implicar su difusión, por todo ello, los funcionarios públicos que tienen acceso a las bases que los almacenan tienen una obligación normativa de mantener su reserva (artículo 101, ley 11683; artículo 157 CP).

Los hechos anteriormente narrados configuran según el código penal de Argentina violación de secretos en los términos del artículo 157, tanto en el caso de los autores (funcionarios) como de los partícipes (particulares), pues se ha acreditado según el tribunal argentino la revelación de datos que por Ley debía permanecer en reserva, los empleados involucrados en este caso, utilizaban su cargo en la Administración Federal de Ingresos Públicos, para tener acceso a la información y hacerse de ella, revelando periódicamente los datos, sin contar con el consentimiento de los titulares de dicha información.

²⁰⁸ La definición de datos personales sensibles que proporciona la legislación salvadoreña se puede encontrar en el artículo 3 literales M Y N de la Ley Especial Contra los Delitos Informáticos y Conexos.

Se puede apreciar que el presente caso podría tipificarse en el artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos de El Salvador, puesto que presenta las condiciones que el mismo exige, ya que ninguno de los titulares de la información y datos que se revelaron dio su consentimiento para efectuar tales acciones.

3.8 Alcances y Limitantes del artículo 26 de la Ley Especial Contra los Delitos Informáticos y Conexos

3.8.1 Alcances

Los avances que han tenido tanto las tecnologías de la información como las tecnologías de la comunicación sin duda alguna han sido de mucha ayuda en las labores diarias de la humanidad, aunque existe la interrogante si el uso que se le está dando a estas herramientas es el adecuado o no²⁰⁹, se puede acceder a redes con información personal básica, para contactar, comunicar e interactuar con las personas en todo el mundo por medio del internet.

Estos progresos tecnológicos han roto casi que completamente la barrera tiempo y espacio, se puede contactar con una persona que este al otro lado del mundo, a miles de kilómetros de distancia, sin presentarse esto mayor problema, siempre y cuando ambos cuenten con una conexión a internet y la información que es emitida puede llegar instantáneamente a otra persona e incluso a otra ciudad, de igual manera posibilita una variedad de opiniones sobre una misma información lo que permite la libertad de expresión, sin

²⁰⁹ El problema que se analiza en el delito de la revelación indebida de datos o información de carácter personal no radica en los avances que han tenido en la actualidad las tecnologías de la información y la comunicación, sino en la mala utilización que se le está dando a los mismos y es una herramienta muy práctica para los delincuentes cibernéticos.

obligar a una persona a estar de acuerdo con una determinada postura o planteamiento.

Aunque estos avances han hecho posible que exista una variedad de opiniones de personas de diferentes regiones, razas, religiones, estatus sociales, preferencias sexuales, entre otros, también provoca que se lesione la integridad moral y psicológica de las personas, puesto que los individuos se expresan sin reparar en los daños o incluso delitos en que pueden incurrir.

Con la entrada en vigencia de la Ley Especial Contra los Delitos Informáticos y Conexos se refuerzan las investigaciones de estos delitos en la Policía Nacional Civil, ya que esta cuenta con una Unidad de investigación de delitos informáticos y así mismo con la capacitación a la policía y jueces de la república, sobre la investigación actual de los delitos informáticos. (A través de UNICEF, UNODC) y Analistas en informática forense/perito, también se recibe la donación de equipo informático para ayuda en las investigaciones.

La Ley Especial de Delitos Informáticos regula la protección de datos personales de todas las personas en integración con la Ley de Acceso a la Información Pública en la que establece el derecho a la protección de los datos personales y sus definiciones, aun cuando en nuestra legislación secundaria si protege este derecho, en El Salvador no existe una ley vigente de protección de datos y es muy importante que exista,²¹⁰ aunque ya existe en la Asamblea Legislativa dos proyectos de Ley que se están discutiendo respecto a dicho tema.

²¹⁰ El proyecto de Ley de protección de datos discutido en El Salvador busca proteger información privada de las personas contenidos en bases de datos y le da el derecho de supresión con excepciones, como la libertad de prensa, busca garantizar la protección de los datos personales de los ciudadanos que hayan sido proporcionados a organismos públicos y privados del país.

Las mujeres en el Salvador tienen una ley especial que protege sus derechos y regula también delitos informáticos cometidos a su persona, en relación al artículo 26 de la revelación indebida de datos o información personal es una integración de leyes que el delito se cometa contra la mujer.

3.8.2 Limitantes

La mayoría de avances tecnológicos o científicos, de las comunicaciones y de la información tiene también algunas limitantes y sin duda alguna una de esas limitantes es la perdida cada vez más evidente de la comunicación tradicional, es decir, la comunicación cara a cara, ya que se es más fácil hacerlo por medio de un aparato, y esto ha transformado la forma de socializar de los individuos, haciendo que cada día que pasa se aislen más del mundo, el tiempo que los jóvenes dedican a estar conectados en las redes sociales, el 25% de ellos pasan entre una hora y menos de dos horas, el 21% entre dos horas y menos de cuatro horas, un 15% entre cuatro y menos de siete horas.²¹¹, a la mimas vez por medio del uso de las redes sociales se puede establecer donde se encuentra una determinada persona, lugar y tiempo.

En el país no existe Fiscalía, Juzgados, ni jueces especializados en la materia del delito informático, y esta situación muchas veces es un obstáculo para el mismo proceso y la falta de conocimiento del mismo por la población, defensores y jueces, que si bien es cierto se han tratado de capacitar aun no es suficiente.

²¹¹ José Luis Alvares Rosales, Melvin Josué Amaya Mejía, Angélica Elizabeth Rauda Pérez, “Estudio diagnóstico sobre la influencia de las redes sociales en el proceso de socialización de estudiantes entre 15 y 17 años de edad que cursan el primer año de bachillerato del Instituto Nacional de San Bartolo en el año 2016” (Tesis de licenciatura: Universidad de El Salvador, 2016), 64.

El poder comunicarse con una persona al otro lado del mundo puede ser un alcance que se ha logrado con estos nuevos avances tecnológicos pero al mismo tiempo representa un riesgo para las personas que hacen uso de estos programas, herramientas o aparatos ya que al no poder ver cara a cara a la persona con la que se está comunicando se corre el riesgo que esta persona no sea quien se cree que es, sino otra totalmente diferente que se está haciendo pasar por alguien más, pudiendo así tener acceso a información de carácter privado o confidencial que está reservada solo a personas específicas²¹².

La seguridad en el internet es casi nula, existe una variedad de archivos e información que es plagiada²¹³ de otras páginas o incluso información falsa, es por esto que se debe tener mucha precaución con el uso del internet y asegurarse que toda la información que sea del interés de los individuos sea válida, real y no falsa, ya que cualquier persona que tenga acceso a una computadora puede ingresar a una red y revelar datos personales o información.

Algunas víctimas de los delitos regulados en la Ley Especial Contra los Delitos Informáticos y Conexos²¹⁴ interponen la denuncia pero abandonan el proceso en la etapa de investigación, por diferentes causas por desinterés, por falta de recursos económicos, por ignorancia de cómo se realiza este tipo

²¹² Al no saber con certeza quien es la persona con la que se está entablando una comunicación o una interacción hace más difícil para el sistema determinar responsabilidades criminales.

²¹³ El plagio es un deliberado delito que consiste en apoderarse de un trabajo ajeno reproduciéndolo palabra por palabra en parte o en su totalidad, Manuel Francisco Reina, *El plagio como una de las bellas artes*, (España: S.A. Ediciones B, 2012), 72.

²¹⁴ El delito que es de interés para esta investigación es el delito de revelación indebida de datos o información de carácter personal, en particular de las mujeres, sin embargo esta limitante del abandono del proceso se da en todos los delitos regulados en la Ley Especial Contra los Delitos Informáticos y Conexos.

de procesos, o por miedo a represarías por parte del o los sujetos responsables del hecho delictivo, este tipo de denuncias por ser delitos relativamente nuevos sus procesos de investigación pueden dilatar bastante desde seis meses hasta 2 o más años, una de las causas por las que algunas víctimas abandonan el proceso.

CONCLUSIONES

Con el surgimiento del internet, las relaciones humanas en El Salvador traspasan fronteras, esto implica que los delitos informáticos se vuelven posibles de realizar, por la facilidad de transferir y acceder a la información por medio de la red, dando con esto lugar a que las personas que realizan estos delitos queden en el anonimato y no puedan ser castigadas como la Ley lo establece, pero al mismo tiempo si se inicia el proceso de este tipo de delitos la policía y fiscalía es la que se encarga de llegar al final del proceso y castigar a los delincuentes cibernéticos.

Por consiguiente cuando se habla del delito informático de la revelación indebida de datos o información de carácter personal, se trata de un delito de naturaleza pluriofensivo porque vulnera una serie de derechos fundamentales como la intimidad, el honor, la integridad sexual y propiedad intelectual, con énfasis en las mujeres.

Las víctimas más frecuentes en este tipo de delitos informáticos son las mujeres, tomando en cuenta factores como las relaciones desiguales de poder entre hombres y mujeres, el control que sufre este sector de la población a través de las distintas redes sociales es cada vez más evidente, volviéndose esta problemática un fenómeno global en constante crecimiento y que se ha extendido en todos los aspectos de la sociedad, ya sea laboral, social, cultural, económico y político, en este sentido transgrede el ámbito privado e íntimo perpetuando la información vulnerada y revelada de las víctimas.

La seguridad de la protección de nuestros datos personales en el internet es casi nula, debido a que personas que acceden a las redes para cometer este

tipo de delitos tratan de borrar o tener información falsa de sus perfiles para no ser encontrados, es por esto que se debe tener mucha precaución con el uso del internet y asegurarse que toda la información que sea del interés de los individuos sea válida, real y no falsa, ya que cualquier persona que tenga acceso a una computadora puede ingresar a una red y revelar datos personales o información del titular, sin el consentimiento de este o lo que es peor aún sin que el titular de la información siquiera se dé cuenta.

Ley Especial de Delitos Informáticos regula la protección de datos personales de todas las personas en integración con la Ley de Acceso a la Información Pública en la que establece el derecho a la protección de los datos personales y sus definiciones, aun cuando en la legislación secundaria salvadoreña si protege este derecho, en El Salvador se discute una ley de protección de datos y es muy importante que exista para que los datos de las personas tengan mayor protección en este tipo de delitos y los demás que puedan cometerse en relación a los datos personales privados y sensibles.

En El Salvador se capacitan a los investigadores, técnicos en sistemas informáticos, policías, fiscales y jueces, tanto con el conocimiento, técnicas y herramientas tecnológicas, por los cambios constantes que presentan estos tipos de delitos, dichas capacitaciones deben ser constantes, necesarias para la búsqueda de evidencias de los delitos informáticos, por ultimo al ser las tecnologías de la comunicación y la información un medio de constante cambio en la red, los delitos informáticos están en evolución, lo que los vuelve más complejos para su investigación, por consiguiente las entidades y las instituciones encargadas para la protección de derechos vulnerados de las mujeres en los delitos informáticos necesitan estar a la vanguardia de los avances tecnológicos, y de las nuevas tecnologías de la comunicación, tanto en equipo como en capacitación de personal.

FUENTES DE INFORMACIÓN

LIBROS:

Agustino, Albert, Jorge Monclus, Ruiz. *Aspectos Legales de las Redes Sociales*. Barcelona, 2016.

Arias Flores, Rebeca, Helena, Van Acker, Arianna, Calza Bini. Programa de las naciones unidas para el desarrollo. Informe "Violencia de género en El Salvador". El Salvador, Mayo 2000.

Amaya Amaya, Jairo. *Sistemas de información*. Colombia, Universidad Santo Tomas.

Balardini, Sergio, Barindelli, Florencia, Carlos G. Gregorio, *datos personales y libertad de expresión en las redes sociales digitales*. Argentina.

Barri Vitero, Ferran. *Sos bullying*. España: Monografías escuela española educación al día. 2006.

Barriuso Ruiz, Carlos *Interpretación del derecho y la informática*, Madrid 1996.

Beekman, George. *Introducción a la Informática*. 6º ed. Madrid 2005.

Bertomeu Martínez, María Angustias. *Medios de Comunicación y Violencia contra las mujeres, La violencia en las tecnologías de la información y la comunicación*, Sevilla, 2003

Buompadre, Jorge Eduardo. *Violencia de género en la era digital. Modalidades mediante el uso de la tecnología*. Buenos Aires Bogotá, Porto Alegre, 2016.

Davara Rodríguez, Miguel Ángel. *Manual de Derecho Informático*, Aranzadi, SA, 2006.

Cabezuelo Arenas, Ana Laura. *Derecho de Intimidad*. Valencia: tirant lo Blanch, 1998.

Comer, Douglas E. *El Libro del internet*, traductor: Hugo Alberto, Acuña Soto y Roberto L. Escalona, 2ª Ed. México, Prentice Hall, 1998.

Consejo General del Poder Judicial. *Derecho al honor, a la intimidad y a la propia imagen II*. MADRID, 1999

De la Luz Lima, María. *Delitos Electrónicos*. Academia Mexicana de Ciencias Penales. Editorial Porrúa. No. 16. Año L. Enero-Junio 1984.

De la Puente Viedma, Carlos. *SPSS/PC+ una guía para la investigación*. Madrid: edit. Complutense.

De Pablos, Carmen. *Informática y comunicaciones en la empresa*. Madrid, edit. ESIC, 2004.

Espinoza Prieto, Alberto. *Introducción a la informática*. Madrid: McGraw-Hill/Interamericana de España, 2002.

Fariñas Matoni, Luis. *El Derecho a la Intimidad*. España: Trivium, 1983.

Garriga Domínguez, Ana. *Nuevas tecnologías y derechos humanos. Algunas consideraciones sobre los derechos humanos en internet*. Valencia, 2014.

Gómez Navajas, Justa. Prologo de Concepción Carmona Salgado. *La protección de los datos personales*, Madrid, 2005.

González Caytano, Norberto. *El Deber del Respeto a la Intimidad*. España: Universidad de Navarra, 1990.

Guardiola García, Javier. *La realización arbitraria del propio derecho*. Universidad de Valencia. 2003.

Jijena Leiva, Renato Javier. *Chile La Protección Penal de la Intimidad y el Delito Informático*. Chile 1992.

Kehoe, Brendan P., Miguel A. Martínez Sarmiento. *Internet del Arte al Zen*. México Prentice Hall, 1995.

León Kanashiro, Laura. *Datos personales y libertad de expresión en las redes sociales digitales*, Argentina

Levine, Guillermo. *Computación y programación moderna*. México, Pearson Educación, 2001.

Lizárraga Guerra, Víctor. *Fundamento del “Ne bis in ídem” en la potestad sancionadora de la administración pública*.

López Herrera, Josefina. *Programación en Tiempo Real y Bases de Datos: Un Enfoque Práctico*, Universidad Politécnica de Catalunya. Barcelona.

Malo Garizabal, Mario Madrid. *Derechos Fundamentales*, Bogotá, 1997.

Mano, Morris M. *Arquitectura de computadoras*. Universidad Estatal de California, Los Ángeles, tercera edición.

Modelell González, Juan Luis. *Temas Penales*. Caracas: Universidad Católica Andrés Bello. 2006.

Morales Prats, Fermín. *La protección del derecho a la intimidad de las personas (fichero de datos)*, Madrid, 1997.

Obando, Ana Elena. *Medios de comunicación y violencia contra las mujeres, Violencia contra las mujeres y nuevas tecnologías: un repaso al "mundo virtual"*, Sevilla, 2003.

Pardini, Aníbal Alejandro. *Derecho de Internet*. Buenos Aires: La Rocca, 2002.

Pérez, Carlota. *Revoluciones tecnológicas y capital financiero*. México, siglo XXI editores, S.A. De C.V.

Pérez, Henrique Cesar, Robledo, Luño. *El procedimiento de habeas data*. Madrid: edit. Dykinson.

Pons Rafols, Xavier. *La Declaración Universal de Derechos Humanos: Comentario artículo por artículo*. Edit. Icaria.

Prada Flores, Ignacio. *Criminalidad informativa, aspectos sustantivos y procesales*. Valencia 2012.

Reina, Manuel Francisco. *El plagio como una de las bellas artes*. España: 2014.

Rinaldi, Paola. *Origen y evolución del delito cibernético*. Abril 27 de 2017.

Robert Alexi, *Los Derechos Fundamentales en el Estado Democrático de Derecho*, en *Neoconstitucionalismo*, Madrid: edit. Trotta, 2003.

Rodríguez, Jorge Felipe. *Telecomunicaciones historia y conceptos básicos*. México: El colegio nacional. 2016.

Rubio Liniers, María Cruz, *Medios de comunicación y violencia contra las mujeres, Internet y la violencia contra las mujeres*, Sevilla 2003, 205.

Sánchez Momtufar, Luis Antonio. *Informática*, México, Pearson Educación, 2005.

Selva, Marta Anna. *Medios de comunicación y violencia contra las mujeres, Publicidad y violencia de género*. Sevilla, 2003.

TRABAJOS DE GRADO:

Alvares Rosales, José Luis, Melvin Josué, Amaya Mejía, Angélica Elizabeth, Rauda Pérez. “Estudio diagnóstico sobre la influencia de las redes sociales en el proceso de socialización de estudiantes entre 15 y 17 años de edad que cursan el primer año de bachillerato del Instituto Nacional de San Bartolo en el año 2016”. Tesis de licenciatura: Universidad de El Salvador. 2016.

Benavides Salamanca, Leo Bladimir, Marlon Iban, Hernández Anzora, Kenia

Katy, León Ardón. “La Penalización De Los Delitos Informáticos En El Salvador” Tesis para optar al Título de: Licenciado en Ciencias Jurídicas, Universidad de El Salvador. 2004.

García Mejía, Athina Vanessa, Víctor Andrés, González Guzmán. “El intrusismo informático y la utilización del Derecho Penal como mecanismo de tutela del derecho a la intimidad.” Tesis de Licenciatura: Universidad de El Salvador, 2017.

López Alfaro, Samuel Dolores, Antonio, Rosales, Wilfredo, Dolores, Jonathan Vladimir, Sabrán Iraheta, “Kit de herramientas de software en informática forense para ser utilizado en seminarios en el laboratorio de hardware de la Universidad Tecnológica de El Salvador”. Tesis de Licenciatura: Universidad Tecnológica de El Salvador. 2014.

LEGISLACIÓN:

Código Penal de El Salvador. Asamblea Legislativa de El Salvador. 1997. Aprobado por Decreto Legislativo N° 1030. D. O. N° 105. Tomo N° 335, del 10 de junio de 1997.

Código Procesal Civil y Mercantil. Decreto Legislativo N° 712, D. O. N° 224, Tomo N° 381, del 27 de noviembre de 2008.

Constitución de la Republica de El Salvador. Asamblea Constituyente de El Salvador. 1983.

Convenio Internacional de Telecomunicaciones. Ratificado por El Salvador el 22 de Julio de 1976.

Declaración Americana de los Derechos y Deberes del Hombre. Adoptado en San José, Costa Rica, el 22 de noviembre de 1969, en la Conferencia Especializada Interamericana Sobre Derechos Humanos. Ratificado por El Salvador el 20 de junio del año de 1978.

Declaración Universal de Derechos Humanos. Adoptada y proclamada por la Asamblea General en su resolución 217 A. Del 10 de diciembre de 1948.

Pacto Internacional de Derechos Civiles y Políticos 1966. Ratificado por El Salvador el 23 de noviembre de 1979. D.L. N° 27. Del 23 de noviembre de 1979. Publicado en D.O. N° 218. Tomo 265 del 23 de noviembre de 1979.

Ley de Acceso a la información Pública. Aprobada por Decreto Legislativo N° 534, D. O. N° 70, Tomo N° 391, 08 de abril de 2011.

Ley de Protección al Consumidor. Decreto Legislativo N° 776, Diario Oficial N° 166, Tomo N° 368, de fecha 08 de septiembre de 2005.

Ley de Reparación Por Daño Moral. Aprobada por Decreto Legislativo N° 216, D. O. N° 5, Tomo N° 410, del 08 de enero de 2016.

Ley Especial Contra los Delitos Informáticos y Conexos. República de El Salvador. Aprobada por Decreto Legislativo N° 260. D. O. N° 40. Tomo N° 410. 26 de febrero de 2016.

Ley Especial Integral Para Una Vida Libre de Violencia Para Las Mujeres. República de El Salvador. Aprobada por Decreto Legislativo N° 520. Publicada en el D. O. N° 2. Tomo 390, de fecha 04 de enero de 2011.

Reglas de Brasilia Sobre Acceso a la Justicia de las Personas en Condición de Vulnerabilidad. <https://acnur.org>

JURISPRUDENCIA:

Cámara Tercera de lo Penal de la Primera Sección del Centro. *Recurso de apelación*. Referencia: INC-259-17. El Salvador: Corte Suprema de Justicia. 2017.

Cámara de lo Contencioso Administrativo. Sentencia con numero de referencia 00036 – 18 – ST – COPC – CAM. El Salvador. Corte Suprema de Justicia. 2018.

Sala de lo Constitucional. Sentencia de Amparo. Referencia número 118 – 2002. El Salvador. Corte Suprema de Justicia. 2004.

Cámara Nacional de Apelaciones en lo Civil y Comercial Federal. Referencia: CFP 12474/2017/44/CA5. Argentina: Corte Suprema de Justicia de la Nación.

DOCUMENTOS INSTITUCIONALES:

Fiscalía General de la Republica de El Salvador. Escuela de capacitación fiscal. Equipo del programa global del ciberdelito. “Análisis jurídico de los delitos contenidos en los capítulos I, II, III, y V del título segundo de la Ley Especial Contra Los Delitos Informáticos y Conexos”. 2018.

FUENTES HEMEROGRAFICAS:

Bryan, Avelar, "Presidente del IAIP renuncia tras filtración de datos de Ciudadanos a la presidencia," revista Factum, 15 de noviembre de 2019. <http://www.revistafactum.com>.

Campos Madrid, Gabriel, Laura, Flores. "Proponen una Ley de datos y habeas data". La prensa gráfica. Sección Política. 25 de junio de 2019.

Callegari, Nidia. "Delitos informáticos y legislación". Revista de la facultad de derecho y ciencias políticas de la Universidad Pontificia Bolivariana. Medellín Colombia 1985.

Consejo de la Judicatura, Órgano Doctrinario e informativo del H. Tribunal Superior de Justicia del estado de Veracruz-Llave, "Revista Jurídica Veracruzana", 2011.

Miranda Enrique. "Asamblea inicia estudio de Ley para proteger datos personales". El Diario de Hoy. Sección Política. 06 de noviembre de 2019.

Naciones Unidas, "Revista Internacional de Política Criminal" Manual de las Naciones Unidas sobre prevención y control de Delitos Informáticos, 1994.

Orellana de Gutiérrez, María Elena, "Habeas Data" Tesis de licenciatura: Universidad Salvadoreña Alberto Masferrer, 1994, Monografía proporcionada por Biblioteca de la Corte Suprema de Justicia.

Osorio Morales, José Edmundo. "Estudio Centroamericano de protección de datos, El Salvador".

Posada, Ricardo. "Presentan proyecto de Ley que busca proteger los datos

personales”. Diario El Mundo. Sección Política. 25 de junio de 2019.

“Salvadoreños serán multados sino cumplen nueva Ley de protección de datos de la UE”. El Diario de Hoy. Sección de negocios. 24 de mayo de 2018.

SITIOS WEBS:

Ayuda en acción. *Blog Mujer. tipos de Violencia contra las mujeres*. 05 de julio de 2018. <https://ayudaenaccion.org/ong/blog/mujer/tipos-violencia-mujeres/>.

Avelar, Bryan. “Presidente del IAIP renuncia tras filtración de datos de ciudadanos a la presidencia”. Revista Factum. <Http://www.revistafactum.com>. 15 de noviembre de 2019.

Alegsa Leandro. *Definición de macrocomputadora o macroordenador*. Alegsa.com.ar, 7 de junio, 2019. <http://www.alegsa.com.ar/Dic/macrocomputadora.php>

Amaya, Javier, Paz Cantalicio, Hollerith Herman. *Tarjetas perforadas, La primera tarjeta perforada*. Consultado 11 de oct de 2019 <https://sites.google.com/site/cantaliciohollerithoa/targetas-perforadas/la-primera-tarjeta-perforada>

Alemán, Misael. Blog *Historia del internet en El Salvador*. 20 de julio de 2017. <https://www.misaelaleman.com/historia-del-internet-en-el-salvador>.

Belloch Ortí, Consuelo. *Las tecnologías de la información y comunicación*.

Universidad de Valencia. Consultado 13 de octubre de 2019.
<https://www.uv.es/~bellochc/pdf/pwtic1.pdf>

Bonilla, Francy Milena. *Origen, historia y evolución de las TIC*. 15 oct, 2019.
<https://sites.google.com/site/ticsyopal5/assignments>

Calderón, Daniel. <https://es.calameo.com/books/00548365172880153bba7>

Campillo, Santiago. *45 Años de ARPANET, el origen de internet*. 21 de nov 2014. <https://hipertextual.com/2014/11/arpamet-45-anos>

Caride, Alba. *Tipos de redes sociales*. 17 de octubre de 2017.
<https://www.hoyreka.com/tipos-redes-sociales/>

Casella, Ayelen, Toia Leonardo *Derecho al Nombre Argentina* 2012.
<http://www.derecho.uba.ar/publicaciones/libros/pdf/la-cadh-y-su-proyeccion-en-el-derecho-argentino/018-casella-toia-nombre-la-cadh-y-su-proyeccion-en-el-da.pdf>

Ceruzzi, P. E. *Historia de la informática*. Madrid. openmind BBVA, 2008.
<https://www.bbvaopenmind.com/articulos/historia-de-la-informatica/>

Checks. Blogs. Delitos Informáticos. *Historia de los delitos informáticos*.
Lunes 14 de Noviembre de 2011.

Chirino, Alfredo *Manual operativo de protección de datos en el salvador*.
2015. http://sia.eurosocial-ii.eu/files/docs/1432887451-DT_26_Chirino.pdf

Consultores Certificados de primer nivel, expertos en Protección de Datos

Personales & Privacy Compliance, HABEAS DAT. *Preguntas Frecuentes: ¿Qué tipo de datos personas hay?* Servicios en protección de datos personales en Argentina, Colombia, Perú y México. Fecha de consulta de página agosto 10, 2019. www.habeasdat.com/faq.html

Consultoría de Protección de datos. *Tipos de datos personales* Rubí – Barcelona, 15 de noviembre de 2018. <https://www.protecciondatos.org/tipos-de-datos-personales/>

Cuauhtémoc M. *El derecho a la intimidad, al honor y a la propia imagen* revista jurídica IUS, Universidad Latina de América. <http://www.unla.mx/iusunla3/reflexion/derecho%20a%20la%20intimidad.htm>

Diario Jurídico, "las redes sociales y protección de datos", 11 diciembre, 2017. <https://www.diariojuridico.com/las-redes-sociales-y-la-proteccion-de-datos/>

División Computer Forensic, *Tipos de delitos Informáticos*, [https:// www.Delitosinformaticos.info/delitos_informaticos_tipos_delitos.html](https://www.Delitosinformaticos.info/delitos_informaticos_tipos_delitos.html)

Estévez, Juan Carlos. *En qué consiste el convenio de Budapest y cómo regula la ciberdelincuencia.* 06 enero 2020. <https://empresas.blogthinkbig.com/convenio-budapest-ciberdelincuencia/>

Faith Davies. *Definición del lenguaje de computación BASIC.* Techlandia, consultado 13 de octubre 2019), https://techlandia.com/definicion-del-lenguaje-computacion-basic-hechos_47795/

FGR y UNODC. *Análisis jurídico de los delitos contenidos en los capítulos I II*

III y V del Título segundo de la Ley especial contra los delitos informáticos y conexos. El Salvador, 2018, <http://escuela.fgr.gob.sv/wp-content/uploads/leyes-nuevas/analisis-juridico-de-la-ley-especial-contra-los-delitos-informaticos-y-conexos-COMPLETO-CAP-I-II-III-V.pdf>

FUSADES. *¿Quiénes somos?* 03 de septiembre 2019. <http://fusades.org/fusades/conocenos/acerca-de-fusades-2>.

García, Santasmases, Alberto, Prieto Espinosa, Premio Ramón Llull 2006. Madrid. Sociedad Científica Informática de España, 2006. <http://www.scie.es/premiado/alberto-prieto-espinosa/>

García en Zinetik, Miryam Consultores. *Violencia de género en redes sociales* (8 noviembre 2019), <https://zinetik.com/violencia-de-genero/>

Guías Jurídicas Wolters Kluwer. *Derecho a la propia imagen*. Consultado 19 mayo 2020. <https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAKMjU1MjE7WY1KLizPw8WYMDQ3MDcyMDkEBmWqVLfnJIZUGqbVpiTnEqAJohrjY1AAAAWKE>.

Gutiérrez, Miriam. *Derecho a una identidad*. <https://www.humanium.org/es/derecho-identidad/>.

Hall Andres. *Tipos de delitos*. Argentina, consultado 19 de noviembre de 2019. http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

Hernández Lotero, Natalia. *Clasificación de los datos personales e implicaciones legales* (Bolivia, fecha de consulta 13 de noviembre de 2019), <https://repository.upb.edu.co/bitstream/handle/20.500.11912/3595/Clasificaci>

%C3%B3n%20de%20los%20datos%20personales%20e%20implicaciones%20legales.pdf?sequence=1

Ibarra Hernández, Rafael Antonio. *Internet en El Salvador*. 27 de abril 2002. <https://nsrc.org/regions/CENTRAM/SV/Internet-SV-04-2002.PDF>

Ibarra, Marco. *Pascalina: Descripción y Características, Funcionamiento*. lifider.com. Consultado 11 de oct 2019. <https://www.lifeder.com/pascalina/>

Industria y comercio Superintendencia. *Protección de datos personales: Aspectos prácticos sobre el derecho de Habeas Data*. 2017. https://protecdatalatam.com/wpcontent/uploads/2017/07/Aspectos_Derecho_de_Habeas_Data.pdf

Isaac Julio. *Herramientas Informáticas y su diferencia con las Tics*. Septiembre 18, 2015. [https:// grupo4 herramientas informatica. blogspot.com/ 2015/09/ herramientas -informatic as-y-su.html](https://grupo4herramientasinformatica.blogspot.com/2015/09/herramientas-informaticas-y-su.html)

La internet. Blog. *La Historia del Internet y su Evolución*. 3 de mayo, 2012. <http://internethistoriayevolucion.blogspot.com/2012/05/concepto-y-caracteristicas-de-la.html>

LemonHead. Blog web de Duiops. Consultado 13 de agosto de 2019. <https://www.duiops.net/hacking/hacking-cracking.htm>

La Cumbre Judicial Iberoamericana. [Https://www.cumbrejudicial.org](https://www.cumbrejudicial.org)

Mecafenix Frank. *¿Qué es un transistor y cómo funciona?* Consultado 8 de agosto, 2019. <https://www.ingmecafenix.com/electronica/el-transistor/>

Ministerio de Asuntos Exteriores, unión europea y cooperación, representación de España ante naciones Unidas y organismo internacionales, <http://www.exteriores.gob.es/RepresentacionesPermanentes/OficinadelasNacionesUnidas/>

Molina Medrano, Carlos. *A un año de la aprobación de la Ley de Delitos Informáticos en El Salvador: retos y desafíos* Unidad de Informática y Comunicaciones Universidad Luterana Salvadoreña, 23 de febrero 2017. <https://www.uls.edu.sv/sitioweb/component/k2/item/551-a-un-ano-de-la-aprobacion-de-la-ley-de-delitos-informaticos-en-el-salvador-retos-y-desafios>

Montero, Damián. *Violencia de género en redes sociales, un peligro silencio*, Europa, 2019. <https://www.hacerfamilia.com/actualidad/violencia-genero-redes-sociales-peligro-silencioso-20170422173729.html>

Navarrete Fernández, Jordi. *Tipos de redes sociales y sus características* Sept. 2018 <https://www.inboundemotion.com/blog/tipos-de-redes-sociales-y-sus-caracter%C3%ADsticas>

Ovies Gage, Mario. *¿Es Whatsapp una red social?* (febrero 28, 2017), <https://medium.com/@MarioOvies/es-whatsapp-una-red-social-8661cbf8238a>

Pérez Porto, Julián, Merino, María. *Definición situación social* Publicado: 2014. Actualizado: 2016. <https://definicion.de/situacion-social/>

PRODATO Protección de datos personales. *¿Qué tipo de datos personales hay? Categorías de datos.* México, junio 30, 2011. <https://prodato.mx/2011/06/30/%C2%BFque-tipo-de-datos-personales-hay/>
Protección de datos. *Tipos de datos personales* Rubí – Barcelona, 15 de

noviembre de 2018. <https://www.protecciondatos.org/tipos-de-datos-personales/Raffino>, María Estela. 10 de enero de 2019. <https://concepto.de/base-de-datos/#ixzz5yWNXjvuS>.

Rouse, Margaret. *Información de identificación personal* (2014), <https://searchdatacenter.techtarget.com/es/definicion/Informacion-de-identificacion-personal-PII>

SPEEDCHECK. *Protocolo de Control de Transmisión y Protocolo de Internet*. 03 de septiembre 2019. <https://www.speedcheck.org/es/wiki/tcp-ip/>

Stelgon Gonzo. *Historia de Delitos informáticos*. 18 de noviembre de 2008. <http://gonzostelgon.blogspot.com/2008/11/historia-de-delitos-informaticos.html>.

Sain, Gustavo. Revista Pensamiento Penal. “*Evolución histórica de los delitos informáticos*”. 2015.

Sistemius, despacho de abogados tecnológicos de Santiago de Compostela. *Ciberdelincuencia: los 4 delitos informáticos más comunes, tipos de ciberdelitos* España, 2 de diciembre 2018. <https://www.sistemius.com/ciberdelincuencia-4-tipos-de-delitos-informaticos.html>

Unión Europea, Junta de Andalucía. *Guía de formación TIC para padres y madres de adolescentes: Tipo de redes sociales* (Sevilla, consultada 29 de noviembre de 2019), <https://www.andaluciaesdigital.es/edu/Carparaproteger/adolescentes/>

[http://www. Pensamientopenal .com. ar/system/files/ 2015/04/doctrina 40877 .pdf.](http://www.Pensamientopenal.com.ar/system/files/2015/04/doctrina_40877.pdf)

[http://delitosi nformaticoslaschecks .blogspot. com 2011/11/historia-de-los- delitos –informaticos .html.](http://delitosinformaticoslaschecks.blogspot.com/2011/11/historia-de-los-delitos-informaticos.html)

OTRAS FUENTES:

Entrevista realizada al Jefe de la Unidad de Investigación de delitos informáticos de la Policía Nacional Civil de El Salvador.