UNIVERSIDAD DE EL SALVADOR

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

ESCUELA DE CIENCIAS JURÍDICAS

EL INTRUSISMO INFORMÁTICO Y LA UTILIZACIÓN DEL DERECHO PENAL COMO MECANISMO DE TUTELA DEL DERECHO A LA INTIMIDAD

TRABAJO DE GRADO PARA OBTENER EL TÍTULO DE:

LICENCIADO (A) EN CIENCIAS JURÍDICAS

PRESENTADO POR:

GARCÍA MEJÍA, ATHINA VANESSA

GONZÁLEZ GUZMÁN, VÍCTOR ANDRÉS

DOCENTE ASESOR:

LIC. MARVIN HUMBERTO FLORES JUÁREZ

CIUDAD UNIVERSITARIA, NOVIEMBRE DE 2017

MIEMBROS DEL TRIBUNAL CALIFICADOR DEL TRABAJO DE GRADO

LIC. FRANCISCO ALBERTO GRANADOS HERNÁNDEZ

(PRESIDENTE)

LIC. SANTOS CECILIO TREMINIO SALMERON

(SECRETARIO)

LIC. MARVIN HUMBERTO FLORES JUÁREZ

(VOCAL)

UNIVERSIDAD DE EL SALVADOR
MSC. ROGER ARMANDO ARIAS
RECTOR

DR. MANUEL DE JESÚS JOYA ABREGO
VICERECTOR ACADEMICO

ING. NELSON BERNABÉ GRANADOS
VICERECTOR ADMINISTRATIVO

MSC. CRISTÓBAL HERNÁN RÍOS BENÍTEZ
SECRETARÍO GENERAL

LIC. RAFAEL HUMBERTO PEÑA MARÍN
FISCAL GENERAL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES
DRA. EVELYN BEATRIZ FARFÁN MATA
DECANA

DR. JOSÉ NICOLÁS ASCENCIO HERNÁNDEZ
VICEDECANO

LIC. JUAN JOSÉ CASTRO GALDÁMEZ
SECRETARIO

LIC. RENÉ MAURICIO MEJÍA MÉNDEZ
DIRECTOR DE LA ESCUELA DE CIENCIAS JURÍDICAS

LIC. MIGUEL ÁNGEL PAREDES B.
DIRECTOR DE PROCESOS DE GRADUACIÓN

LICDA. MARÍA MAGDALENA MORALES
COORDINADORA DE PROCESOS DE GRADUACIÓN DE LA ESCUELA DE CIENCIAS JURÍDICAS

ÍNDICE DE CONTENIDO

CAPÍTULO II
FUNDAMENTOS TEÓRICOS DEL DERECHO A LA INTIMIDAD Y DE LA INTRUSIÓN INFORMÁTICA

CAPÍTULO III

REGULACIÓN JURIDICA EN MATERIA PENAL Y DERECHO INTERNACIONAL RELATIVA AL DERECHO A LA INTIMIDAD

CAPÍTULO IV
ANÁLISIS DOCTRINAL DE LA INTERVENCIÓN DEL DERECHO PENAL EN LA INTERNET

CAPÍTULO V

COMENTARIOS JURIDICOS Y DOCTRINAL A LOS DELITOS TIPIFICADOS EN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS QUE PROTEGEN EL DERECHO A LA INTIMIDAD DE LA INTRUSIÓN INFORMÁTICA.

RESUMEN

El desarrollo de la Informática trajo como consecuencia que se pudiera "almacenar" información de manera voluminosa, mediante las computadoras. Creándose "banco de datos" o "banco de memoria", acumulando información en un mínimo espacio. El registro, pues, contenido en un banco de datos es la información que se le ha suministrado a la memoria de la computadora, la cual mantiene por tiempo indefinido, pudiendo tener acceso a ella, no sólo una persona, sino algunas autorizadas, y otras en algunos casos no autorizadas, así como la información puede ser transferida a un número indefinido de otras computadoras.

Se puede decir que aquellas personas, cuyos datos individuales, sin discriminación entre públicos y privados, están dentro de un banco de datos, se encuentran indefensas en cuanto al resguardo de su intimidad y la de su familia, pues la manipulación impacta negativamente en las relaciones individuales y sociales en general, afectando bienes jurídicos, en este orden de ideas la evolución de la informática ha obligado al legisferante a tratar de imponer límites a conductas humanas delictivas. Siendo el caso que en El Salvador poco o nada toma en consideración los nuevos parámetros tecnológicos que existen para la comisión de ilícitos en especial los que afectan el derecho a la Intimidad.

Por lo que en esta investigación se expondrá la vulnerabilidad que representa el tráfico de información en las redes, que presuponen una puerta abierta a la intimidad, y la posibilidad de que esta información confidencial o personal pueda ser accedida por terceros con facilidad afectando la intimidad y privacidad de su titular.

INTRODUCCIÓN

La tecnología en El Salvador es una de las herramientas que tienen los salvadoreños, la cual los hace ser más productivos de lo que eran décadas atrás cuando no tenían los avances tecnológicos de la actualidad, así como la tecnología los ayuda a producir, lamentablemente también ayuda a delincuentes a cometer delitos en el anonimato, por ejemplo la intimidad ha sido uno de los derechos que más ha sido vulnerado en los últimos años, esto debido a la complejidad que conlleva proteger la esfera privada de una persona frente a las posibilidades de vulneración que ofrece las tecnologías digitales.

En esta investigación titulada “El Intrusismo Informático y La Utilización Del Derecho Penal Como Mecanismo De Tutela Del Derecho a La Intimidad” se pretende efectuar un análisis sobre la protección penal de la intimidad en el ciberespacio, abordándolo en cinco capítulos los cuales pueden quedar resumidos de la siguiente forma.

En el capítulo uno se aborda la evolución histórica de la intimidad e informática, planteando aspectos y contextos internacionales y nacionales que fueron relevantes para la constitución de ambos conceptos; seguidamente en el capítulo dos se plantean fundamentos teóricos de la intimidad e informática logrando con cada uno de estos las definiciones, características y elementos que los constituyen; en el capítulo tres se pretende abordar desde una visión del Derecho comparado la manera de como se ha regulado la protección de este derecho frente a las tecnologías informáticas y es que en distintos países de la región han estado afrontando problemáticas por los avances tecnológicos, y en su mayoría se concluye creando leyes de delitos informáticos e incluso creando instituciones que se

especializan en tecnología, esto con el fin de enfrentar el fenómeno del internet.

En el capítulo cuatro se hace mención del involucramiento del Derecho Penal en el internet, con ello se busca entender la evolución que ha tenido el derecho con el fin de salvaguardar bienes jurídicos; por último en el capítulo cinco se hacen comentarios jurídicos y doctrinales de los delitos tipificados en la Ley Especial contra los Delitos informáticos y conexos aprobada en El Salvador el pasado seis de febrero de 2016, con énfasis en la protección a la intimidad.

Es de acotar que para el desarrollo de esta investigación se adoptó una metodología de tipo documental, considerando a los autores con conocimientos en la materia así mismo disposiciones legales y jurisprudencia nacional e internacional.

ABREVIATURAS

Art. Artículo.

Arts. Artículos.

Cpr. Pn. Código Procesal Penal de El Salvador.

Cc. Código Civil de El Salvador.

Cpn. Código Penal de El Salvador.

Cn. Constitución de la República de El Salvador.

Coord. Coordinadores.

Ed. Edición.

Edit. Editorial.

Et al. Y Otros.

Ibíd. Ibídem.

Inc. Inciso.

N.d. No Date.

Ref. Referencia.

Trad. Traductor.

Vol. Volumen.

SIGLAS

ARPANET. Red de la Agencia de Proyectos de Investigación Avanzada.

CONACYT. Consejo Nacional de Ciencia y Tecnología.

DARPA. Agencia de Investigación de Proyectos Avanzados.

GLACY. Acción Global Contra el Cibercrimen Extendido.

HP. Hewlett-Packard.

IBM. International Business Machines.

NSF. Fundación Nacional de Ciencia.

OEA. Organización de los Estados Americanos.

ONU. Organización de las Naciones Unidas.

LECDIC. Ley Especial Contra los Delitos Informáticos y Conexos.

CAPÍTULO I
ANTECEDENTES HISTÓRICOS DE LA INTIMIDAD COMO DERECHO HUMANO Y ASPECTOS GENERALES DE LA INFORMÁTICA

En el presente capitulo, se estudian los antecedentes históricos de la intimidad como derecho humano y los aspectos generales de la informática, con el objeto de verificar y determinar con exactitud su origen, el desarrollo en el transcurrir de la historia, tanto a nivel internacional y nacional; y acercarse más a los términos Intimidad e Informática.

A lo largo de la evolución de la humanidad, las personas se han percatado que necesitan espacios intelectuales o materiales orientados a preservar sus ideas y sueños, de manera tal, que las demás personas no puedan invadir este campo, es así que los psicólogos crean el concepto de la extimidad como la exposición de los aspectos íntimos de la persona, neologismo que de alguna forma expresa que lo más interno, lo más íntimo, se encuentra en el exterior.[1]

La reflexión sobre lo íntimo, individual o lo propio, no enmarcado en término de bienes, se remonta muy atrás en la historia, ligado con la especulación sobre la libertad, mezclándose incluso con uno de los aspectos más destacados en la historia de las civilizaciones, la cual yace en el fondo una distinción de lo público con lo privado, misma que es muy necesario para un adecuado enfoque de este derecho fundamental, quizás una de las primeras reflexiones sobre la intimidad -aunque obviamente sea desde una óptica o

[1] La extimidad es un concepto que es acuñado al francés Jacques Lacan en 1958, sin embargo fue hasta el siglo XXI que se usa por los psicoanalistas para referirse a la tendencia de las personas a hacer pública su intimidad.

punto de vista religioso-, son los primeros símbolos de la intimidad, tratados en el libro del Génesis, en el relato de la creación y la manera a través de la cual Adán y Eva después de comer del árbol del bien y el mal, a consecuencia de la pena que sentían, se tapaban sus zonas corporales íntimas, como una demostración de la intención positiva de guardarse cierta parte del cuerpo, -órganos genitales-, para sí, la cual no deseaban que fuese expuesta a Dios, ni a las demás criaturas que moraban en el Jardín del Edén.

De los párrafos que anteceden se puede afirmar que el ser humano viene al mundo desnudo sin guardarse nada y conforme evoluciona, y convergen una serie de situaciones, -según el relato bíblico, comen del fruto del árbol del bien y el mal-, surge la necesidad de delimitar de algún modo su esfera de intimidad, muy probablemente como un mecanismo de supervivencia y para el logro de una calidad de vida mínima, la cual se acrecentó con la llegada de más seres humanos.

Dicho lo anterior, fácilmente se puede llegar a la conclusión que cuanto más sofisticada o refinada sea una sociedad, más valor tiene en ella la intimidad, contrario sensu mientras más primitiva sea esta, más valor tiene en ella la vida comunitaria y por ende, menos valor tiene el individuo como tal de forma aislada, a efecto de demostrar de forma fehaciente, las ideas planteadas, a continuación se describen aspectos relevantes de las civilizaciones Griega y Romana, haciendo mención a contextos históricos sociales que aportaron elementos para la configuración del Derecho de Intimidad.

1. Antecedentes históricos del derecho a la intimidad

En torno a la problemática del origen del concepto intimidad se han formulado dos teorías contrapuestas, la primera podría llamarse “racionalista”

pues sitúa el alba de este derecho en el período del "racionalismo"[2] y de la "ilustración"[3] en conexión con el ascenso de la burguesía; la segunda podría calificarse de "histórica" sosteniendo que la intimidad como derecho y como fenómeno nació antes de la revolución francesa haciendo alusión a los datos históricos que se han ido recabando, así como los filosóficos y antropológicos.

1.1. Grecia

Los estudiosos de la Grecia antigua han puesto de relieve que si hay un trazo característico de la idea de Estado de los griegos, es el valor ilimitado que se atribuye a la comunidad, valor de tal magnitud que la existencia de una esfera reservada a la vida propiamente personal del ser humano estaba en principio, excluida; apenas hay algún terreno de la vida que no le esté vedado,[4] el individuo apenas posee una vida espiritual propia y su intimidad se manifiesta en los resquicios que deja lo público, es decir la idea griega del Estado tiene la concepción de la sumisión completa del individuo a este.[5]

El Estado Griego, al menos en teoría, podía intervenir en casi todo, es decir, que los mismos griegos, le reconocían una autoridad prácticamente ilimitada, ya que el Estado podía intervenir en la moralidad privada de un individuo o de sus creencias religiosas, de modo paralelo la libertad y los derechos del

[2] *Corriente filosófica formulada por René Descartes, que se complementa con el criticismo de Immanuel Kant, y que es el sistema de pensamiento que acentúa el papel de la razón en la adquisición del conocimiento, en contraste con el empirismo, que resalta el papel de la experiencia, sobre todo el sentido de la percepción.* Racionalismo. N. d., goo.gl/fw051v.

[3] *Movimiento cultural e intelectual europeo (especialmente en Francia e Inglaterra) que se desarrolló desde finales del siglo XVII hasta el inicio de la Revolución francesa, aunque en algunos países se prolongó durante los primeros años del siglo XIX. Fue denominado así por su declarada finalidad de disipar las tinieblas de la humanidad mediante las luces de la razón. El siglo XVIII es conocido, por este motivo, como el Siglo de las Luces.* Ilustración. N.d., goo.gl/YUVXoU.

[4] Carlos Ruiz Miguel, "La Configuración Constitucional del Derecho a la Intimidad" (tesis doctoral, Universidad Complutense de Madrid, 1992), 12.

[5] Ibíd.

individuo y sus contrarios; la obligación y el deber político, son nociones que no existen o que aparecen solo de forma embrionaria en el pensamiento griego.[6]

Puede afirmarse, por tanto, que en Grecia no se diferenciaba entre vida pública y vida privada, puesto que la democracia ateniense se basaba fundamentalmente en la participación de todos los ciudadanos en las cuestiones públicas, siendo iguales todos para el desempeño de cargos públicos, ya que la esencia del hombre se centraba en el ser público.[7]

1.2. Roma

"La ciudadanía en Roma"[8] dispuso de un sistema jurídico mucho más flexible y adaptable de lo que nunca conoció Grecia, ya que la ciudadanía para los romanos no significaba necesariamente aquel parentesco social que constituyó un límite absoluto y fatal para la política griega; sin duda, la plena ciudadanía supuso al principio, un tipo de unión de parentesco total, en lo político, religioso, lo moral y lo social, en Roma, se empieza a percibir cierta protección de la esfera privada del individuo no obstante ello, todavía se trata de un estadio muy preliminar y pocos avances significativos se producen en el reconocimiento de la intimidad en la antigua Roma.

Con los romanos se consigue la sistematización y enseñanza del Derecho,

---

[6] Lucia Victoria Hernández Martínez, "El Derecho a la Intimidad Personal y su Actual Regulación Dentro del Ordenamiento Jurídico Salvadoreño" (Tesis de grado, Facultad de Jurisprudencia y Ciencias Sociales, Universidad de El Salvador, San Salvador, El Salvador, 2009), 13.

[7] Al respecto, resultan interesantes las clásicas obras de Platón y de Aristóteles, dejando entrever el poco valor que daba en Grecia a la intimidad en contraposición con la vida comunitaria, véase: Aristóteles, *La Política* (edit. y trad. Julio Pallí Bonet. 1981); Platón, *La Republica* (Madrid: Clásicos Bergua).

[8] *La ciudadanía romana era una posición social privilegiada en relación con las leyes, estatus social, propiedad y acceso a posiciones de gobierno, que se otorgaba a ciertos individuos a lo largo de la historia de la Antigua Roma. Ciudadano Romano*. N.d., goo.gl/g2T0vy.

algo que no existía con los griegos, contemplándose con ello, algunas acciones que tienden a la reparación de los daños producidos en la esfera de lo privado, siendo la correspondencia uno de los ámbitos protegidos.

Asimismo en el Derecho romano ya existía la posibilidad de ejercitar una actio iniuriarum "acción de injuria",[9] puesto que el concepto de injuria alcanza al ultraje del pudor de ciertas personas y, con la misma acción, se protege la inviolabilidad del domicilio.

Sin lugar a dudas, la protección de la inviolabilidad del domicilio es la manifestación más significativa y la que con mayor claridad perdura en los ordenamientos jurídicos de influencia romana, sin embargo, es importante tener en cuenta un pequeño matiz, consiste en que la idea del respeto al domicilio no deriva de la idea de garantizar el respeto hacia la persona o familia, sino más bien, por una extensión personal del derecho real de propiedad, es decir, se trataba de una protección vinculada al derecho de propiedad y no a la dignidad personal.

De lo enunciado en los párrafos precedentes, se afirma que ni en Grecia ni en Roma se puede hablar del derecho a la intimidad como tal, aunque como se ha visto en el Derecho romano se vislumbran ciertas manifestaciones jurídicas de la intimidad, siendo la del respeto al domicilio y el respeto a la correspondencia las más significativas.

1.3. La Revolución Francesa

Francia en los años de 1789 a 1799 considerada como el indicador del final de una época histórica y el punto de arranque de una nueva etapa, conocida

[9] María Álvarez Caro, *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital* (Madrid: editorial Reus, 2015), 34.

en los libros de historia como “Revolución Francesa”[10] El profesor Pérez Luño afirma que es tras este contexto social y político que se inicia el proceso de “positivación”[11] de los derechos naturales, bajo la fórmula moderna de “los derechos subjetivos”[12] pretendiéndose así, elaborar un instrumento técnico para la protección de los intereses patrimoniales de los particulares, y en especial, de la propiedad. En palabras del profesor Luño nos explica *“si atendemos a su origen histórico resulta indiscutible que la aparición del concepto de intimidad se halla estrechamente ligada al nacimiento de la burguesía”.*[13] En este sentido la intimidad se configuró como la aspiración de la burguesía de acceder a lo que antes había sido privilegio de unos pocos; de ahí que los caracteres, que desde sus inicios van conformando la idea moderna de intimidad se hallen estrechamente vinculados a las necesidades y a la propia ideología de la clase social que la reclama.

De este modo la propiedad es la condición para acceder a la intimidad y la idea burguesa de intimidad está pensada para su disfrute por grupos selectos sin que, en consecuencia, exista una inquietud para hacerla llegar a los estratos más humildes de la población; por ello, el nacimiento de la intimidad, que cronológicamente coincide con la afirmación revolucionaria de los derechos del hombre, no supuso en la sociedad burguesa la realización de una exigencia natural de todos los hombres, sino la consagración del privilegio de una clase.

---

[10] *Surgido en Francia pero con un impacto que traspasó fronteras, alcanzando otras naciones europeas. Enfrentó a defensores y detractores del sistema conocido como Antiguo Régimen. Se inició con la autoproclamación del Tercer Estado como Asamblea Nacional en 1789 y finalizó con el golpe de estado de Napoleón Bonaparte en 1799.* Álvarez, *Derecho al olvido en internet,* 34 (Véase la nota 4).

[11] Refiriéndose a la incorporación de éstos al Derecho Positivo; es decir, escrito.

[12] Son las facultades y poderes concretos atribuidos a un titular, a cuyo arbitrio se remite su ejercicio.

[13] Citado por Ruiz, “La Configuración Constitucional", 7 (Véase la nota 4).

1.4. Ordenamiento Jurídico Ingles (Derecho Anglosajón)

Durante los siglos XVI y XVIII tendrá especial importancia el reconocimiento de los derechos en el ordenamiento jurídico inglés. *La Petition of Rights* -*Petición de Derechos*- de 1628, el *Bill of Rights -Declaración de Derechos*- de I689, y el *Act of Settlement* -El Acta de Establecimiento- de 1701 son algunos de los textos más relevantes.[14] Todos ellos tienen el nexo común de limitar las prerrogativas del monarca, creando un sentimiento racional que los derechos que al hombre pertenecen son legítimas aspiraciones del ciudadano.

1.5. El Derecho de Privacidad (The right of privacy)

El derecho a la vida privada como se le conoce en el Common Law norteamericano,[15] tiene su punto de partida en 1890, cuando dos abogados de Boston Estado Unidos, Samuel D. Warren y Louis Brandeis, escribieron un ensayo titulado The right to privacy -El Derecho de Privacidad-, publicado en el Harvard Law Review una revista de derecho publicada por un grupo independiente de estudiantes de la Escuela de Leyes de Harvard, que se reconoce al derecho de intimidad como un derecho autónomo.

El origen de este derecho, está marcado por el conflicto con el derecho a la

[14] Álvarez, *Derecho al olvido en internet*, 38 (Véase la nota 9). La Petición de Derechos de 1628 fija garantías concretas para los súbditos, garantías que el Rey tiene prohibido violar, contenía restricciones o limitaciones sobre impuestos no establecidos por el Parlamento, entrada forzada de soldados en casas particulares de civiles, encarcelamiento sin causa y restricciones en el uso de la Ley marcial; por otra parte la Declaración de Derechos de 1689 estableció limitaciones a los poderes de la corona y se establecen los derechos del Parlamento y las normas para la libertad de expresión en el Parlamento, la exigencia de elecciones regulares al Parlamento y el derecho de petición ante el monarca y sin temor a represalias; y por último El Acta de Establecimiento o Ley de Instauración de 1701 no sólo regula la sucesión al trono, sino también previene otras cosas importantes, como: establece que los jueces pueden ser censurados por las dos cámaras del Parlamento y que ninguna censura puede ser perdonado por el Monarca.

[15] Derecho común de los Estados Unidos de América. Es un sistema jurídico en que la ley suprema es la Constitución, las leyes aprobadas por el Congreso y los tratados forman la base para las leyes federales en los cincuenta estados y otros territorios del país.

información y específicamente con la libertad de expresión, ya que Samuel D. Warren, fue casado con la hija de un conocido Senador de la República y debido a esto, fue objeto de comentarios acerca de su vida privada; razón por la cual decidió asociarse con Louis Brandeis, para escribir un ensayo que desarrollara el tema de la vida privada y la necesidad de protegerlo frente a la intromisión de la prensa.

En el ensayo, los autores desarrollaron el concepto *to be let alone* -para ser dejado solo-, es decir, el derecho a la soledad, el derecho a vivir en paz, el derecho a no sufrir interferencias, ni del Estado ni de terceras personas, en asuntos que sólo corresponden a la esfera de su privacidad.[16]

El concepto de *privacy* -privacidad- ha ido ampliándose de una manera sorprendente, merced a la jurisprudencia de la Corte Suprema, y para darse una idea del alcance del *right of privacy* -derecho de privacidad- en Estados Unidos, hay que tener en cuenta que abarca desde la mera tutela del domicilio y en general la esfera inmaterial de la persona en todo lo que desea tener reservado, hasta la misma propiedad privada, además de ello los juristas norteamericanos han introducido una nueva acepción de la *privacy*. Se trata de *la privacy of autonomía o informational privacy* -privacidad de la autonomía o privacidad informativa-, con la que se intenta señalar el atentado a la persona perpetrado por la simple recogida y catalogación de informaciones, nueva modalidad que se une al concepto tradicional de *privacy of disclosure* -privacidad de la divulgación-, en el que se engloban los atentados provocados por la difusión y revelación de noticias y datos personales cuyo conocimiento está limitado a un círculo restringido;[17] esto

[16] Hernández, "El Derecho a la Intimidad Personal", 29-31 (Véase la nota 6).
[17] Humberto Nogueira Alcalá, "Tópicos constitucionales sobre la vida privada y la libertad de información ante la informática en Chile", 6. goo.gl/34BvjR.

debido a la facilidad de interferir en la vida de los demás. Y esto es así, entre otras razones, por el desarrollo tecnológico, el cual ha motivado una evolución jurisprudencial y doctrinaria del objeto de estudio.

1.6. Evolución y protección del derecho a la intimidad en El Salvador

La historia del derecho a la intimidad en El Salvador, es reciente, en razón que hace 33 años exactamente fue reconocido y tutelado de forma expresa en la Constitución de la República de El Salvador de 1983, en el artículo 2 inciso 2, que establece: *"…Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen…"* Además de ser reconocido constitucionalmente, fue tutelado penalmente, es decir, que el art. 2 inc.2 Cn., dio origen a que se incorpore en el Código Penal de 1997 un capítulo nuevo, en donde se agrupan los delitos relativos a la Intimidad, específicamente está ubicado en el Libro Segundo, Parte Especial: de los Delitos y sus Penas, Título VI: Delitos relativos al Honor y la Intimidad, Capítulo II: De los Delitos relativos a la Intimidad, artículos 184 al 190 del Cpn.

Establecerlo de esta forma resulta fácil, pero para llegar a este punto, en donde el legisferante establece de forma expresa el reconocimiento y la tutela penal del derecho a la intimidad, no lo es, ya que el derecho a la intimidad ha tenido un recorrido extenso en el transcurso del tiempo, fue regulada y tutelada de forma análoga a otras garantías.

1.7. Base Constitucional del Derecho a la Intimidad

Tal como se enunció en el apartado anterior, el derecho a la intimidad como garantía constitucional, fue reconocido en la Constitución de la República de El Salvador de 1983, pero previo a esta, existieron garantías constitucionales

que trataban de regular la intimidad; para ello se analiza la legislación salvadoreña, en dos dimensiones, la primera como un estado federado y la segunda como estado independiente.

1.7.1. Constituciones Federales de Centro América

1.7.1.1. Constitución de la República Federal de Centroamérica de 1824

Estableció dos garantías,[18] la primera regulada en el artículo 168 donde se estableció que ninguna casa podía ser registrada, sin mandato escrito de autoridad competente, la segunda regulada en el artículo 169 determino que los papeles de los habitantes de la República solo podían ser utilizados en los Delitos de traición, cuando fueran indispensables para la averiguación de la verdad y que tuvieran relación con lo que se indagaba.

1.7.1.2. Constitución de la República Federal de Centroamérica 1835

Reconoció dos garantías análogas a la intimidad, la primera regulada en el artículo 173 manifestaba que ninguna casa podía ser registrada, sin mandato escrito de autoridad competente, la segunda regulada en el artículo 175 que estableció que era inviolable el secreto de las cartas, y las que sustraían de las oficinas de correos o de sus conductores no producían efecto legal, ni podían presentarse en testimonio contra ninguno.[19]

1.7.1.3. Constitución Política de los Estados Unidos de Centroamérica de 1898

Estableció dos garantías, la primera en el artículo 30 referente a la

[18] Miguel Ángel Gallardo, *Cuatro Constituciones Federales de Centro América y las Constituciones Políticas de El Salvador* (San Salvador: Trip. La Unión, 1945).
[19] Ibíd.

inviolabilidad de la correspondencia epistolar y telegráfica, y a la correspondencia interceptada que no haría fe, ni podría figurar en ninguna especie de actuación; y la segunda en el artículo 31 en donde se estableció que el domicilio es inviolable y no podrá decretarse allanamiento, salvo para la averiguación de los delitos o en persecución de delincuentes, siempre que estén determinados por la ley.[20]

1.7.1.4. Constitución Política de la República de Centroamérica de 1921

Reconoció tres garantías, la primera en el artículo 53 donde se establece la inviolabilidad de la correspondencia epistolar, la telegráfica y los papeles privados, la segunda en el artículo 54 determino que la correspondencia particular, papeles y libros privados, solo podían ocuparse o inspeccionarse por la autoridad competente y en los casos establecidos por la ley, y la tercera en el artículo 56 referente a la inviolabilidad del Domicilio, y que solo podrá decretarse allanamiento por la autoridad y en los casos establecidos por la ley.[21]

1.7.2. Constituciones Políticas de El Salvador

1.7.2.1. Constitución del Estado del Salvador de 1824

La manifestación de protección del derecho a la intimidad en la legislación salvadoreña, se encuentra primeramente en la Constitución del Estado del Salvador de 1824, como Estado Federado.[22] Según el artículo 66 la protección de la casa, libros y correspondencia fue sagrado, y no se permitía que tercero o que autoridades interfirieran o registraran las propiedades anteriores salvo si así lo ordenaba la ley.

---

[20] Ibíd.
[21] *Constituciones de la República de El Salvador 1824-1962*, Tomo II A, Primera Parte (San Salvador, El Salvador: UCA Editores, 1993).
[22] Ibíd.

1.7.2.2. Constitución del Estado del Salvador de 1841; 1864 y 1871

Los constituyentes protegen la intimidad de los ciudadanos, aunque no de una forma directa, sino en sus manifestaciones el Art. 84 Cn., protegía la correspondencia epistolar manifestando la inviolabilidad de ésta, salvo requisitos o excepciones que la misma ley estableciera. Asimismo las constituciones de 1864 (artículo 90), Constitución de 1871 (artículo 116), siguen refiriéndose a la misma garantía que la constitución de 1841.[23]

1.7.2.3. Constituciones de los años 1872; 1880; 1883; 1885; 1886 y 1939

Regularon la inviolabilidad de la correspondencia epistolar y telegráfica estableciendo que esta no podía interceptarse ni abrirse, salvo en los casos establecidos por la ley ni revelarse, y la que fuera interceptada no presta fe en juicio ni fuera de él. Las Constituciones de los años de 1880, 1883, 1885, 1886 y la de 1939, en los artículos 30, 28, 30, 30 y 49 respectivamente.[24]

1.7.2.4. Constitución de los años 1939 y 1945

La constitución de 1939 adopta por primera vez, y de forma clara la protección del domicilio (artículo 38 inciso 2º), por su parte la Constitución de 1945 (artículo 21 inciso 2º), establece que el domicilio es inviolable y solo podrá decretarse allanamiento, para la averiguación de los delitos, persecución de delincuentes o para fines sanitarios, en la forma y los casos determinados por la ley asimismo resguarda la inviolabilidad de la correspondencia que regulo en el Art. 30, retomando el texto de la Constitución de 1886.[25]

---

[23] Ibíd.
[24] Ibíd.
[25] ibíd.

1.7.2.5. Constitución de 1950 y 1962

La Constitución de 1950 regula en el artículo 165 que la morada es inviolable y solo podrá decretarse allanamiento en caso de incendio u otros análogos, para la averiguación de los delitos, y persecución de delincuentes y para los fines sanitarios, en la forma y circunstancias que determine la ley, esto se inicia hasta antes de la reforma, que se reproduce en la Constitución de 1962, regulando el texto en el mismo artículo 159, donde establecía la inviolabilidad de la correspondencia, pudiendo ser interceptada solo en casos de concurso y quiebra. También se cambian el concepto de domicilio por el de "morada" por ser este más amplio, así regularon también la inviolabilidad de la morada en el mismo artículo 165.[26]

1.8. La intimidad como bien jurídico protegido por el derecho penal

En la historia salvadoreña, aparecen seis códigos penales, que desde 1826, año del primero, han sido instrumentos de control social, expresión del Ius puniendi del Estado. Siendo la regla que una garantía constitucional, siempre lleva emparentada una protección penal, por ello el Código Penal de 1997, regula un capítulo nuevo, en donde se tipifican los delitos relativos a la intimidad, pero previo a esta tipificación especifica de la intimidad, existieron tipos penales que trataron de tutelar la intimidad de las personas, es así que en los códigos de 1904 y 1973 se lograron dar matices de lo que se consideraba privado.

El Código Penal de 1904, logro tipificar el "Allanamiento de morada" (artículo 445: el particular que entrare en morada ajena contra la voluntad de sus morador...); asimismo el "Descubrimiento y revelación de secretos" (artículo

[26] Ibíd.

452: el que para descubrir los secretos de otro se apoderare de sus papales o cartas y los divulgare…).

Código Penal de 1973, regulo "la inviolabilidad de morada y lugar de trabajo (artículo 228); así mismo se tipifico la "Violación de correspondencias y Comunicaciones Privadas" (artículo 231).

Como se ha visto hasta antes de 1983 en las constituciones y los códigos penales, el Derecho a la Intimidad era enfocado únicamente al aspecto de la inviolabilidad de la morada, correspondencia y revelación de secretos, con la entrada en vigencia de la Constitución de 1983, se contempla un concepto de intimidad no restringido a la morada, siendo necesario ampliar el ámbito de protección, ya que con la propagación de la informática en el ámbito de la comunicaciones se genera un nuevo ámbito de vulneración para este Derecho, en razón de lo anterior, se vuelve necesario dedicar algunos apartados a la informática.

1.9. Antecedentes históricos de la informática

Desde la antigüedad, y la mayoría de las veces de forma inconsciente, el hombre ha tratado de reducir al máximo su trabajo, para ello es que se inventaron las herramientas y las máquinas, y con ayuda de estos dispositivos el hombre disminuye la necesidad de esfuerzo físico y se dedica a funciones superiores, como son la puesta en marcha y control de las operaciones a realizar por los instrumentos antes citados.

Paralelamente al desarrollo de las herramientas y las maquinas, 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

física o mental previamente programada, aplicada a los procesos industriales, su fin es suprimir el eslabón hombre en la cadena de producción, se pretende llegar a la fábrica automática en la cual las maquinas regulan su propio comportamiento, desde el principio hasta el fin de la producción.

La informática puede considerarse como la ciencia y tecnología aplicada a la automatización del razonamiento y del tratamiento de la información, puede decirse 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 cálculo.[27]

Por lo tanto, al describir los inicios de la informática es imprescindible hablar de los inicios de las computadoras ya que estas son la base de la informatización, es así que el ser humano desde tiempos antiguos tuvo la necesidad de contar, sumar, restar, multiplicar y dividir, siendo este el medio para poder sobrevivir.

1.9.1. Evolución de las computadoras

Al tratar del origen de las computadoras debemos remontarnos hacia la edad antigua, siendo el ábaco el primer instrumento matemático para poder efectuar las operaciones aritméticas supra descritas, estaba basado en un sistema numérico de diez unidades debido a que fueron primero los diez dedos de la mano lo que sirvió en su entonces para poder sobrellevar aquellas complicados datos aritméticos.

[27] Alberto Prieto Espinosa et al., *Introducción a la Informática* (Madrid: McGraw-Hill/ interamericana de España, 2002), 56.

A partir del ábaco, se empezaron a desarrollar nuevos instrumentos para simplificar las operaciones matemáticas y se desarrolló la primera calculadora mecánica siendo su creador el inventor francés Blaise Pascal en el año de 1642 D.C., dándose a tal máquina, en su honor, el nombre de “pascalina”; posterior a ello era necesario tener algunas bases de datos o información resguardada en algún medio de fácil acceso, siendo así que en el año 1801 otro francés Joseph Marie Jacquard, quien poseía un taller de telas y que tenía necesidad de crear nuevos patrones de tela, creo la Tarjeta Perforada siendo este el inicio de almacenamiento de información por medio de orificios.

Tanto la pascalina como las tarjetas perforadas son el germen de las actuales computadoras, distinguiendo dentro de la evolución de estas, cinco tipos de generaciones de computadoras.[28]

1.9.1.1. La Primera generación, 1951 a 1958 bulbos al vacío

Las computadoras de la primera Generación emplearon bulbos para procesar información. Los operadores ingresaban los datos y programas en código especial por medio de tarjetas perforadas. El almacenamiento interno se lograba con un tambor que giraba rápidamente, sobre el cual un dispositivo de lectura y escritura colocaba marcas magnéticas. Esas computadoras de bulbos eran mucho más grandes y generaban más calor que los modelos contemporáneos.

1.9.1.2. Segunda generación, 1959-1964 Transistores

El invento del transistor hizo posible una nueva Generación de computadoras, más rápidas, más pequeñas y con menores necesidades de

[28] Ibíd.

ventilación. Sin embargo el costo seguía siendo una porción significativa del presupuesto de una compañía. Las computadoras de la segunda generación también utilizaban redes de núcleos magnéticos en lugar de tambores giratorios para el almacenamiento primario. Estos núcleos contenían pequeños anillos de material magnético, enlazados entre sí, en los cuales podían almacenarse datos e instrucciones.

1.9.1.3. Tercera generación, 1964-1971 Circuitos Integrados

El desarrollo de los circuitos integrados trajo aparejado el desarrollo de la tercera generación de las computadoras, en los cuales se colocaban miles de componentes electrónicos, en una integración en miniatura, lo que las hacía más pequeñas, más rápidas, generaban menos calor y eran energéticamente más eficientes.

1.9.1.4. Cuarta generación, 1971 a 1981 Microprocesador, Chips de memoria

Es en esta etapa que aparecen los microprocesadores que es un gran adelanto de la microelectrónica, los cuales consisten en circuitos integrados de alta densidad y con una velocidad impresionante. Las microcomputadoras con base en estos circuitos son extremadamente pequeñas y baratas, por lo que su uso se extiende al mercado industrial. Aquí nacen las computadoras personales que han adquirido proporciones enormes y que han influido en la sociedad en general sobre la llamada "revolución informática"

1.9.1.5. Quinta generación, 1982 a la fecha Desarrollo del software

La acelerada marcha de la microelectrónica forzó el desarrollo del software y los sistemas con que se manejan las computadoras. Dejando el avance que se tenía hasta la cuarta generación -en relación al hardware-, hoy se habla

ya de computadoras cuánticas, Inteligencia artificial, robótica, sistemas expertos, redes de comunicación, entre otros.

Con la creación de las computadoras y la aplicación de estas a las telecomunicaciones, fue necesaria la creación de un mecanismo que facilitara el tráfico de información, logrando que la distancia no constituyera impedimento a efecto de transferir grandes cantidades de información, siendo así que en un primer momento se creó una red para fines militares denominada ARPA,[29] como respuesta a la necesidad de esta organización de buscar mejores maneras de usar los computadores de ese entonces, pero enfrentados al problema de que los principales investigadores y laboratorios deseaban tener sus propios computadores, lo que no solo era más costoso, sino que provocaba una duplicación de esfuerzos y recursos, idea que originó el desarrollo de lo que actualmente denominamos internet.

1.9.2. Internet

La historia del Internet se remonta al año de 1962, creando una serie de memorándum escritos por Joseph Carl Robnett Licklider, también conocido como J.C.R. Licklider, quien posteriormente se convirtió en la cabeza del programa de investigación de computación de la Agencia de Investigación Avanzada de Proyectos del Departamento de Defensa de los Estados Unidos institución que dio desarrollo al Internet, y cuyo propósito principal era la investigación y desarrollo de protocolos de comunicación.[30]

Internet surgió hace ya varias décadas, gracias al esfuerzo de interconectar la red de la Agencia de Proyectos de Investigación Avanzada o como se

[29] Agencia de Investigación de Proyectos Avanzados, y que hoy se conoce como DARPA, siglas en inglés de Defense Advanced Research Projects Agency.
[30] Aníbal Alejandro Pardini, *Derecho de Internet* (Buenos Aires: La Rocca, 2002).

conoce en inglés Advanced Research Projects Agency Network[31] del Departamento de Defensa Estadounidense con varias redes enlazadas por medio de satélite y de radio. En el modelo ARPANET, la comunicación ocurre entre una computadora fuente y un destino, por lo tanto, las computadoras que se comunican deben asegurarse que la comunicación 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 DARPA.[32]

Si bien es cierto, la idea original estaba intrínsecamente ligada a la seguridad militar, su evolución e implementación tuvieron lugar alrededor del mundo académico y es que la misma red en experimentación sirvió para conectar a los científicos desarrollándola y ayudarlos a compartir opiniones, colaborar en el trabajo y aplicarla para fines prácticos. Pronto, ARPANET conectaría todas las agencias y proyectos del Departamento de Defensa de los Estados Unidos de América y para 1972 se habían integrado ya 50 universidades y centros de investigación diseminados en los Estados Unidos.

Eventualmente 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.[33]

Fue recién en 1990 que Internet comenzó a llegar a la población en general. Este año, el ingeniero inglés Tim Bernes Lee desarrolla la World Wide Web, permitiendo el uso de una interfaz gráfica y la creación de sitios más

[31] Hoy denominada como Agencia de Proyectos de Investigación Avanzados de Defensa o DARPA.
[32] Ed Krol, *Conéctate al mundo de Internet: Guía y Catálogo* (México: McGraw-Hill, 1995).
[33] Breve Historia del Internet. Glosario Web, goo.gl/eR2lFH.

dinámicos y visualmente interesantes. Para facilitar la navegación a través de Internet, hubo múltiples navegadores como, por ejemplo, Microsoft Internet Explorer y Netscape Navigator. La aparición de los proveedores de acceso y servicios en línea portales contribuyeron a este crecimiento.

El Internet es utilizado por varios segmentos sociales, como por ejemplo los estudiantes comenzaron a buscar información para la investigación de la escuela, mientras que los jóvenes lo usaron por pura diversión en los juegos online, las salas de chat se convirtieron en puntos de encuentro para una charla virtual en cualquier momento, los desempleados están buscando empleos a través de las agencias de empleo o sitios de envío de currículos por correo electrónico, la transferencia de datos se hizo de manera casi automática entre computadoras; mientras que por su parte, las empresas encuentran en Internet una excelente manera de mejorar sus ganancias y aumentar las ventas en línea, convirtiendo a Internet en centros comerciales virtuales. En la actualidad, es imposible pensar en el mundo sin Internet, ya que esta tomó parte de los hogares de personas alrededor de todo el mundo, de manera tal que estar conectado al mundo Wide Web se ha convertido en una necesidad de extrema importancia.

1.10. Las primeras computadoras en El Salvador

International Business Machines o conocida por sus siglas IBM, fue una empresa que buscó socios o aliados de negocios en el mercado salvadoreño, es así que en el año de 1962 la empresa La Constancia Sociedad Anónima fue posiblemente la primera en comprar una computadora IBM modelo 1401. Desde ese instante las computadoras en el país han pasado por una cadena evolutiva desde aquellas que fueron importadas para empezar a tener las primeras bases de datos tal y como lo demostró la Universidad Centroamericana José Simeón Cañas adquiriendo la

computadora HP-1000 modelo 21mx para llevar el registro académico. Hasta lo que se conoce como los servidores o estaciones de trabajo.[34]

1.11. Internet en El Salvador

A principios de 1990 en El Salvador la Administración Nacional de Telecomunicaciones, no satisfacía la demanda de abonados. Los salvadoreños debían esperar hasta una década para que les fuera asignada una línea telefónica. Los números de teléfono se consideraban activos fijos y era común encontrar en los clasificados de los periódicos anuncios de compra y venta de líneas telefónicas por miles de colones. Por ello la responsabilidad de conectar a El Salvador a Internet no fue atribuida enteramente al estado, el primer país de Centroamérica en conectarse a Internet fue Costa Rica en 1993. El Salvador pocos meses después dio los primeros pasos para conectarse a Internet.

En septiembre 1994 las universidades, la Fundación Salvadoreña para El Desarrollo Económico y Social, el Consejo Nacional de Ciencia y Tecnología "CONACYT" y Administración Nacional de Telecomunicaciones formaron la Asociación SVNET.[35] Ese mismo año el 4 de noviembre El Salvador obtuvo el domino ".sv" que distinguiría a los sitios salvadoreños de los demás. Continuando con el proceso acordaron con la empresa de datos UUNET (hoy Verizon Business) la transmisión de datos desde y hacia El Salvador.

En diciembre de 1994 se hicieron las primeras pruebas del servicio de correo electrónico y en marzo de 1995 se comenzó a ofrecer el servicio de correo electrónico al público con la terminación "@es.com.sv". Al principio el envío de correos no era instantáneo; el servidor salvadoreño se conectaba cada

[34] José Rivas. *Historia de la Computación en El Salvador*, goo.gl/lx49kj.
[35] Véase: goo.gl/2uYXon.

media noche con los servidores de UUNET para sincronizar los correos entre El Salvador y Estados Unidos.

Las primeras conexiones dedicadas a Internet se establecieron con la ayuda del proyecto la Red Hemisférica Universitaria de Ciencia y Tecnología de la Organización de los Estados Americanos. Estas conexiones dedicadas se establecieron con las empresas de telecomunicaciones SPRINT y RACSA. Permitiendo que los primeros sitios web se alojaran en servidores ubicados en el país, ya que los pocos sitios web salvadoreños que existían antes de 1996 utilizaban servidores ubicados en Estados Unidos.

La Universidad de El Salvador, la Universidad Centroamericana José Simeón Cañas, CONACYT y la Universidad Don Bosco fueron de las primeras en tener estos enlaces dedicados a Internet. En la segunda fase del proyecto se conectaron más instituciones de gobierno. En 1996 Internet aún no era tecnología para las masas, su fin era más que todo científico tal como se puede apreciar en la misión de la Red Hemisférica Interuniversitaria Información Científica y Tecnológica: "Conectar a las instituciones de los países miembros al internet, para integrar una red electrónica de intercambio de información científica y tecnológica entre catedráticos, investigadores y especialistas de las universidades de los países miembros".[36]

[36] *Historia del Internet en El Salvador*, goo.gl/R6txw3.

CAPÍTULO II
FUNDAMENTOS TEÓRICOS DEL DERECHO A LA INTIMIDAD Y DE LA INTRUSIÓN INFORMÁTICA

El propósito del presente capitulo, es brindar un soporte teórico que permita entender los términos Intimidad e Informática, estableciendo su definición, naturaleza, características y todo los elementos que los componen.

Esta era es conocida como la “sociedad de la información”, esto debido al desarrollo de avances tecnológicos y científicos que tiene la informática, entiéndase la informática como la disciplina o actividad que consiste en el tratamiento, almacenamiento, y procesamiento automatizado de la información, por medio de cualquier aparato electrónico que tenga como objetivo la obtención y facilitación de la información;[37] cuyo uso inadecuado y sin control puede vulnerar derechos de rango constitucional, ya que esta al usarse de manera negativa se vuelve perniciosa, para el individuo y la sociedad en general, considerando que la información al estar almacenada y ordenada mediante aparatos informáticos, se vuelve fácil para que terceros puedan sustraer datos de la esfera privada de un individuo.

De esta guisa se desprenden dos conceptos, la Intimidad y la Informática, son precisamente estas las piezas claves de esta investigación, por lo que surge la necesidad de hacer un abordaje doctrinario de cada uno de los

[37] El desarrollo tecnológico y el avance de las telecomunicaciones han obligado a los Estados a desarrollar una legislación con el fin de proteger, garantizar y respetar la intimidad de los seres humanos. Benjamín Constant afirmaba que: *"hay una parte de la existencia humana que, necesariamente, tiene que mantenerse individual e independiente y que queda, por derecho, fuera de toda competencia social". Citado por* José Pablo Cabrera Moreira, "Los límites de la actuación de la prensa en relación con la administración de justicia en el ámbito penal" (Tesis Doctoral, Universidad Nacional de Loja, Ecuador. 2013), 8.

elementos que componen dichos términos.

2. Conceptualización y definición del derecho a la intimidad

Se dice que la intimidad es una necesidad humana y un derecho natural del hombre por lo que es independiente y anterior a su regulación positiva, si bien la noción de intimidad implica una gran variedad de perfiles y criterios en ocasiones difusos y difíciles de precisar, lo cual lleva a la conclusión de que no existe una definición unívoca válida en torno a la cual haya unanimidad, sino que su concepto es más fluctuante y dependiente del medio social y cultural, se intentará dar una definición de la misma teniendo en cuenta algunos puntos comunes de la doctrina entorno a ella.

La raíz de la palabra intimidad se encuentra en intimus, la cual se traduce del latín por íntimo, el más íntimo, encontrando que su procedencia deriva del adverbio intus, traducido "por dentro" o "hacia adentro"[38] y que es utilizada, en principio para referirse al ámbito más profundo, inherente y reservado de la personalidad del ser humano, pero, por extensión, también al ámbito de la vida familiar y asociativa que tenga la misma particularidad de interioridad y reserva; desde esta etimología se dice que la intimidad, está vinculada a lo secreto, a lo que se quiere mantener fuera del alcance del conocimiento ajeno, bien sea de la vida privada en la esfera individual, familiar o incluso social de la persona humana.

En ese sentido el diccionario de la Lengua Española de la Real Academia Española, la palabra intimidad es definida en los siguientes términos: *"f. Amistad íntima; f. Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia".* Definición que no logra aclarar el

[38] Norberto González Gaytano, *El Deber del Respeto a la Intimidad* (España: Universidad de Navarra, 1990), 17.

termino en mención,[39] el concepto de intimidad es asumido por la mayoría de la doctrina como sinónimo de privacidad o de vida privada, entendiendo entonces que abarca los diversos actos, situaciones y circunstancias que por su carácter personalísimo no deben, salvo el consentimiento de la persona afectada o por razones legítimas, estar expuestos a la curiosidad y a la divulgación, sino salvaguardados de la injerencia extraña, al ser uno de los valores que en toda sociedad democrática debe tener el hombre para ser el auténtico dueño de su núcleo jurídico personalísimo.[40]

Para Ana Isabel Herrán, quien señala al respecto *"…consiste en un conjunto de facultades del individuo para desenvolverse sin lesionar derechos ajenos y también en un poder de exclusión del conocimiento ajeno de su vida íntima y familiar"*.[41]

Nahím Emén, manifiesta en relación al derecho de intimidad lo siguiente: *"consiste en la facultad que tiene cada persona de disponer de una esfera, ámbito privado o reducto infranqueable de la libertad individual, el cual no puede ser invadido por terceros ya sean particulares o el propio Estado, mediante cualquier tipo de intromisiones, las que pueden asumir muy diversos signos".*[42]

En líneas jurisprudenciales la Sala de lo Penal maneja el concepto de intimidad como "*aquel derecho humano por virtud del cual la persona tiene el poder de excluir a las demás del conocimiento de su vida personal, sentimientos, emociones, datos biográficos y personales e imágenes y tiene,*

[39] Diccionario de la lengua española, goo.gl/3RE2vx.
[40] Mario Madrid Malo Garizábal, *Derechos Fundamentales* (Bogotá, 1997), 200.
[41] Ana Isabel Herrán Ortiz, *El derecho a la intimidad en la Nueva Ley Orgánica de Protección de datos personales* (Madrid: edit. Dykinson, 2002), 25.
[42] Citado por Santiago Velásquez Velásquez. "El Derecho a la Intimidad y la Competencia Desleal", *Universidad Católica de Santiago de Guayaquil,* (2006), 8, goo.gl/lSN8pi.

además, la facultad de determinar en qué medida esas dimensiones de la vida personal pueden ser legítimamente comunicadas a otras".[43]

Asimismo la Sala de lo Constitucional manifiesta que este derecho pertenece a la categoría de derecho fundamental que han sido positivadas en el texto constitucional, gozando asimismo de la supremacía y la protección reforzada de las que goza la propia Constitución, lo cual desarrolla una función de fundamentación material de todo el ordenamiento jurídico; y que hace referencia "*al ámbito que se encuentra reservado ad intra de cada persona (...) y cuyo conocimiento importa únicamente a éste y en su caso, a un círculo concreto de personas seleccionadas por el mismo. Por tanto, en dicho ámbito opera la voluntad del individuo para disponer de todos aquellos aspectos que puedan trascender al conocimiento de los demás".*[44]

Ciertamente el Derecho a la Intimidad es el Derecho fundamental del siglo XXI, y que, como afirma Álvarez Cienfuegos, *"si no hay intimidad no habrá nada";* donde no se protege la intimidad no se protegen otros muchos derechos. Por eso se dice que es un derecho raíz, pues funda, alimenta y da razón de ser a otros muchos.[45] Verbigracia jurisprudencia en el que este derecho es manejado como derecho fundamental, teniendo la facultad de elegir que mostrar a terceros, y aunque este derecho en las conceptualizaciones que anteceden se limita únicamente al individuo y a aspectos que no trascienden del concepto tradicional de la no intromisión en la vida privada, esto en los últimos años ha cambiado, a tal grado que hoy es muy difícil de definir con precisión, pues tiene connotaciones diversas

[43] Recurso de Casación, Sala de lo Penal, *Referencia 478-CAS-2004* (El Salvador, Corte Suprema de Justicia, 2005), 4, goo.gl/kNlzWW.
[44] Sentencia de Hábeas Corpus, Sala de lo Constitucional, *Referencia 135-2005AC* (El Salvador, Corte Suprema de Justicia, 2008), 8, goo.gl/jsHAIt.
[45] Citado por Carmen Sánchez Carazo, *La intimidad: un derecho fundamental de todos,* goo.gl/gFDtF.

dependiendo de la sociedad de que se trate, ya que este afecta a las esferas más profundas de la personalidad y junto a un componente estable y permanente, ofrece también otros factores cambiantes fruto de la coyuntura; sin embargo, dentro de ese derecho se pueden considerar las relaciones personales y familiares, afectivas y de filiación, las creencias y preferencias religiosas, convicciones personales, inclinaciones políticas, condiciones personales de salud, identidad y personalidad psicológica, inclinaciones sexuales, comunicaciones personales privadas por cualquier medio y herramienta electrónica, situación financiera personal y familiar, información en bases de datos, entre otros, como aspectos que no están destinados a trascender e impactar a la sociedad de manera directa y donde en principio los terceros no deben tener acceso alguno, siempre que las actividades que en ella se desarrollan no sean de su incumbencia, ni afecten y pongan en riesgo los intereses de los demás ciudadanos.

2.1. Distinción entre Honor, Privacidad, Propia imagen, Intimidad familiar y personal

El Derecho de Intimidad es muchas veces utilizado como sinónimo, cometiendo el yerro de equipáralo con muchos otros conceptos y derechos, siendo el caso más frecuente de los términos y derechos que se proponen en este apartado.

2.1.1. Honor

Se acostumbra a distinguir dos clases de honor que es el subjetivo y el objetivo,[46] el honor subjetivo consiste en el sentimiento de aprecio que una persona tiene de sí misma, y el honor objetivo consiste en la reputación,

[46] Sentencia de Amparo, Sala de lo Constitucional, *Referencia 227-2000* (El Salvador, Corte Suprema de Justicia, 2001), 8; y Sentencia de Amparo, Sala de lo Constitucional, *Referencia 494-2001* (El Salvador, Corte Suprema de Justicia, 2002), 3.

fama o buen nombre de los que goza un individuo frente a los otros. Así también se sabe que la Constitución acoge los conceptos jurídicos de dignidad y honor, reconociendo a los mismos como conceptos fundamentales que posibilitan la convivencia humana en un Estado de Derecho.

"…La definición de honor no se presta fácilmente para una conceptualización abstracta; es preferible, a la hora de definirlo, mantener viva la maleabilidad social que lo caracteriza. Dicho de otra manera, para su definición habrá de considerar siempre las reglas culturales asumidas por el conjunto del cuerpo social. En ese sentido, se ha llegado, incluso, a considerar que el honor es un concepto jurídico indeterminado, que necesariamente obliga al intérprete a acudir a la valoración social...".[47]

Los Derechos honor e intimidad, son próximos, pero no coincidentes, el honor está vinculado con la participación del individuo en la sociedad, en la intimidad lo que se pretende, a contrario sensu es garantizar un ámbito de no intervención activa en la vida social, bien a través de asegurar la falta de información, o mediante el control sobre dicha información.

Novoa Monreal hace distinción entre el honor y la intimidad, partiendo de los perjuicios que le puede ocasionar a esta dualidad de derechos. Así, el atentado en contra de la vida privada no exige ni supone que quien lo ejecuta formule un juicio adverso o se proponga un rebajamiento moral de su víctima, ya que es suficiente con que, en virtud de injerencia indebida, tome conocimiento de aspectos reservados de la vida de una persona, pudiendo omitir todo gesto o expresión de agravio, porque hasta podría darse el caso

[47] Sentencia de Amparo, Sala de lo Constitucional, *Referencia 375-2011* (El Salvador, Corte Suprema de Justicia, 2015). Considerando IV párrafo 2.A.

de que el atacante de la intimidad aprobara las manifestaciones de la vida privada que ha llegado a conocer, sin que con ello quedará excluida la violación de la misma que ha cometido.[48]

Por el contrario, el atentado en contra del honor no exige ni supone que la expresión, gesto o imputación que se formulan y que lesionan el honor subjetivo o el objetivo, correspondan a una información reservada que el sujeto activo haya logrado sobre su víctima mediante injerencia en su intimidad, porque, perfectamente, pueden concebirse atentados en contra del honor en los que se emplean datos que el sujeto activo conoció legítimamente o en los que se formulan imputaciones que son conocidas desde antes por algunas o por muchas personas. Para esta clase de atentados, basta el agravio intencionado a la estimación propia o ajena de la víctima, sin que sea necesario que el hecho que se emplea para agraviar pertenezca a la vida privada.

Se puede expresar la diferencia sintéticamente, diciendo que lo esencial en la intimidad es lo que no incumbe a otras personas, a los terceros, mientras que en el honor lo fundamental es el no verse menospreciado o rebajado ante la opinión pública y ante uno mismo.[49]

2.1.2. Privacidad

El origen de la palabra privacidad se encuentra en el derecho anglosajón en el término *privacy*, en concreto en Estados Unidos de América, en el escrito *right to privacy,*[50] término que se traduce como “derecho a la privacidad”.

[48] Eduardo Novoa Monreal, *Derecho a la Vida Privada y Libertad de Información: un Conflicto de Derechos* (Argentina: siglo veintiuno, 2001), 75.
[49] Ibíd.
[50] Ensayo escrito por Samuel Warren y Louis Brandeis, y publicado en el 1890 Harvard Law Review, primera publicación en Estados Unidos que defendió el derecho a la privacidad.

Se sabe que el derecho a la intimidad protege la parte más íntima de una persona, es decir, esa esfera personal que define qué es y qué no es privado, dicho de otra forma, hablar de intimidad es hablar de sentimientos, de creencias -políticas, religiosas-, pensamientos o de una información, o la relativa a la vida sexual, cuya difusión puede producir ciertas reservas al individuo. Se trata en definitiva de aquellos datos que bajo ninguna circunstancia proporcionaría un individuo de manera libre y consciente.[51]

La privacidad, sin embargo, es un término más amplio, se refiere a aquella parte del individuo que va más allá de lo íntimo, esto es, información que tomada por sí misma puede no ser relevante, pero que analizada en un momento o contexto concreto puede lograrse la construcción de un perfil muy fiable del individuo que permita su caracterización e identificación.[52]

De forma lacónica la Intimidad es el dominio exclusivo de la persona, en cambio, la privacidad es el dominio de la persona que puede ser accesible a otras personas.[53] Sin embargo, la diferencia entre privacidad e intimidad, va más allá de las numerosas discusiones de los diferentes doctrinantes sobre lo particular y lo íntimo, no tiene efectos jurídicos en el ordenamiento jurídico vigente del país, en atención directa a que la protección del derecho a la intimidad constituye parte integrante de su privacidad. Razón por la cual estos conceptos no se sobre ponen, no son excluyentes; sino que por el contrario son complementarios e interdependientes de la existencia humana.

---

[51] Flor María Ávila Hernández et al.**,** "Los Derechos a la Intimidad y a la Privacidad en Venezuela y en el Derecho Comparado"*, Filosofía y Derecho,* Nº 11, 2007/2008, goo.gl/kiZSdd.

[52] ibíd., 2.

[53] Carlos Colautti, hace un distinción semántica, sosteniendo que entre acciones privadas y acciones íntimas, existe una relación de género a especie; por lo que las acciones íntimas son una especie dentro de las acciones privadas, esto porque todas las acciones íntimas son privadas, pero no todas las acciones privadas son íntimas; así por ejemplo la cuenta bancaria es privada.

2.1.3. Propia Imagen

Este derecho, protegido en el Artículo dos de la Constitución de la República, provee al ciudadano la facultad de permitir o no la reproducción, difusión o comercialización de su figura a través de cualquier medio.[54]

En definitiva, lo que se logra inferir en la dimensión constitucional es que los seres humanos son dueños de su imagen, por lo tanto son capaces de permitir o evitar que se haga uso de ella, impidiendo la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad -informativa, comercial, publicitaria, científica, cultural-.

2.1.4. Intimidad Personal y Familiar

Cuando se habla de intimidad por lo general se hace referencia a la intimidad personal, no obstante también la familia como institución goza del Derecho a la Intimidad, es decir, el derecho es entendido en cuanto a miembros de una familia y no en cuanto a personas en si o individuales, es así que el Derecho a la Intimidad se extiende, no sólo a los aspectos de la vida propia personal, sino también a determinados aspectos de otras personas con las que se guarde una personal y estrecha vinculación familiar, aspectos que por la relación o vínculo existente con ellos, inciden en la propia esfera de la personalidad del individuo que los derechos del artículo 2 de la Constitución protegen, así ciertos eventos que pueden ocurrir a padres, cónyuges o hijos

[54] Sentencia de Hábeas Corpus, Sala de lo Constitucional, *Referencia 231-2006* (El Salvador, Corte Suprema de Justicia, 2009). La Sala reconoce dos dimensiones del derecho a la imagen la positiva, que implica la facultad de cada persona natural para obtener la reproducción, de forma recognoscible, de rasgos, facciones o la figura del titular del derecho, reproducirla o publicarla; y la dimensión negativa para impedir tal obtención, reproducción o publicación, con la consiguiente facultad de recabar la protección jurisdiccional frente a terceros, ya sea mediante la adopción de medidas cautelares frente a la amenaza de vulneración, o mediante el reclamo de la consiguiente indemnización por su uso indebido.

tienen, normalmente y dentro de las pautas culturales de la sociedad, tal trascendencia para el individuo, que su indebida publicidad o difusión, incide directamente en la propia esfera de la personalidad.

Sucintamente se han diferenciado los conceptos que tienden a tomarse como sinónimos, concluyendo que dichos Derechos tienen diferentes alcances, pero se ha dejado claro que existe un elemento en común para todo ellos, y es que el derecho origen para todos es la Intimidad, ya que existen elementos comunes y vinculantes entre todos, pues forman parte de la personalidad.

2.2. Características del derecho de intimidad

El derecho a la intimidad, como derecho reconocido constitucionalmente en la legislación salvadoreña, posee las siguientes características:

a. Es Originario e Innato: Se configura con el origen del titular, es decir que le pertenece a la persona desde su nacimiento.[55]

b. Es Absoluto: Por su condición de derecho erga omnes,[56] es decir, ejercitables ante cualquiera. Sin embargo, aunque se caracterice de absoluto no significa que sea ilimitado sino, que limitará las libertades de expresión cuando éstas atenten contra la vida privada del titular.

c. Es Extra patrimonial: Porque se encuentra fuera del comercio, imposibilitando así que pueda valorarse en dinero, por lo que sobre este derecho, es imposible hacer negocio jurídico alguno.

d. Es indisponible: Puesto que el titular carece de poder de disposición sobre el mismo, es decir, que no tiene la facultad o poder de realizar un acto que decida el destino del derecho, ni tampoco puede hacer dejación de su titularidad.

---

[55] Ana Laura Cabezuelo Arenas, *Derecho de Intimidad* (Valencia: tirant lo Blanch, 1998).
[56] Herrán**,** *El Derecho a la Intimidad* (Véase la nota 41).

e. Es Irrenunciable: Debido a su indisponibilidad, también porque limita al titular a que pueda renunciar a este derecho, por ser innato a él.

f. Es intransmisible: Por la indisponibilidad del titular, lo imposibilita para que pueda trasmitirlo inter vivos y mortis causa.

g. Es Inembargable e Inexpropiable: Por consecuencia de la indisponibilidad y la intransmisibilidad, es decir que el derecho de intimidad, no puede ser apartado de la vida del ser humano; por lo tanto es intransferible.

h. Es Imprescriptible: Dada a su inherencia a la persona el derecho se extingue con ella, además por su característica de extra patrimonial es imposible pensar, que se le pueda aplicar la prescripción, en virtud del Artículo 2237 del Código Civil que establece: "Se gana por prescripción el dominio de los bienes corporales raíces o muebles, que están en el comercio humano…".

i. Es Vitalicio: Porque le pertenece al titular durante toda su vida.

j. Es Inalienable: A consecuencia de su extra patrimonialidad y de su indisponibilidad, imposibilita a que pueda ser susceptible de enajenación por ningún título, ya que se encuentra fuera del comercio.

2.3. Naturaleza jurídica y titularidad del derecho de intimidad

Según Santos Cifuentes el Derecho a la Intimidad es el *"derecho personalísimo que permite sustraer a la persona de la publicidad o de otras turbaciones a la vida privada, el cual está limitado por las necesidades sociales y los intereses públicos".*[57]

Para Fariñas Matoni, El fenómeno intimidad es sumamente complejo, de ahí la dificultad de precisar su naturaleza jurídica, pero el autor relaciona su

[57] Citada por Sebastián Castelli. "Intimidad, informática y derecho", *Artículo*, goo.gl/81sb09.

naturaleza, como psicosocial, porque se considera un bien moral de la espiritualidad de cada ser humano, facultad que posee de excluir 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 categoría de derecho personalísimo por ser éste inherente al desarrollo del ser humano, al brindarle la potestad de resguardar para sí todos los hechos, pensamientos, emociones y sentimientos, que la persona decida no compartir con el resto de la sociedad.[58]

La naturaleza jurídica que el derecho a la intimidad posee es de aquellos derechos fundamentales, y es que cuando se habla de Derechos Fundamentales, se hace referencia a ciertos derechos que poseen una serie de elementos especiales, que se reputan como indispensables para que una persona pueda desarrollarse, sin obstáculos, un plan de vida digno y pleno, en términos generales.

Para que sea considerado derecho fundamental debe cumplir con las siguientes características:[59] **i)** Debe de ser resguardado por la constitución, de allí que toda norma que los infrinja es inconstitucional y, en consecuencia, nula por regla general; **II)** Debe poseer tutela judicial en todos los sentidos, así la observancia de éstos se hallan plenamente controlada por los tribunales;[60] **III)** Determinan la estructura de una sociedad, es decir estos tienen límites; **IV)** El texto constitucional es sucinto, vacío de declaraciones; ya que, establece los derechos fundamentales pero no prevé todos los supuestos en los cuales se aplican esos derechos

[58] Luis Fariñas Matoni, *El Derecho a la Intimidad* (España: Trivium, 1983), 303.
[59] Robert Alexi, *Los Derechos Fundamentales en el Estado Democrático de Derecho, en Neoconstitucionalismo* (Madrid: edit. Trotta, 2003).
[60] Sentencias Definitivas de Inconstitucionalidad, Sala de lo Constitucional, *Referencia: 64-2006AC* (El Salvador, Corte Suprema de Justicia, 2008), considerando número II, 10, goo.gl/uG6xeG.

2.3.1. Titulares del derecho a la intimidad

Una vez comprendida la naturaleza jurídica del derecho a la intimidad queda claro que la titularidad de dicho derecho por antonomasia es para todos los seres humanos, ahora bien saber si una persona jurídica posee este derecho se vuelve imprescindible para esta investigación, esto en razón que el intrusismo informático no solo se comete en perjuicio de seres humanos también se cometen en contra de personas jurídicas, en tal sentido se aborda de forma compendiosa esa duda y así poder aclarar si este derecho es extensible para las personas ficticias.

2.3.1.1. Persona Natural

Con el fin de no ser tautológico cabe hacerse la siguiente pregunta ¿Cuándo comienza a existir un ser humano? la respuesta más precisa a esta cuestión la hace el doctor Jéröme Lejeune, profesor de Genética Fundamental en la Universidad de René Descartes ante el Subcomité del Senado de los Estados Unidos manifestó: "*…La biología moderna nos enseña que los progenitores están unidos a su progenie por un eslabón material continuo, de modo que de la fertilización de una célula femenina (el óvulo) por la célula masculina (el espermatozoide) surgirá un nuevo miembro de la especie. La vida tiene una historia muy, muy larga, pero cada individuo tiene un comienzo muy preciso, el momento de su concepción…*"[61] en El Salvador es aplicable debido a que así lo dispuso la Constitución en su artículo uno inciso segundo, desplazando así la concepción de persona humana que se regulaba en el código civil, en tal sentido y siendo la intimidad inherente al ser humano, puede decirse que dicho derecho se tutela desde el instante de la concepción, es innegable que el feto no pueda ejercer dicho derecho, pero si lo pueden ejercer sus familiares.

[61] Francisco José Herrera, *El Derecho a la Vida y el Aborto* (Colombia: Colección de Textos Jurídicos, 1999), 106.

2.3.1.2. Persona Jurídica

Al analizar los conceptos de privacidad e intimidad, se observa que no son lo mismo pero que son complementarios entre sí, partiendo de ese punto se plantea una nueva interrogante, ¿poseen la personas jurídicas derecho a la intimidad? se puede decir que entre las disimilitudes existentes entre la intimidad y la privacidad, puede señalarse que a diferencia de esta última, la primera implica necesariamente la posibilidad de excluir a los demás en la medida que protege un ámbito estrictamente personal, y que como tal, resulta indispensable para la realización del ser humano, a través del libre desarrollo de su personalidad; por lo que las personas jurídicas, prima facie, no son titulares del derecho a la intimidad, en la medida que no pretenden el desarrollo de una personalidad, sino el cumplimiento de sus fines.

Por otra parte y siendo la minoría, algunos autores aseguran que las personas jurídicas son titulares del derecho a la intimidad afirmando que las personas jurídicas tienen derecho a un nombre, al honor y a la reputación, entonces ¿por qué razón no podrían utilizar la protección que surge del derecho al respeto de la vida privada?[62] Sostienen que en vista de los desarrollos de las técnicas de espionaje industrial, las compañías comerciales deberían estar capacitadas para ampararse en el derecho al respeto de la vida privada al igual que los individuos particulares.

Téngase en cuenta, por un lado, que las personas jurídicas son creadas por las personas naturales con vistas a la consecución de determinados fines que de otra forma no sería posible conseguir, por lo que las personas jurídicas constituyen un instrumento al servicio de los intereses de las personas físicas que las crearon, a criterio personal no las calificamos como

[62] Miguel Ángel Ekmekdijian et al., *Hábeas Data: El Derecho a la Intimidad frente a la Revolución informática* (Buenos Aires: Desalma, 1996).

titulares plenos, aunque si bien es cierto las personas jurídicas están bajo la cobertura de algunas manifestaciones del derecho de intimidad, estas por si solas no pueden ejercer o reclamar sus derechos, por lo que no se concibe la idea de que una persona ficticia tenga un ámbito íntimo.

No cabe duda que existen intromisiones por parte de terceros en una persona ficticia, pero indiscutiblemente serán todas aquellas personas naturales que tienen cualquier vínculo con la persona jurídica las que perciban el mayor daño de esa intromisión.

2.4. Manifestaciones del derecho de intimidad

El derecho a la intimidad es Inherente e irrenunciable, toda persona humana puede excluir del conocimiento a las demás personas -naturales o jurídicas-, de los aspectos personalísimos que le corresponden por su naturaleza, así como también, el tener la potestad, de determinar en qué condiciones y momentos esos aspectos personalísimos los puede dar a conocer a los demás legítimamente.

A lo largo de la historia ha tenido diferentes manifestaciones muy variadas, aparentemente sin relación entre sí, pero que constituyen excepciones de un mismo y único fenómeno, a continuación se abordan las diferentes manifestaciones que conforman el derecho a la Intimidad, con el objetivo de brindar un panorama más amplio de los alcances del derecho en estudio, ya que su ámbito de aplicación no se reduce únicamente al aspecto personal o familiar, sino que incluye otras áreas de desarrollo del ser humano.

2.4.1. Domicilio

Carlos Creus, dice: "…Una de las manifestaciones de la libertad individual es, como se vio, el mantenimiento de una esfera de reserva dentro de la cual el

individuo puede desenvolverse sin la injerencia de terceros. Esa esfera de reserva se traduce, entre otras manifestaciones, en el ámbito de la intimidad del individuo constituido por su domicilio…".[63]

En palabras de Arévalo Silva el domicilio como un atributo de la personalidad, consiste en el lugar donde la persona tiene su residencia con el ánimo real o presunto de permanecer en ella.[64]

González Trevijano, establece que el Domicilio es: "El ámbito de privacidad que comprende tanto la esfera física estricta donde se despliegan las actividades más propias de la vida íntima y familiar, como aquellas no estrictamente domésticas, y que sin embargo se presentan también como manifestaciones principales de la personalidad".[65]

El Código Civil lo define en el Artículo 57 de la manera siguiente: El domicilio consiste en la residencia acompañada, real o presuntivamente, del ánimo de permanecer en ella.

Muy variadas son las definiciones del domicilio, así mismo sus sinónimos, ya que comúnmente se utiliza para referirse al domicilio el concepto de morada, casa, habitación, vivienda, residencia y otros, en la Constitución se encuentra regulado en el Articulo 20 la inviolabilidad del domicilio, el cual reza 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…"; es por

[63] Carlos Creus, *Derecho Penal: Parte Especial,* Tomo I. 6 Ed. (Buenos Aires: Edit. Astrea, 1999), 341.
[64] José Raúl Arévalo Silva, *La Normativa del Domicilio Civil en El Salvador* (El Salvador: Instituto de Investigación Jurídica, Univ. Dr. José Matías Delgado, 2012).
[65] Citado por Joaquín Álvarez Martínez**,** *La inviolabilidad del domicilio ante la inspección de tributos* (España: La Ley, 2007), 168.

ello que cuando se hace referencia al domicilio como una manifestación del derecho de intimidad se refiere a la inviolabilidad del domicilio, como puede observarse en las definiciones anteriores la persona tiene un lugar determinado donde realiza y desarrolla su vida personal, la cual está al margen de los demás.

Por ello la inviolabilidad del domicilio es un aspecto del derecho a la intimidad, que se manifiesta en la intimidad del domicilio, lo que ha sido puesto en contacto con la libertad de cada persona a la hora de decidir sobre las personas con acceso al lugar concreto donde desarrollan los aspectos más íntimos de su vida, y también, para excluir de este ámbito a las personas no deseadas.

2.4.2. Correspondencia y Telecomunicación

En la actualidad se han desarrollado medios masivos de comunicación, veloz, económico, idóneos para enviar y recibir todo tipo de mensajes de texto, correos de voz, fotografías, archivos de sonidos, gráficos e información en grandes volúmenes, volviendo el campo de acción del derecho a la intimidad más amplio, así mismo abriendo puertas por medio de las cuales la intimidad pueda verse afectada.

La correspondencia es definida como aquel derecho, derivación o concreción del derecho a la intimidad, en virtud del cual se prohíbe a los poderes del Estado, oficiales y particulares, la detención y apertura ilegal de la correspondencia. Por otra parte la inviolabilidad de las telecomunicaciones pretende impedir la injerencia e intercepciones de cualquier medio de comunicación.

Es indudable que en el momento en que se redactó el artículo 24 de la

Constitución, no se podía estar pensado en el fenómeno de internet y las nuevas formas de correspondencia y comunicación que existirían, sin embargo es de entenderse que hay que ser taxativo a la hora de restringir un derecho fundamental, siendo al contrario en la tutela, en este caso es válido hacer interpretaciones extensivas con el fin de resguardar derechos fundamentales.

Planteada esa postura la pregunta de rigor es ¿Qué se entiende por correspondencia? El máximo tribunal constitucional de El Salvador manifiesta que la correspondencia no se reduce a la escrita, sino también a la formulada a través de cualquier medio que exprese palabras u otro tipo de lenguaje;[66] amplitud que se fundamenta en el tenor literal de la Constitución, la cual no contempla una concreción del medio utilizado para la correspondencia garantizada, ni señala el contenido de esta, sino que se refiere a todo tipo de correspondencia.

Según la línea marcada por la Sala de lo Constitucional, no solo las cartas manuscritas que tienen un emisor y un receptor es correspondencia, se considera correspondencia toda aquella que exprese palabras u otro tipo de lenguaje sin importar el medio, por lo que se incluye la comunicación electrónica, en ese sentido la ley Especial Contra los Delitos Informáticos y Conexos en su artículo 3 letra F dice que *Comunicación Electrónica: es toda transmisión de datos informáticos, cuyo contenido puede consistir en audio, texto, imágenes, videos, caracteres alfanuméricos, signos, gráficos de diversa índole o cualquier otra forma de expresión equivalente, entre un remitente y un destinatario a través de un sistema informático y las demás relacionadas con las Tecnologías de la Información y la Comunicación.*

[66] Sentencia de Hábeas Corpus, Sala de lo Constitucional**,** *Referencia 135-2005AC*, (El Salvador, Corte Suprema de Justicia, 2008), 6, goo.gl/jsHAIt.

Aclarado el alcance de la correspondencia, resta explicar que es telecomunicación, resulta que este término se introdujo en la Constitución hasta la reforma del artículo 24,[67] sustituyendo la frase *"se prohíbe la interferencia y la intervención de las comunicaciones telefónicas"* por *"se prohíbe la interferencia y la intervención de las telecomunicaciones"* siendo este último más atinado para el contexto actual en que se desarrolla, se entiende telecomunicación como la trasmisión a distancia de datos de información por medios electrónicos o tecnológicos, que tiene por objetivo establecer una comunicación a distancia, es decir, que es un proceso de transmisión de mensajes, un proceso en cuyo curso se hacen llegar a otro expresiones del propio pensamiento articulados en signos no meramente convencionales.

La relación que tiene el derecho a la intimidad con la inviolabilidad de la correspondencia y telecomunicaciones es muy significativa ya que el verdadero atentado se centra en las intromisiones ilegales que se puedan hacer por parte de particulares o del Estado mismo, y es que la comunicaciones realizadas por un ínfimo mensaje, cualquiera que sea el medio utilizado, que haya generado y trasmitido, integra ese ámbito de intimidad jurídicamente protegido, la esfera de reserva de la persona se completa, respecto de todo lo que desea mantener fuera del conocimiento de extraños o reducirlo al conocimiento de un número limitado de personas.

2.4.3. Secreto profesional

El individuo a menudo busca un consejo profesionalmente objetivo de personas cuyo status en la sociedad asegura que no usarán en su perjuicio esos datos que él proporciona. Para proteger esta forma de comunicación

[67] Constitución de la Republica de El Salvador (El Salvador, Asamblea Legislativa de El Salvador, 1983).

limitada, los individuos emisores, gozan de privilegios legales frente a un desvelamiento de dichos datos, así por ejemplo en el código penal del país en al artículo 187 se encuentra regulado lo concerniente a la revelación de secreto profesional.[68]

Obsérvese que se trata de algo más que la simple discreción, pues el secreto implica un deber de reserva plena y total. Como deber, supone un vínculo jurídico, un lazo interpersonal en torno a un objeto corporal o incorporal del que se comparte el conocimiento. La reserva implica ocultar al vulgo y dejar para sí el objeto conocido, con el fin de no alterar la intimidad de la persona, el bien jurídico que se protege con el derecho a la inviolabilidad del secreto profesional es la intimidad de las personas.

2.4.4. Protección de datos

Los datos de toda persona deben ser objeto de protección para que éstos puedan ser tratados o elaborados, y finalmente ser convertidos en información, y en consecuencia, sólo ser utilizados para los fines y por las personas autorizadas.[69]

Los datos según la nueva tecnología informática, pueden ser interconectados y cruzados, como resultado se obtiene una radiografía completa del titular de esos datos, invadiendo y afectando así la intimidad del titular, obligando a considerar el problema de las relaciones entre intimidad e información bajo un nuevo prisma, en tal sentido teniendo en consideración el gran volumen de información que se maneje por medio de bancos de datos ya sean

[68] Se entiende por secreto profesional la obligación que tienen determinados profesionales de no divulgar información confidencial que han conocido en el ejercicio de su profesión, es decir cuando un individuo deposita su confianza en un profesional, le genera a este ultimo la obligación de no revelar lo conocido.
[69] LEGAL CORP. *El Derecho a la Protección de Datos Personales*, goo.gl/P3BGPu.

públicos o privados, verbigracia, registro de la propiedad, registro de automotores, registro de antecedentes penales, padrones electorales, etc., por mencionar algunos, es que en El Salvador, se ha creado bajo líneas jurisprudenciales el derecho de autodeterminación informativa como una nueva extensión del derecho a la intimidad, ya que un tercero que ingrese ilegítimamente en un banco de datos, comete una acción tan reprochable contra el titular de esos datos, como quien allana un domicilio sin orden judicial, afectando 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 legítimo interés en que no se difundan más allá de un círculo determinado.

Se denomina autodeterminación informativa a la "facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente los almacenados mediante medios informáticos".[70]

2.4.5. Publicaciones en internet

Las publicaciones son acciones consistentes en hacer del dominio público cierta información, dándola a conocer a muchas personas o en su defecto a personas seleccionadas, se sabe que al publicar cualquier tipo de información en el internet se relega el derecho a la intimidad, ya que se quiere mostrar al mundo cierta parte del individuo, sin embargo toma relevancia el derecho a la privacidad, y como se ha sostenido estos derechos son complementarios e interdependientes entre sí.

Como se ha señalado, en virtud del derecho a la privacidad un individuo

[70] Ricardo Manuel Trigo Calonge, *Internet, Intimidad y Privacy* (Madrid: 2008), 12, goo.gl/srH5XL.

puede sustraer aspectos de su vida privada del escrutinio público, pero ¿Realmente existe este derecho dentro del internet? Esta pregunta se contestaría en sentido afirmativo. Esto debido a que hace tiempo, la mayoría de las empresas proveedoras de redes sociales online, blog, foros, comunidades virtuales, chats o sistema de correos electrónicos, han incluido, dentro de sus propias páginas de Internet, políticas en materia de privacidad, bajo los contratos de adhesión online.[71]

Esto demuestra tanto la existencia del derecho como su reconocimiento por parte de los sitios sociales en Internet. A pesar de lo anterior, ¿Por qué se verifican invasiones importantes al derecho a la privacidad de los cibernautas? La respuesta se encuentra relacionada con el comportamiento que éstos asumen al momento de registrarse en una red social, por ejemplo los usuarios no toman el tiempo para revisar de manera adecuada los contratos de adhesión, y en su afán de integrarse a una comunidad en línea, un usuario podría perder de vista tanto la información personal que un sitio social le requiere para poder ser admitido como las políticas que se seguirán en el tratamiento de sus datos.[72]

Si bien el comportamiento de los usuarios de las redes sociales es determinante para disminuir los riesgos de invasión a su vida privada e identidad digital, las empresas proveedoras de estos servicios también se

[71] Carlos Useros Raboso, "El Contrato de Adhesión Online en Redes Sociales", *Artículo,* goo.gl/wggmdu. Los Centrados de adhesión online son aquellos en los cuales el contenido contractual ha sido determinado con prelación, por uno solo de los contratantes, en este caso por los proveedores de estos servicios, el usuario al realizar el proceso de registración en cualquier sitio web que preste este tipo de servicios debe obligatoriamente aceptar y prestar conformidad a los términos y condiciones del sitio y políticas de privacidad impuestas unilateralmente, la naturaleza jurídica del contrato que rige la relación, llamados comúnmente "Términos de Uso", "Términos y condiciones", "Políticas de Privacidad".

[72] Diego García Ricci**,** *El Derecho a la Privacidad en las Redes Sociales en Internet*, goo.gl/MJC3GX.

encuentran obligadas a respetar el derecho a la privacidad de los cibernautas.[73] Dichas empresas deben ofrecer un manejo responsable y cauteloso tanto de la información que poseen en sus archivos como de las aplicaciones que sus sitios web desarrollan, pues en ocasiones, éstas son generadas por terceros ajenos a los mismos sitios, esto se advierte con el hecho de que tanto las sociedades en general como los Estados se encuentran obligados a vigilar el cumplimiento del derecho a la privacidad dentro de internet.

2.5. Definición y conceptualización de la informática

El derecho a la intimidad y el desarrollo tecnológico genera formas, procedimientos y técnicas que permiten la intromisión en ese reducto de soberanía individual, sin que en muchos casos sea siquiera perceptible.

Cuando las inmensas posibilidades de la técnica no se aplican al servicio del hombre, sino para someterlo, la informática deviene una terrible amenaza para la libertad de los hombres, convirtiendo la sociedad en una inmensa casa de cristal en la que todas nuestras manifestaciones, nuestras grandezas y nuestras miserias, quedan al desnudo ante cualquier observador.[74]

Por ello, se debe de acotar que es la informática, identificando los elementos que la constituyen, ya que la mayoría no conocen los conceptos relacionados

[73] La definición más básica seria la identidad en Internet, pero se debe dar más profundidad. La RAE dice que la identidad es "Conjunto de rasgos propios de un individuo o de una colectividad que los caracterizan frente a los demás". En ese sentido identidad digital es el conjunto de expresiones personales o grupales que realizan en Internet. Estas expresiones son fruto de la capacidad de editar en diferentes espacios web redes sociales online, perfiles profesionales, blogs, página de empresa, comentarios que se realizan en noticias, opiniones en foros, etc.

[74] Luis Alfonso Ureña López, *Fundamento de Informática* (México: edit. Alfaomega, 2005), 108.

con esa ciencia y su tratamiento, aunado a esto se tiene una percepción parcial de lo que es informática y los alcances que esta pueda tener en la vida del ser humano.

Al momento de definir la informática, según las múltiples fuentes consultadas, parecen existir tres posturas principales, claro, que cada una de las definiciones presenta sus matices particulares: una, que la considera como un campo o ciencia emergente donde concurren distintas disciplinas; otra que la identifica con la computación; y una tercera que la considera una ciencia de la información,[75] siendo la última la que se tratara de concatenar con el derecho a la intimidad.

Asimismo, el concepto de informática tiene muchas definiciones dependiendo del autor que maneje los términos, sin embargo todos coinciden en que el origen de la palabra informática obedece a la fusión de los términos Información y automática,[76] haciendo referencia al conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento automático y racional de la información por medio de dispositivos electrónicos que pueda ejecutar cualquier función de la tecnología de la información -informática- y la comunicación -telemática-.

En un glosario especializado se define informática como la disciplina que tiene como objeto de estudio los procesos que se ejercen sobre datos e información,[77] por ejemplo, generación, obtención, registros, depuración, ordenamiento, validación, codificación, almacenamiento, integración, acceso,

[75] Es una rama de la ciencia que estudia la práctica del procesamiento de información y la ingeniería de los sistemas de información. Tiene un fuerte vínculo con las ciencias de la computación.
[76] Ureña, *Fundamento de Informática* (Véase la nota 74).
[77] Ricardo A. Guibourg, *Manual de Informática Jurídica* (Argentina: edit. Astrea 1996), 89.

recuperación, visualización, siguiendo esta definición se puede rescatar que datos e información no es lo mismo, el primero es el elemento de conocimiento que carece de significado por sí mismo, o que está fuera de su contexto, es decir se trata de algo incompleto que necesita un complemento en la forma de otro dato o un proceso de elaboración que le dé más sentido, por tanto el dato tiene un carácter individualizado y simple frente a un producto semielaborado como es la información, que son los datos o conjuntos de datos, elaborado y situado en un contexto, de forma que tiene un significado para alguien en un momento y lugar determinado.[78]

Para este estudio se entiende por informática como una ciencia de la información,[79] que se ocupa del tratamiento automático y racional de la información, a través de cualquier medio electrónico -hardware y software- que tenga la capacidad de procesar, recibir y transmitir, información de cualquier índole. Para que esa información en el contexto de la sociedad informatizada pueda crearse, recibirse y transmitirse deben existir los recursos idóneos, amalgamados en lo que se conoce técnicamente como sistema informático,[80] en ese sentido se debe de saber cuáles son estos elementos constituyentes.

2.6. Elementos constituyentes de un sistema informático

Son tres los elementos que constituyen un sistema informático y que por

[78] Carmen de Pablos, *Informática y Comunicaciones en la Empresa* (Madrid: edit. ESIC, 2004), 16.
[79] Al referirse a ciencia de la información se debe decir que es una rama de la ciencia que estudia la práctica del procesamiento de información y la ingeniería de los sistemas de información.
[80] Según la Ley Especial Contra los Delitos Informáticos y Conexos, se entiende por sistema informático o S.I., como un elemento o grupo de elementos interconectados o relacionados, pudiendo ser electrónicos, programas informáticos, enlaces de comunicación o la tecnología que en el futuro los reemplace, orientados al tratamiento y administración de datos e información.

consiguiente hacen posible el desarrollo, aprovechamiento y flujo de información.[81]

2.6.1. Elemento físico "Hardware"

La palabra hardware se refiere a todas las partes físicas de un sistema informático; es decir la propia computadora, los dispositivos externos a la misma, así como todo material físico relacionado con los ordenadores; esta misma definición es aplicada para aquellos dispositivos electrónicos que pueda ejecutar cualquier función de la tecnología de la información y la comunicación.[82]

2.6.2. Elemento Lógico "Software"

Se considera la parte lógica del sistema informático, que dota al equipo físico de la capacidad para realizar cualquier tipo de tareas,[83] considerando esta definición, el concepto de software va más allá de los programas de computación en sus distintos estados: código fuente, binario o ejecutable; también su documentación, los datos a procesar e incluso la información de usuario forman parte del software: es decir, abarca todo lo intangible, todo lo "no físico" relacionado.

2.6.3. Elemento Humano

Es el conjunto de personas que desempeñan las distintas funciones relacionadas con la utilización y explotación de un sistema informático, este último elemento no debe confundirse con lo que se conoce como Hacker, por lo general y a no ser la excepción, estas personas se encuentran fuera de un sistema informático, ya que no han sido autorizados para el manejo de la

[81] Ureña, *Fundamento de Informática* (Véase la nota 74).
[82] De Pablos, *Informática y Comunicaciones en la Empresa*, 54 (Véase la nota 78).
[83] Jairo Amaya Amaya, *Sistemas de Información Gerencial, Hardware, Software, Redes, Internet, Diseño* (Bogotá: Ecoe Ediciones 2010).

información, razón por la cual sus acciones encajan en tipos penales, relativamente nuevos para el país.[84]

2.7. Intrusismo Informático

Actualmente se viene incluyendo por la doctrina mayoritaria bajo el concepto de Delito informático tanto el delito tradicional cometido a través de ordenador o la Red -Internet- como el estrictamente entendido como tal, esto es el dirigido contra la informática, los datos y la información informatizada, o las redes de telecomunicación, especialmente a través de Internet;[85] entre ellos se encuentra la delincuencia intrusiva, y es que el intrusismo informático o "hacking" presume en su comisión una conducta de acceso o permanencia no autorizados a sistemas informáticos, una interferencia en redes de telecomunicación electrónicas protegidas.

El hacking, vulnera la confidencialidad y exclusividad de la información, puesto que se trata del ingreso ilícito a sistemas informáticos protegidos por medidas de seguridad y limitaciones de acceso. El hacker[86] que es la persona que irrumpe en el sistema informático, y accede a la información de forma ilícita, vulnera la confidencialidad y exclusividad de ésta; violentando la intimidad del titular de la información.

---

[84] Véase: Ley Especial Contra los Delitos Informáticos y Conexos (El Salvador, Asamblea Legislativa de El Salvador, 2016), Titulo II.

[85] Enrique del Canto. *Ciberdelincuencia Intrusiva: Hacking y Grooming*, goo.gl/lb88Al.

[86] Es un término de origen anglosajón que para Hugo Daniel Carrion, puede ser definido como *"un informático que utiliza técnicas de penetración no programadas para acceder a un sistema informático con los más diversos fines: satisfacer su curiosidad, superar los controles, probar la vulnerabilidad del sistema para mejorar su seguridad, sustraer, modificar, dañar o eliminar información; y cuyas motivaciones también responden a los más variados intereses: ánimo de lucro, posturas ideológicas anarquistas, avidez de conocimientos, orgullo, propaganda política, etc."*.

CAPÍTULO III
REGULACIÓN JURIDICA EN MATERIA PENAL Y DERECHO INTERNACIONAL RELATIVA AL DERECHO A LA INTIMIDAD

Todas las personas, en cualquier momento de su existencia, han reclamado el reconocimiento y protección de su vida privada o íntima, tanto por parte de las autoridades públicas como de los particulares, sin embargo, se desconoce los fundamentos legales que otorga la ley para lograr su efectividad y materialización.

En este capítulo se examinan aquellas normas legales nacionales que protegen el derecho a la intimidad del intrusismo informático, por lo que se hace un estudio práctico y descriptivo de la legislación; en ese sentido se retoma lo que dice la doctrina mayoritaria, y se empieza por lo que está sobre todo el ordenamiento jurídico, la Constitución.

3. Leyes de la República de El Salvador

3.1. Constitución de la República.

La Constitución de la República de El Salvador,[87] constituye la norma fundamental y suprema, lo dicho anteriormente queda consagrado en el artículo 246 inc. 2 de la Cn. que señala: “La Constitución prevalecerá sobre todas las leyes y reglamentos...”. Asimismo los artículos 144 y 145 Cn., prescriben que los Tratados internacionales son leyes de la república, pero cuando estos entren en conflicto con otras leyes prevalecerán sobre las mismas, sin que alteren, restrinjan o afecten por ningún motivo las disposiciones establecidas en la constitución.

[87] Constitución de la República de El Salvador (El Salvador, Asamblea Legislativa de El Salvador, 1983).

Bajo esa prisma la Intimidad como todo Derecho fundamental contiene raigambre constitucional, es así, que el artículo 2 inciso segundo de la Carta Magna del país expresa que: “se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen”, según establece la citada 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 demás.

Lo dicho anteriormente es la cláusula general que se le da a este derecho fundamental; sin embargo como se expresó en el capítulo dos cuando se hizo referencia a las manifestaciones del derecho a la intimidad esta tiene diferentes formas, es así que el constituyente también protege esas extensiones que por antonomasia pertenecen al derecho a la intimidad, se habla del derecho a la inviolabilidad de la morada, en el artículo 20 Cn. estableciendo taxativamente los supuestos bajo los cuales se puede ingresar, pudiendo ser 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 el mismo supuesto se encuentra la inviolabilidad a la correspondencia y a las telecomunicaciones, ambas se encuentran reguladas en el artículo 24 Cn.

En el primero de los casos se establece que la injerencia en esta no dará fe ni podrá figurar en ninguna actuación, determinando las únicas dos excepciones, que es en el caso de concurso y quiebra; en el segundo caso se incluye el término telecomunicación, dejando de lado el termino comunicación que un primer momento se refería únicamente a la telefonía, hoy este término abarca tanto las comunicaciones que se hacen a través de un celular, como aquellas conversaciones privadas que utilicen cualquier

medio electrónico; al igual que en los derechos supra enunciados, este puede ser perjudicado siempre y cuando exista una orden judicial, esta tendrá que ser de forma escrita, motivada y temporal, de no seguir estos parámetros la prueba se catalogará como ilegal consecuentemente carecerá de valor probatorio, así mismo el funcionario que transgreda este derecho sin previa autorización, será destituido dando lugar a la indemnización por daños y perjuicios ocasionados. La Constitución tiene como objeto tutelar el bien jurídico que en este caso concreto es la Intimidad de las personas físicas, a través de la protección 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.

3.2. Protección del Derecho a la Intimidad por Instrumentos Internacionales

El derecho a la intimidad tiene diferentes concreciones, vuelve escabroso aglomerar los instrumentos internacionales que de alguna manera coadyuvan al desarrollo y protección del derecho a la intimidad, sin embargo se pueden mencionar aquellos instrumentos que se encuentra vigentes y aplicables en El Salvador.

3.2.1. Declaración Americana de los Derechos y Deberes del Hombre

Ratificado por El Salvador el 20 de junio del año de 1978.[88] 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 creada teniendo en

[88] 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, ratificada por El Salvador el 20 de junio del año de 1978.

cuenta que los pueblos americanos han dignificado la persona humana y que sus constituciones nacionales reconocen que las instituciones jurídicas y políticas, rectoras de la vida en sociedad, tienen como fin principal la protección de los derechos esenciales del hombre y la creación de circunstancias que le permitan progresar espiritual, materialmente y alcanzar la felicidad.

Regula un catálogo de derechos entre ellos Derecho a la vida, la libertad, la seguridad e integridad de la persona. En cuanto al derecho a la intimidad en su artículo V establece el derecho de protección a la honra, la reputación personal y vida privada familiar, 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”. Dentro de esta declaración, no se encuentra regulado ningún tipo de procedimiento en caso de interpretación o aplicación del instrumento, de modo que será la OEA su autoridad de aplicación en caso de controversia.

El derecho a la inviolabilidad de la correspondencia es expresamente reconocido en el artículo X, al mencionar en el capítulo primero titulado “Derechos” que toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia.

3.2.2. Declaración Universal de los Derechos Humanos

La Asamblea General proclamo la presente Declaración Universal de Derechos Humanos 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 aseguren los estados, por medidas progresivas de carácter nacional e internacional, su reconocimiento y aplicación universales y efectivos.

En tal 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".[89]

Así 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 titular.[90] Expresando además que la ley tiene que proteger contra injerencias o ataques de terceros, es decir, injerencias de extraños a la esfera de su vida individual y familiar, porque se le otorga la facultad de excluir a otras personas el conocimiento de aspecto que reserva para sí o para quien el considere pertinente manifestar.

3.2.3. Convención Americana Sobre Derechos Humanos (Pacto de San José, OEA 1969)

Este Instrumento Regional aprobado por la OEA el 22 de Noviembre de 1969. Según manifiesta en sus considerandos fue creado con el propósito de consolidar dentro de las instituciones democráticas, un régimen de libertad personal y de justicia social, fundado en el respeto de los derechos esenciales del hombre. Sin duda alguna, regula el derecho a la intimidad, quedando de manifiesto su protección en la parte I "Deberes de los Estados

[89] El Salvador como Estado Miembro de la Organización de las Naciones Unidas aprobó el 10 de diciembre de 1948 la Declaración Universal de Derechos Humanos.
[90] Xavier Pons Rafols*, La Declaración universal de derechos humanos: comentario artículo por artículo* (Barcelona: trad. Victoria Pradilla edit. icaria), 229, goo.gl/6BwmZA.

y Derechos Protegidos"; Capítulo I "Enumeración de Deberes"; artículo 11 "Protección de la Honra y de la Dignidad". Numeral 2, al señalar que "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada…. en su domicilio o en su correspondencia".[91]

En el párrafo transcrito se aluden dos derechos diferentes: el derecho a la privacidad y el derecho a la intimidad, porque establece las injerencias en el domicilio y en la correspondencia, sin embargo existen casos en los que las legislaciones y la doctrina han mezclado el concepto de privacidad con intimidad, al utilizarlos como sinónimos. Pero la distinción entre ambos conceptos, está en que la privacidad implica acciones que no afectan a terceros, en un ámbito de conocimiento que únicamente, permite injerencia ajena por el consentimiento del titular. Así, existen dos conductas, una es la ética privada, lo particular y personal y otra es la totalmente pública. Lo que existe es una relación de género (privacidad) a especie (intimidad). La intimidad es el área reservada de la persona que está protegida del conocimiento ajeno.[92] El derecho a la intimidad, se distingue esencialmente con el derecho a la privacidad, porque este último incluye acciones que de ningún modo, puede ofender la moral pública o perjudicar a terceros, a diferencia de la vida privada. [93]

3.2.4. Pacto Internacional de Derechos Civiles y Políticos

Este pacto fue ratificado por el país el 23 de Noviembre de 1979.[94] Reconoce los derechos que se derivan de la dignidad inherente a la persona humana,

[91] Convención Americana Sobre Derechos Humanos Pacto de San José, OEA 1969.
[92] Romina Petrino, *Convención Americana sobre Derechos Humanos y su Proyección en el derecho argentino* (Argentina: Universidad de Buenos Aires, 2013), 209-210.
[93] Ibíd., 2013.
[94] Pacto Internacional de Derechos Civiles y Políticos 1966. Ratificado por El Salvador, DL. Nº 27, de 23 de noviembre de 1979 publicado en DO. Nº 218, Tomo 265 del 23 de noviembre de 1979.

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 citada tiene como finalidad hacer que reconozcan los de 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.

3.2.5. Convenio Internacional de Telecomunicaciones

Ratificado por El Salvador, el 22 de Julio de 1976. Su principal objetivo es mantener y ampliar la cooperación internacional para el mejoramiento y el uso racional de toda clase de telecomunicaciones, y a su vez, favorecer el desarrollo de los medios técnicos y su más eficaz explotación a fin de aumentar el rendimiento de los servicios de telecomunicaciones, acrecentar su empleo y generalizar en lo posible su utilización para el público. El organismo internacional de origen de este convenio es la Unión Internacional de Telecomunicaciones y por lo tanto la autoridad de aplicación, con sede es la ciudad de Ginebra.

En su artículo 32 reconoce expresamente el Secreto de las Telecomunicaciones, con este se pretende proteger las comunicaciones entre las personas, de cualquier interceptación ilegal de terceros, existiendo la excepción, para su afectación a esta dimensión del derecho a la intimidad, cuando la ley lo disponga.[95] Este derecho no tiene carácter absoluto porque en el mismo artículo, se reservan el derecho a comunicar esta

[95] Javier Díaz Revorio “El derecho fundamental al secreto de las comunicaciones”. *Universidad de Castilla-La Mancha* (2006): 159, goo.gl/n54Rn4.

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 excluyen de la obligación para colaborar en alguna investigación penal.

3.3. Legislación Secundaria

Antes de abordar las diferentes leyes que protegen el derecho a la intimidad, se define el concepto de ley, así el código civil de El Salvador en su artículo 1 expresa: "La ley es una declaración de la voluntad soberana que, manifestada en la forma prescrita por la Constitución, manda, prohíbe o permite". A continuación se desarrolla la legislación pertinente al derecho a la intimidad, si bien es cierto, existe regulación jurídica en materia civil, familia y mercantil, pero por la naturaleza de la investigación, solo se consideran las leyes penales.

3.3.1. Código penal

El código penal, fue creado el 26 de abril de 1997.[96] Regula los delitos, faltas y sus penas. Así, el derecho penal, se aplica y responde al principio de mínima intervención, que establece que solo debe intervenir en aquellos hechos más graves que transgreden los bienes jurídicos más importantes de la sociedad, dejando para otras ramas del derecho, las infracciones que no le interesa proteger. En cuanto al derecho a la intimidad su protección se encuentra, en su título VI denominado delitos relativos al honor y la intimidad, regula en su capítulo II los delitos relativos a la intimidad, la violación de comunicaciones privadas. Dispone de un catálogo de delitos, que protegen el derecho a la intimidad, entre ellos, el delito de violación de comunicaciones privadas regulado en el artículo 184, que establece lo siguiente:

[96] Código Penal (El Salvador, Asamblea Legislativa de El Salvador, 1997).

“El que con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido o se apodere de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivo o registro público o privado, será sancionado con multa de cincuenta a cien días multa.

Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de cien a doscientos días multa.

El tercero a quien se revelare el secreto y lo divulgare a sabiendas de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa”.

En el artículo en comento, se tutela el bien jurídico intimidad, la acción constitutiva de delito que consiste en apoderarse de la comunicación escrita, soportes informáticos, documentos o el medio en que está, el secreto o los datos personales o familiares, es decir que mediante esa intromisión se vulnerara la intimidad de la persona, esta conducta tiene como objetivo descubrir los secretos, en otras palabras aquel conocimiento que pertenece exclusivamente a un número limitado de personas, y el revelarlo o divulgarlo a otras personas u otra depende únicamente de la voluntad de estas. El sujeto activo puede ser cualquier persona, con excepción de los que por su cualificación están incorporados en la descripción del tipo penal agravado, regulado en el artículo 185 del Cpn. En cuanto al sujeto pasivo es la persona titular del secreto. Además el tipo penal exige que el sujeto activo ejecute la acción porque quiere tener conocimiento para sí o para un tercero.

In fine del inciso primero se establece la sanción de cincuenta a cien días

multas, asimismo 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 delito.

El artículo 185 del mismo cuerpo normativo regula la Violación Agravada de Comunicaciones, expresa: *"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".*

Esté tipo penal contiene una agravación, en cuanto a la calidad del sujeto activo, siempre que ejecuten las conductas descritas en el artículo 184 y tengan la calidad de sujetos encargados o responsables, asimismo el secreto este en un fichero, soporte informático.

El artículo 186 regula el delito de Captación de Comunicaciones, 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".

Al igual que el delito anterior el bien jurídico protegido por el tipo penal, es la intimidad de la persona. La acción típica se ejecuta al interceptar, impedir o interrumpir una comunicación telegráfica o telefónica o la utilización de medios o artificios medios tecnológicos de escucha, transmisión o grabación del sonido, de la imagen o de cualquier otra señal de comunicación, es decir que incluye los modernos avances tecnológicos en comunicación, como el fax, el internet, lo que implica intrusismo informático, también denominado hacking, es decir el acceso sin autorización, a los archivos y bases de datos contenidos en los sistemas informáticos ajenos, aunque por lo general de grandes empresas o instituciones, al accesar sin consentimiento a la información que se considera secreta, estando en presencia de intrusismo informático, aunque el tipo penal no lo regula expresamente.

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 multa. El inciso tercero, regula con sanción de multa de treinta a cincuenta días, para la divulgación del secreto, por parte de una persona diferente al que ejecuto el tipo básico, sabiendo del origen ilícito de la información y el inciso final regula la pena de dos a seis años de prisión, al que ejecute los actos señalados en el primer inciso con la

finalidad 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 Cpn.

Además, hay que destacar que el sujeto activo del delito tiene como propósito, vulnerar 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 revelarse aún tercero, sin el consentimiento expreso del titular.

En la redacción del tipo penal el legislador previno el fenómeno de internet y las nuevas formas de correspondencia y comunicación que existen, al establecer en la descripción *"…cualquier otra señal de comunicación…"*

Asimismo cuando se expresa *"…utilizare instrumentos o artificios técnicos…"* para ejecutar cualquiera de los verbos rectores del tipo penal se puede inferir que el sujeto que quiera obtener dicha información obligadamente tiene que tener conocimientos y herramientas de hacking para ejecutar el delito en comentó,[97] sin embargo no se requiere una calidad especial para ejecutar la acción descrita.

La siguiente concreción del derecho a la intimidad, es la protección del derecho a la inviolabilidad de la morada, el código penal manifiesta en el artículo. 188: *"El particular que, sin habitar en ella, se introdujere en morada ajena o en sus dependencias, sin el consentimiento de quien la habitare, de*

[97] Verbigracia los siguientes dispositivos: Stingray, Longship, Kingfish, Harpoon, Triggerfish, estos dispositivos tienen en común que pueden recopilar datos de los teléfonos móviles que están operando en su rango, véase: goo.gl/IdhdW5.

manera clandestina o con engaño o permaneciere en la misma contra la voluntad del morador, pese a la intimación para que la abandonare, será sancionado con prisión de dos a cuatro años y multa de treinta a cincuenta días multa.

Si el ingreso o permanencia se hiciere concurriendo una o más de las siguientes circunstancias: con violencia en las personas, aprovechando la nocturnidad, portando armas de cualquier tipo, simulando ser agente de autoridad o por dos o más personas, la sanción será de tres a seis años de prisión y multa de cincuenta a cien días multa."

El bien jurídico protegido al igual que la anterior disposición, es la intimidad, el tipo penal establece la acción de introducirse a una morada sin el permiso del dueño, es decir aquel ámbito o espacio en el que una persona desarrolla su vida. Así cuando un sujeto se introduce a la morada sin el consentimiento del titular vulnera la intimidad personal, esta es una invasión totalmente física, la sanción establecida es la pena de prisión de dos a cuatro años y multa de treinta a cincuenta días multa. Cualquier sujeto puede ejecutar el delito, porque no se requiere calidad especial, solo tiene que ser una persona que no habite en la morada afectada.

Además el inciso segundo establece una agravación, al disponer que si el allanamiento se realizare de forma clandestina o con engaño o permaneciere contra la voluntad del morador, y no someterse a la voluntad del morador para que abandone el lugar, la sanción será prisión de dos a cuatro años y multa de treinta a cincuenta días multa. Por último se vulnera la intimidad cuando se introducen o permanecen en la morada, en contra de la voluntad del titular realizando una o más de las siguientes circunstancias: con violencia en las personas, aprovechando la noche, portando armas de

cualquier tipo, simulando ser agente de autoridad o por dos o más personas, lo que podría llegar al concurso de delito. Para este caso la sanción es de tres a seis años de prisión y multa de cincuenta a cien días multa.

Dicho lo anterior se dice que para vulnerar la morada esta tiene que ser ajena al sujeto activo del delito, además debe de entrar por completo a la morada ajena o a sus dependencias, es decir no es suficiente la sola puesta de alguna extremidad y este tiene que negarse a salir cuando se lo soliciten. Sin embargo el sujeto activo también puede hacer uso de la tecnología, y es que utilizando diferentes clases de hardware y software, se puede introducir a la morada de una persona, en este caso muy probablemente el sujeto pasivo tardara en darse cuenta que está siendo monitoreado cibernética y clandestinamente.

3.3.2. Ley Especial para la Intervención de las Telecomunicaciones

Esta ley dispone en su artículo 1 garantizar el secreto de las telecomunicaciones y el derecho a la intimidad, estableciendo la excepción a la vulneración de la intimidad, únicamente, mediante autorización judicial, de forma escrita y motivada, interviniendo temporalmente[98] cualquier clase de telecomunicaciones,[99] preservándose en todo caso el secreto de la información privada que no guarde relación con la investigación o el proceso penal, esta disposición, se relaciona básicamente con el artículo 24 de la Constitución que prohíbe la interferencia y la intervención de las telecomunicaciones.

[98] La ley dispone en el inciso primero del artículo 12 que *la intervención de las telecomunicaciones se autorizará por plazos no superiores a tres meses, que podrán prorrogarse hasta por tres períodos más*.

[99] Ley Especial Para la Intervención de Las Telecomunicaciones, artículo 1 (El Salvador, Asamblea Legislativa de El Salvador, 2010).

Sin embargo, en su inciso 2 permite que excepcionalmente se intervenga de manera judicial con un motivo fundado, y en los casos que determina la ley, así la Ley Especial para la Intervención de las Telecomunicaciones**,** establece los delitos de procedencia: extorsión, comercio de personas, tráfico ilegal de personas, trata de personas y su forma agravada, los delitos previstos en la Ley Reguladora de las Actividades Relativas a las Drogas, los delitos previstos en la Ley Especial contra Actos de Terrorismo, los delitos previstos en la Ley contra el Lavado de Dinero y de Activos, entre otros.[100]

Asimismo para vulnerar el derecho a la intimidad, interviniendo las telecomunicaciones, la ley en comento establece como condición para solicitar y aplicar la intervención, la existencia de una investigación que manifesté indicios racionales que se ha ejecutado, o se está ejecutando o está por ejecutarse un delito de los que determina la misma ley, para que el juez autorice la medida, es decir, que aun cumpliendo los requisitos anteriores solo puede intervenirse las telecomunicaciones, con autorización del juez competente.

Esta intrusión de un tercero extraño a la comunicación, es decir el centro de intervención, independiente de los medios que empleen para intervenir las llamadas telefónicas, transgrede el derecho a la intimidad personal, porque toda persona puede comunicarse libremente por medios telefónicos, al comunicarse manifiesta información reservadamente a personas determinadas, así, los operadores de telecomunicaciones codifican las comunicaciones, protegiendo la intimidad del emisor, para que no las capte un tercero que no está autorizado para recibir la información. Pero la misma norma constitucional dispone que “excepcionalmente podrá autorizarse

[100] Ibíd., artículo 5.

judicialmente, de forma escrita y motivada, la intervención temporal de cualquier tipo de telecomunicaciones, preservándose en todo caso el secreto de lo privado que no guarde relación con el proceso. La información proveniente de una intervención ilegal carecerá de valor “.

De esta forma, las autoridades pueden vulnerar la intimidad de las comunicaciones, para accesar con fines judiciales, lo que permite determinar que el derecho a la inviolabilidad de las comunicaciones no es absoluto, porque puede ser transgredido en los casos establecidos en la constitución y la ley, si bien es cierto la norma constitucional protege la intimidad de las personas ante el Estado, pero no quiere decir, que se garantizara, la impunidad de determinados hechos ilícitos, por lo tanto como una excepción pueden transgredirse las comunicaciones para la investigación de hechos ilícitos, siempre y cuando la intervención a las comunicaciones esté debidamente autorizada. Esta es la única ley en El Salvador, que permite violar, la intimidad de las personas, en las áreas de las comunicaciones (teléfono, email, correo, mensajes digitales).

3.3.3. Ley Especial Contra los Delitos Informáticos y Conexos

En materia penal también se encuentra la Ley Especial Contra los Delitos Informáticos y Conexos, fue creada el 4 de febrero del año 2016. Los delitos regulados en esta ley serán objeto de análisis en otro capítulo por lo que no se profundizara, por el momento.

Así, contiene tres títulos, treinta y seis artículos, en el título I regula las disposiciones generales. El objeto de la presente ley, según el artículo 1 es la protección los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos

almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, y regula expresamente la protección a la intimidad, porque establece, como objeto de protección en su artículo 1 inciso final:.. “intimidad e imagen de las personas naturales o jurídicas”….disposición que se desarrolla en el correspondiente al análisis de los delitos de la ley.[101]

El título II regula los delitos, el capítulo I contiene un catálogo de delitos contra los sistemas tecnológicos de información; el capítulo II regula los delitos informáticos; el capítulo III contiene los delitos Informáticos relacionados con el contenido de los datos; capítulo IV tiene el catálogo de delitos informáticos contra niñas, niños y adolescentes o personas con discapacidad; y el capítulo V dispone los delitos contra el orden económico. Y el título III regula las disposiciones finales.

3.3.4. Ley de Acceso a la Información Pública

Además existe la Ley de Acceso a la Información Pública, creada mediante Decreto No. 534 del 2 de diciembre de 2010.[102] Si bien es de carácter administrativo pero tiene relevancia en cuanto al derecho a la intimidad y por lo tanto se elabora un breve cometario. Tiene por objeto garantizar el derecho de acceso a la información pública, a toda persona, así, respecto a la protección del derecho a la intimidad, se encuentra regulado en el Capítulo III denominado Información Confidencial, establece en su artículo 24 lo siguiente: “a. La referente al derecho a la intimidad personal y familiar, al honor y a la propia imagen, así como archivos médicos cuya divulgación

[101] Ley Especial Contra Los Delitos Informáticos y Conexos (El Salvador, Asamblea Legislativa de El Salvador, 2016).
[102] Ley de Acceso a La Información Pública (El Salvador, Asamblea Legislativa de El Salvador, 2010).

constituiría una invasión a la privacidad de la persona. b. La entregada con tal carácter por los particulares a los entes obligados, siempre que por la naturaleza de la información tengan el derecho a restringir su divulgación. c. Los datos personales que requieran el consentimiento de los individuos para su difusión. d. Los secretos profesionales, comerciales, industriales, fiscales, bancarios, fiduciarios u otro considerado como tal por una disposición legal. Los padres, madres y tutores tendrán derecho de acceso irrestricto a la información confidencial de los menores bajo su autoridad parental."

El artículo en comento regula la Información que se considera confidencial y que afecta la intimidad de las personas, por ejemplo: los datos personales, en este caso únicamente se puede disponer de ellos, según su naturaleza, cuando exista consentimiento del individuo para su difusión. El derecho a la información, es el que tiene toda persona para solicitar y recibir información generada, administrada o en poder de las instituciones públicas y demás entes obligados de manera oportuna y veraz, sin sustentar interés o motivación alguna, según lo dispone el artículo 2 de la ley en cometo.

Sin embargo, existe información que por su naturaleza confidencial no se proporciona a cualquier persona, así el artículo 24 en comento dispone como información confidencial, la relativa al derecho a la intimidad personal y familiar, al honor y a la propia imagen, así como archivos médicos que al revelarlo constituye una invasión a la privacidad de la persona, entre otras, la misma ley define Información confidencial en el artículo 6: f) de la siguiente forma: "es aquella información privada en poder del Estado cuyo acceso público se prohíbe por mandato constitucional o legal en razón de un interés personal jurídicamente protegido." Asimismo la ley define los 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 y familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, a la intimidad personal y familiar y a la propia imagen, según lo dispone el artículo 6: b).

Además el artículo 24 de la citada ley considera como información confidencial, ciertos datos personales, que requieren el consentimiento de los individuos para su difusión, la misma ley entiende por datos personales: la información privada referente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra análoga, según lo manifiesta el artículo 6: a).

Se desprende de lo anterior que la información aludida es de interés personal, es decir, que pertenece a la esfera de la intimad de una persona, pero está a disposición de la administración del estado, los miembros de los entes encargados de esta información no pueden difundir, distribuir o vender la información personal, que resguardan en los sistemas de información, sin embargo por excepción pueden hacerlo, solo si se realiza con consentimiento expreso y libre, por escrito o por un medio equivalente, de las personas titulares.[103]

3.4. Derecho comparado en cuanto al respeto y protección del derecho a la intimidad

En derecho comparado se utiliza, como sinónimo de intimidad, el concepto de derecho a la vida privada, los datos personales, así, el derecho en comento se protege a nivel constitucional, en algunas legislaciones utilizando

[103] Según lo establece el artículo 25, sin embargo la misma ley dispone los casos de difusión sin consentimiento, el artículo 34 regula los supuestos, por ejemplo: a. "*Cuando fuere necesario por razones estadísticas, científicas o de interés general, siempre que no se identifique a la persona a quien se refieran"*… entre otros.

los términos: vida privada, y tiene su regulación jurídica, a su vez en algunas leyes secundarias, que tutelan la confidencialidad, los datos personales, incluso la libertad, como parte de la dimensión del derecho fundamental a la intimidad.

3.4.1. República de Argentina

3.4.1.1. Constitución

En argentina se reconoce el derecho a la protección integral de los datos personales, en el artículo 43 inciso tercero, de la constitución expresa: *"Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística"*.[104]

Al manifestar la disposición en comento: "esta acción" se refiere al proceso de amparo, según el inciso 1 de la misma disposición, así regula el habeas data, la norma suprema reconoce el derecho a la protección de los datos personales, entendida esta como parte de la intimidad, porque es información de exclusivo conocimiento del titular, y que la única forma de accesar a ella, es que el autorice.

Por lo tanto corresponde a los poderes públicos organizar y tutelar el habeas data, sin embargo el inciso transcrito no establece expresamente los derechos que se tutelan, solo manifiesta los supuestos de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o la

[104] Constitución de la República de Argentina (Argentina, 1853).

actualización de los datos personales.

La falta de especificación en cuanto al derecho tutelado causo en un primer momento, diversas interpretaciones, un sector sostenía que sólo se tutelaba el derecho a la intimidad y otro que la tutela es el derecho a la intimidad, la imagen, el honor, la identidad, la libertad informática, la reputación. Pero con la entrada en vigencia de la ley 25.326 de Protección de los Datos Personales, permite determinar los derechos tutelados, el artículo 1, establece el objeto de la ley, es decir, la protección integral de los datos personales, garantizando el derecho al honor y a la intimidad de las personas, y el acceso a la información de los registros de sus datos públicos o privados.[105]

3.4.1.2. Legislación penal

El código penal de la nación argentina, está vigente desde abril del año 1922. Tutela como bien jurídico protegido: la libertad que reclama el derecho de conservar, reservar lo que se piensa, hace, tiene o soporta, como parte de la intimidad, para la legislación argentina se trata de proteger la manifestación de la libertad individual, prohibiendo la intromisión de terceros en la intimidad de las personas.[106] Tipifica en su artículo 153 la siguiente conducta: *"Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una*

[105] Matilde Susana Martínez, *Protección de datos y habeas data: una visión desde Iberoamérica* (Madrid: Agencia española de protección de datos, 2015), 26.
[106] Diego J. Avaca, *Código penal Comentado y Anotado parte especial* (Argentina: Andrés José d' Alessio, la ley, 2004) 358.

correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica…"[107]

El tipo penal sanciona, en el primer inciso con prisión de quince días a seis meses, al que ejecute cualquiera de los verbos rectores, a su vez el inciso final establece una agravación en la pena, al establecer la sanción de prisión de un mes a un año, si el autor del delito también comunicare a otro o publicare el contenido.

El sujeto activo puede ser cualquier persona, es decir, que no requiere una calidad especial. La acción típica, se ejecuta al abrir ilegítimamente una correspondencia cerrada, la cual podría ser una carta, un pliego, un despacho u otro papel privado, así como las comunicaciones electrónicas.

El término "indebidamente" que este tipo penal utiliza, nos refleja que están excluidas las acciones de protección a sistemas informáticos, como antivirus, algoritmos para correos electrónicos que desvían los mensajes spam o correos no deseados. La acción consiste en abrir la correspondencia para el caso electrónica, sin tener el derecho. Lo anterior permite determinar que, el tipo penal prohibitivo reconoce las causas de justificación, como podría ser el

[107] Código Penal, artículo 153 (Argentina, 1984).

cumplimento de un deber, el ejercicio de un derecho, al utilizar el término indebidamente, admite, así, abrir la correspondencia, cuando medie por ejemplo, autorización judicial, para la investigación de delitos.

El artículo153 BIS del mismo código penal, establece: *"Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.*

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros o de un proveedor de servicios públicos o de servicios financieros".[108]

La descripción antes referida es lo que en derecho comprado, se denomina: intrusismo informático o hacking, llamado en la legislación argentina como acceso ilegítimo a un sistema informático. Al cometer el delito, por parte del sujeto activo, se transgrede la confidencialidad de la información, en cuanto a la intimidad. El tipo penal describe una conducta que únicamente puede ejecutarse, en relación con un sistema informático de datos, como objeto sobre el cual recae la acción típica del delito. Precisamente el delito en comento, describe la conducta utilizando, el término: sistema o dato informático de acceso restringido, transgreden la intimidad del titular, que no ha manifestado su consentimiento para que un tercero conozca la intimidad contenida en dichos sistemas ya sea como parte de un organismo público estatal o de un proveedor de servicios públicos o del sistema bancario.

[108] Ibíd., art. 153 bis.

3.4.2. República de Colombia

3.4.2.1. Constitución

La Constitución de Colombia reconoce el derecho a la intimidad, en el párrafo primero del artículo 15 de la norma suprema colombiana expresa lo siguiente: *"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas."*[109] El artículo en comento protege la intimidad de las personas, obligando al estado a respetarla y hacerlo respetar, su finalidad es resguardar la esfera de la vida privada personal y familiar, de personas ajenas y de cualquier clase injerencias, sin el consentimiento del titular.

Como la médula central del derecho a la intimidad, es el área intangible, que tiene que ser inmune a intromisiones externas, permitiendo establecer que nadie puede ser obligado a oír o a ver lo que no quiere, así como el derecho a no ser escuchado o visto cuando no lo ha autorizado.[110] Asimismo, reconoce la protección del derecho a un buen nombre, según su jurisprudencia constitucional, es la reputación o fama de una persona, el derecho al buen nombre, está vinculado a los actos que realice una persona en el conglomerado social.[111] A su vez, el artículo en comento reconoce la protección de los Datos Personales, es decir, el denominado Habeas Data, como un derecho fundamental, mediante el que, toda persona tiene el derecho de conocer, actualizar y rectificar toda clase de información que esté contenida en los bancos o bases de datos electrónicos, por lo general en

[109] Constitución de la República de Colombia (Colombia, 1991).
[110] Sentencia No. T-530/92.
[111] Sentencia T-129/10.

archivos de entidades públicas y privadas. De la redacción de la disposición constitucional el derecho a la Intimidad, se interrelaciona con derechos como el del buen nombre y el habeas data, protegidos por el Estado.

3.4.2.2. Legislación penal

El código penal de Colombia, fue creado en julio del año 2000. Respecto al derecho a la intimidad, regula tipos penales informáticos que lo protege, es así, que el bien jurídico tutelado, es el derecho fundamental a la intimidad y la visión ius-informática.

El artículo192 tipifica el delito de violación a la intimidad, reserva e interceptación de comunicaciones, que a la letra expresa: *"El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de dieciséis (16) a cincuenta y cuatro (54) meses, siempre que la conducta no constituya delito sancionado con pena mayor.*

Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será prisión de treinta y dos (32) a setenta y dos (72) meses".[112]

El delito en comento, contiene dos tipos: unos simple y otro agravado, así, en el inciso primero se encuentra el simple, estableciendo la sanción de prisión de dieciséis a cincuenta y cuatro meses, siempre que la conducta no constituya delito sancionado con pena mayor. La acción típica del tipo penal se estructura con los siguientes verbos alternativos para el tipo penal básico: sustraer, ocultar, extraviar, destruir, interceptar, controlar o impedir

[112] Código Penal de Colombia, (ley 599 de 2000).

ilícitamente, una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, que vulneraria la intimidad personal.

Se describe una pluralidad de acciones, y con una misma consecuencia jurídica, lo que en doctrina se le denomina tipo penal compuesto. Pero si para ejecutar la conducta se utiliza medios electrónicos, telemáticos o informáticos, se está, ante un delito informático relativo a la intimidad, el inciso segundo establece la agravación, a la pena de prisión a treinta y dos a setenta y dos meses, si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro. Asimismo en esta legislación ubicamos la ley 1273-2009, que tipifica como delitos conductas relativas a los datos personales. El artículo 269-A, regula el delito de acceso abusivo a un sistema informático, que a la letra dispone: "*El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes."*

Así, este delito tutela el bien jurídico denominado: la protección de la información y de los datos, vinculado con la intimidad, porque es información y datos personales de carácter sensible que no están a disposición de cualquier persona. Este delito es una modalidad de intrusismo informático, porque la acción típica se ejecuta al accesar de forma virtual, (es decir que por la naturaleza del delito no puede ser físico, tendría que ser lo que en informática se denomina hacking), sin autorización o por fuera de lo acordado, en todo o en parte a un sistema informático, abusos de terceros (ingresar a cuentas de correo electrónico ajenas) protegido o no con una

medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

El tipo penal establece el término; el que, es decir, que cualquier persona, puede ser sujeto activo, el delito no exige calificación especial respecto al que lo ejecute, sin embargo, estas acciones por lo general son ejecutadas por los denominados; hacker, pero para el delito en comento es suficiente con que sea un intruso. Asimismo el tipo penal establece como, sanción la pena de prisión de cuarenta y ocho a noventa y seis meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. En cuanto al sujeto pasivo, por la redacción del tipo, sirve para determinar, que es toda persona titular del medio informático que resulta objeto material del delito, cuando accede un tercero de forma abusiva, asimismo puede ser sujeto pasivo, el titular de los datos personales, sensibles o secretos almacenados en archivos o bases de datos, al que se le ha transgredido la intimidad personal, lo que permite, establecer que esta conducta constituye una especie de intrusismo informático.

3.4.3. República de Chile

3.4.3.1. La Constitución

La Constitución de Chile, fue creada en el año de 1980. En su capítulo III denominado los Derechos y Deberes Constitucionales, reconoce la protección a la intimidad, sin embargo no se utiliza este término, porque emplea, el de vida privada, en el artículo 19 ordinal cuarto y quinto manifiesta: *"La Constitución asegura a todas las personas:*

4° El respeto y protección a la vida privada y a la honra de la persona y su familia.

5°. La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados

interceptarse, abrirse o registrarse en los casos y formas determinados por la ley".[113]

El reconocimiento y protección constitucional, de los intereses propios a la privacidad se plasman en esté texto constitucional, con el respeto y la protección a la vida privada, a la inviolabilidad del hogar y de toda forma de comunicación privada. El interés jurídicamente protege la no intromisión en la vida propia, en su dimensión corporal, familiar y espacial, y a su vez la información relativa a una persona.

La doctrina chilena entiende por privacidad a la manifestación jurídica del respeto y protección que se debe a cada persona, protegiendo la dignidad y libertad humana, otorgando al titular poder de control en su ámbito de la vida del que no participan otras personas.

Asimismo, la privacidad se refiera a los derechos, constitucionales y legales, relacionados con el de poder de control, en la vida privada, la inviolabilidad de las comunicaciones y la protección de sus datos personales.[114]

3.4.3.3. Legislación penal

En la legislación de Chile se encuentra el código penal, creado en noviembre del año 1874. En su título III, número 5, establece los delitos relativos al respeto y protección a la vida privada y pública de la persona y su familia. Tutelando el bien jurídico la vida privada, mediante el artículo 161-A que regula el delito de violación de la privacidad, a la letra expresa: *"Se castigará con la pena de reclusión menor en cualquiera de sus grados y multa de 50 a*

[113] Constitución de la República de Chile, art. 19, n. 4,5 (Chile, 1980).
[114] Carlos Lara, *La privacidad en el sistema legal chileno,* (Chile: ONG Derechos Digitales, 2005), 12.

500 al sujeto que sin autorización del afectado y por cualquier medio, capte, intercepte, grabe o reproduzca conversaciones o comunicaciones de carácter privado; sustraiga, fotografié, fotocopie o reproduzca documentos o instrumentos de carácter privado; o capte, grabe, filme o fotografié imágenes o hechos de carácter privado…"[115]

En cuanto al sujeto activo, el tipo penal no requiere de una calificación especial, para ejecutarlo solo exige realizar cualquiera de los verbos rectores, así, al captar y reproducir hechos de la vida privada, sin el consentimiento del titular, por ejemplo, instalando cámaras o micrófonos ocultos. El inciso primero del artículo 161-A, tipifica conductas, que transgreden el secreto contenido en una conversación, utilizando para su ejecución cualquier medio tecnológico, la captación sustracción, fotografiar, fotocopiar, sin el consentimiento expreso del titular, transgrede el derecho a la intimidad, porque ingresa al área exclusiva de otra persona, de forma clandestina que podría ser en lugares públicos o privados, introduciéndose en la vida privada de otros. El inciso primero impone la sanción de pena de reclusión menor en cualquiera de sus grados y multa de 50 a 500. Asimismo es necesaria la naturaleza privada de las comunicaciones, los documentos y las imágenes, y que la interceptación o captación, la grabación, se ejecute sin el consentimiento del titular, afectando su derecho a la intimidad personal.

Ley No:19223, creada el 28 de mayo del año de 1993.Tipifica conductas relativas a los delitos informáticos, está ley tutela como bien jurídico protegido por el derecho penal, la confidencialidad, asimismo regula un catálogo de delitos, de los que únicamente por el objeto de investigación se tratara el delito tipificado en el artículo 2, este expresa: *"El que con el ánimo*

[115] Código Penal, articulo 161. A (Chile, 1874).

de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".[116]

El tipo penal regula la intromisión en la información a la que no tiene por qué tener acceso lícitamente. Este delito regula conductas orientadas a realizar los accesos no autorizados, en cuanto a la conducta, el tipo penal se integra de tres formas de acciones alternativas, es decir los verbos rectores son: interceptar, interferir y accesar, todas a un sistema informático de tratamiento de información. Respecto a la palabra interceptar se refiere a la información contenida y transmitida en un sistema de tratamiento informático, incorporal no es solo apoderarse, usar o conocerla. Dentro de este verbo se adecua la interceptación de datos contenidos en redes inalámbricas wifi no encriptados o no codificados por sus propietarios.

El verbo rector interferir, consiste en la interposición o superposición de señales ópticas, acústicas, electrónicas, magnéticas, u ondas de que resulta en ciertas condiciones, aumento, disminución o neutralización de los impulsos magnéticos. En cuanto al verbo acceder, es la acción de ingresar al sistema de tratamiento de información desde un disco o desde cualquier otro medio, al acceder, se utiliza el denominado hacking para que constituya un acceso indebido,[117] y por tanto intrusismo informático, vulnerando la confidencialidad como parte de la intimidad, porque se está invadiendo el espacio virtual del sujeto pasivo, en el que desarrolla sus actividades, libre de injerencias de terceros.

[116] Ley Relativa a Delitos Informáticos, LEY No. 19223 (Chile).
[117] Romina Moscoso Escobar, "La Ley 19.223 en general y el delito de hacking en particular". *centro de estudios de derecho informático*, Vol. 3 N.1 (2014), 33. goo.gl/q6zOjz.

CAPÍTULO IV
ANÁLISIS DOCTRINAL DE LA INTERVENCIÓN DEL DERECHO PENAL EN LA INTERNET

El presente capitulo tiene como propósito desarrollar un análisis de la intervención del Derecho Penal en la Internet, estableciendo el Bien Jurídico protegido que surge producto de la utilización de tecnología, los problemas de persecución que presentan los delitos informáticos, los aspectos, características, y clasificación del delito informático.

4. Ejecución de delitos mediante la internet

4.1. Generalidades del fenómeno

La dimensión de las nuevas tecnologías ha hecho que intervengan en todos los ámbitos de la vida de las personas, haciendo inevitable utilizarlas con fines delictivos.[118] La informática[119] proporciona diversos medios que pueden ser utilizados para ejecutar acciones delictivas, y potencia los efectos de los llamados delitos convencionales.

[118] Luz Gutiérrez Francés, *Fraude Informático y Estafa* (Madrid: Ministerio de Justicia, 1991), 43-44. Sostiene que las modernas tecnologías tienen aplicación en una dimensión negativa de la informática, es decir, los denominados *riesgos* que existen y tienen relevancia jurídico penal, así añade que son los siguientes: el entorno de la información que los nuevos métodos potencian, desarrollan el uso abusivo de la información de los ciudadanos que causa conflictos con el sistema de garantías de un Estado de derecho, con la intimidad de las personas. La informática tiene un entorno común a un bien objeto de trafico jurídico con valor económico, estas características más la vulnerabilidad de los sistemas informáticos del procesamiento transmisión, y almacenamiento, lo sitúan como un medio infinito para ejecutar una gran variedad de delitos. Véase: Manuel Avilés Gómez et al., *Delitos y delincuentes: Cómo son*, cómo actúan, (España: club universitario, 2010), 113-115.

[119] Francisco José Villazán Olivarez, *Manual de Informática I* (México: Universidad Michoacana de San Nicolás de Hidalgo, Facultad de Contaduría y Ciencias Administrativas, 2010), 8. goo.gl/rLtoIo. La informática es la ciencia de la información. El término se forma de la combinación de las palabras información y automática, así, es el conjunto de conocimientos que permiten el tratamiento automático de la información y se utiliza para abordar a todo lo relacionado con el manejo de datos e información mediante las computadoras.

Con el desarrollo y expansión del internet, como un medio de comunicación masiva de datos, adquiere alcances en la vida diaria de las personas, con la ejecución de acciones delictivas en diferentes ámbitos como la intimidad, lo financiero, lo comercial. Lesionando bienes jurídicos protegidos por el derecho penal.[120] Así las acciones delictivas mediante la red,[121] constituyen una adaptación al espacio virtual de los delitos, el derecho penal[122] y sus principios garantistas, esenciales[123] fundamentados en modelos de delincuencia física. Con el surgimiento del internet, la institución encargada de la represión se enfrenta a esta nueva forma de ejecutar delitos.

Las acciones delictivas mediante el internet de acuerdo a la doctrina son difíciles para su detección y persecución porque existe: el anonimato, la falta de conciencia de los usuarios respecto a tener medidas preventivas de seguridad, y la naturaleza transnacional de algunos delitos.[124]

Las acciones ejecutadas mediante la internet, en esencia no son nuevas porque algunas se realizan asimismo por medios materiales, pero el internet es un modo extraordinario de ejecutar delitos, obligando a las legislaciones a

---

[120] Gutiérrez, *Fraude Informático y Estafa*, 43 (Véase la nota 118).

[121] Alfonso Galán Muñoz, *El fraude y la estafa mediante sistemas informáticos* (Valencia: edit. Tirant lo Blanch, 2005), 27. Comenta que se está, ante un nuevo espacio o medio para las relaciones humanas a la que denomina ciberespacio, caracterizado por ser un medio no físico no delimitado, obligando a la creación de nuevas normas jurídicas para estas conductas.

[122] Gonzalo Rodríguez Mourullo, *Derecho Penal: Parte General,* 1a. ed. (Madrid: Edit. Civitas, 1978), 11. Sostiene que el Derecho Penal (ius poenale) es el conjunto de normas jurídicas que a determinadas conductas previstas como delitos se impone penas o medidas de seguridad, al que la ejecuta. El Derecho Penal tiene dos sentidos, un objetivo, es decir como conjunto de normas, y otros en sentido subjetivo como facultad que tiene el Estado de crear delitos e imponer penas y medidas de seguridad a los sujetos que llevan a cabo la conducta constitutiva de delitos.

[123] Principio de intervención mínima, Principio de legalidad, Irretroactividad, Lesividad, entre otros.

[124] Javier Gustavo Fernández Teruelo, *Cibercrimen los delitos cometidos a través de internet* (España: edit. Constitutio Criminalis Carolina, 2007), 13-14.

realizar actualización de los tipos penales, en algunos casos están en el texto de la ley, descritos para acciones físicas, interpersonales, lo que genera una ruptura con los esquemas clásicos que han determinado, la ineficacia de las figuras típicas. Dentro de la amplia gama de acciones delictivas que se puede ejecutar por el internet destacan las relativas a la pornografía infantil, los daños informáticos, los delitos contra la propiedad intelectual, las estafas informáticas, los delitos contra la intimidad,[125] el intrusismo informático, la protección de la dignidad humana.[126]

En la actualidad los delitos ejecutados mediante el internet se desarrollan y cambian al adaptarse a las nuevas formas de tecnología. Así, existen manifestaciones concretas, por ejemplo los accesos no autorizados a bases de datos o a sistemas informáticos ajenos, que consiste en el supuesto de hecho que tiene como finalidad el acceso a un archivo o base de datos protegido por procedimientos lógicos informáticos, por terceros no autorizados, para ello, se refiere asimismo al ingreso, sin autorización del titular a un sistema informático.[127]

4.2. Bien jurídico

La especialidad de las acciones tipificadas como delitos ejecutados a través del Internet y los medios informáticos han irrumpido las actividades de las personas, causando la necesidad de proteger los bienes jurídicos transgredidos.[128] Así, es preciso y pertinente determinar cuál es el bien jurídico tutelado por el derecho penal, por lo que resulta necesario previo a

[125] Ibíd.
[126] Avilés, *Delitos y Delincuentes*, 129 (Véase la nota 118).
[127] Carlos María Romero Casabona, *De los delitos informáticos al cibercrimen. (*España: Universidad de Salamanca, 2007), 649, goo.gl/6kA7eD.
[128] Moscoso, "La Ley 19.223", 14 (Véase la nota 117). La especialidad de los delitos informáticos se basa en la protección que se requiere para la nueva realidad que es el internet.

ello, abordar el tema “bien jurídico”, en sus aspectos generales, sin ahondar. Garrido Montt citando a Franz Von Liszt, lo define como un bien vital de la comunidad o del individuo que por su significación social es protegido jurídicamente, Garrido Montt continua diciendo que la noción de bien jurídico[129], no es un concepto pacífico y asimismo es difícil determinar qué se tiene que entender por tal; así, existen, tres teorías al respecto: a) La trascendentalista; b) La inmanentista, y c) La político-criminal, y, como modalidad de esta última, la dinámico-crítica.[130] A continuación se hará un breve comentario de estas teorías.

4.2.1. Corriente Trascendentalista

Sus representantes más destacados son: Liszt,[131] Welzel, Maurach-Zipf-Gössel y Jescheck. De acuerdo a esta, los bienes jurídicos existen desde antes de la norma penal y son creaciones de la vida (orden social).[132] Se refieren al individuo, es decir bienes individuales y asimismo a la sociedad los denominados colectivos, y no son creados por la ley, son recogidos por esta,

[129] Santiago Mir Puig, *Introducción a las bases del Derecho Penal* (Argentina: Julio César Faira, 2003), 112. El bien jurídico desde mediados del siglo XIX es parte de los conceptos fundamentales del derecho penal.

[130] Mario Garrido Montt, *Derecho Penal: Parte General, Tomo I* (Chile: Editorial jurídica de Chile, 2010), 64. Mediante estas teorías se definen los intereses dignos de protección penal. Superado el criterio de mediados del siglo XIX, en el que se sostenía que el delito lesionaba "derechos subjetivos", como el derecho a la vida, o a la libertad, en abstracto.

[131] Enrique Bacigalupo, *Manual Derecho Penal: Parte General* (Colombia: Temis, 1996), 9. Bien Jurídico es el interés protegido jurídicamente. Todos los bienes jurídicos añade citando a Von Liszt, son intereses vitales, intereses del individuo o de la comunidad: los intereses no los crea el ordenamiento jurídico sino la vida; pero la protección jurídica eleva el interés vital a bien jurídico; y Carlos Fontan Balestra, *Derecho Penal: Introducción y parte general,* (Argentina: Abeledo-perrot, 1998), 23, 24. A los intereses jurídicamente protegidos, se les denomina bienes jurídicos; no nacen del Derecho, por que surgen de la vida, siendo intereses vitales para el individuo y para la sociedad. El Derecho, mediante su tutela, eleva el interés vital a bien jurídico.

[132] Rodríguez, *Derecho Penal: Parte General*, 19 (Véase la nota 122). Afirma que sólo se puede configurar, si primero se establece que se tiene que entender por “bien” añade que este perteneciente a la teoría general de los valores y que es todo aquello que satisface las necesidades físicas, intelectuales o morales del hombre, y en la medida en que el Derecho protege a los bienes, éstos se convierten en bienes jurídicos.

lo que le dota de la calidad de jurídicos.[133]

4.2.2. Corriente Inmanentista

El principal exponente de esta teoría es Binding, esta corriente se basa en el supuesto que los bienes jurídicos subyacen en la norma jurídica, determinándolos y regulándolos. Así, el Estado es el que crea las normas, de tal forma que es, el creador de los bienes jurídicos.

Garrido Montt comenta que esta concepción, equipara a la corriente trascendentalista, y no da importancia definitiva al bien jurídico, a la lesión del interés por la ejecución del hecho delictivo; lo determinante es la desobediencia del mandato establecido por el Estado.[134]

4.2.3. Tendencia Político-Criminal

Esta tendencia se fundamenta en la corriente trascendentalista, porque su nacimiento en la doctrina está en el pensamiento político-criminal de Liszt, que se centra en el hombre, y no en el Estado, al derecho penal. En el pensamiento trascendentalista surgen la corriente constitucional y la sociológica. El pensamiento constitucionalista, tiene como fin determinar cuáles son los límites del ius puniendi,[135] encontrándolos en los derechos fundamentales plasmados en la Constitución, estos derechos constituyen los intereses (bienes) jurídicos que se tienen que respetar y dirigen la

---

[133] Montt, *Derecho Penal: Parte General*, 64 (Véase la nota 130); Rodríguez, *Derecho Penal: Parte General*, 19 (Véase la nota 122). Afirman que en la medida en que el Derecho protege a los bienes, éstos se convierten en bienes jurídicos.

[134] Montt, *Derecho Penal: Parte General*, 66 (Véase la nota 130).

[135] Pablo Sánchez et al., *El sistema español: Los Delitos* (España: Universidad de Navarra), goo.gl/PtVlEp. Así, el bien jurídico cumple lo que en doctrina se denomina función, político-criminal, que sirve para determinar los límites a la acción del legislador cuando define conductas como delitos y la intervención del Estado, lo que en Derecho penal garantista impone límites al ius puniendi, en cuanto no sometido al ius poenale.

interpretación de la ley represiva. Por otro lado el pensamiento sociológico se funda en el funcionalismo, respecto a la incorporación de los intereses políticos a los principios normativos para la determinación del merecimiento de pena y de su ejecución.

De acuerdo a esta tendencia los bienes jurídicos, limitan la facultad de castigar del Estado, en un contexto político-criminal liberalizador, así, sostiene que se debe calificar como bienes jurídicos exclusivamente a las "condiciones elementales de la vida social, que afectan las eventuales participaciones de los individuos en el sistema social".[136]

4.2.3.1. Teoría dinámico-critica

Esta teoría sostiene que el bien jurídico es un instituto cambiante, no ahistórico, e identificable con creaciones de naturaleza racionalista. Garrido Montt comenta que existe una corriente que radicaliza a esta tendencia de la siguiente forma: el bien jurídico es personal; independientemente se refiera a la persona o al sistema social, pero siempre se tienen que referir a la persona. Asimismo, sostiene que el bien jurídico es un elemento legitimador de la intervención del Estado porque garantiza los derechos; pero a su vez es deslegitimador de su intervención cuando el Estado no los tiene en cuenta. Asimismo afirman que el bien jurídico es una noción dialéctica, político-jurídica, que expresara la lucha por la democracia en permanente análisis ante la realidad social concreta.

Esta corriente tiene como uno de sus principales exponentes a Juan Busto, de acuerdo a él un bien jurídico "es una síntesis normativa determinada de una relación social concreta y dialéctica".

[136] Montt, *Derecho Penal: Parte General*, 66 (Véase la nota 130).

Expuesto estas teorías, se tomará en cuenta lo que establece Von Liszt es decir la teoría trascendentalista, al respecto de "bien jurídico" este puede ser definido como un interés vital para el desarrollo de los individuos de una sociedad determinada, que adquiere reconocimiento jurídico.

De la definición anterior se colige que el bien jurídico es: a) Un interés vital que preexiste al ordenamiento normativo, pues tales intereses no son creados por el derecho sino que éste los reconoce, y, mediante ese reconocimiento, es que esos intereses vitales son bienes jurídicos;[137] b) la referencia a la sociedad determinada señala que ese interés que es fundamental en un determinado grupo social y en un contexto histórico, puede no serlo en otro, por esa razón es discutible la idea de la existencia de intereses universales y eternos; c) la noción de que el bien es un interés reconocido por el ordenamiento jurídico obliga a preguntar qué rama del ordenamiento jurídico es la que "crea" los bienes jurídicos,[138] es decir, la que reconoce intereses fundamentales, ¿lo es el derecho penal? La respuesta es negativa, el derecho penal no crea bienes jurídicos, sino que se limita a sancionar con una pena a ciertas conductas que lesionan ciertos bienes de cierta forma.[139]

---

[137] Nicolás García Rivas. *El Poder Punitivo en El Estado Democrático* (Cuenca: Universidad de Castilla - La Mancha, 1996), 28, goo.gl/BfAE6N. Von Liszt se expresó de la siguiente manera: "Nosotros llamamos bienes jurídicos a los intereses protegidos por el Derecho. Bien jurídico es el interés jurídicamente protegido. Todos los bienes jurídicos son intereses vitales del individuo o de la comunidad. El orden jurídico no crea el interés, lo crea la vida; pero la protección del Derecho eleva el interés vital a bien jurídico".

[138] Eugenio Raúl Zaffaroni et al., *Derecho penal: Parte general,* 2° Edi. (Buenos Aires: Ediar, 1977) 98, 486. "...la legislación penal no crea bienes jurídicos, sino que éstos son creados por la Constitución, el derecho internacional y el resto de la legislación. (…) La ley penal sólo eventualmente individualiza alguna acción que lo afecta de cierto modo particular, pero nunca puede brindarle una tutela amplia o plena, dada su naturaleza fragmentaria y excepcional".

[139] Mariano Kierszenbaum, "El Bien Jurídico En El Derecho Penal. Algunas Nociones Básicas Desde La Óptica De La Discusión Actual", *Universidad de Buenos Aires,* (2009), 188-189, goo.gl/OcNpsE.

4.3. Bien jurídico Tutelado

4.3.1. La Intervención Penal en internet

Como se dijo el bien jurídico no es creado por el derecho, el bien jurídico nace de una necesidad de protección a ciertos y cambiantes bienes inmanentes a las personas como tales, esta protección es catalizada por el constituyente al recogerlas en el texto constitucional, de la cual existirían bienes cuya protección será cumplida por otras ramas del derecho, es decir que no todos los bienes jurídicos contenidos en la constitución tienen una protección penal, existen bienes jurídicos de tutela civil, laboral, administrativa, etcétera, al determinar cuáles son los bienes jurídicos que merecen tutela penal siempre se tendrá en cuenta el principio de tener al derecho penal como última ratio o última opción para la protección de un bien jurídico ya que este afecta otros bienes jurídicos a fin de proteger otros de mayor valor social.[140]

Gonzales Rus manifiesta que existen dos criterios respecto a la intervención del derecho penal en las acciones realizadas mediante el internet; uno sostiene que hay que incorporar a la tutela penal los nuevos bienes jurídicos que surgieron como producto de los medios y procedimientos informáticos, intereses, que merecen la protección del derecho penal, teniendo en cuenta que la regulación de conductas en el derecho penal son insuficiente para enfrentar los problemas de punición que presenta el internet y las redes de transmisión de datos. El segundo criterio es partidario de agotar las posibilidades de protección que tiene el derecho vigente, fundamentándose en los bienes jurídicos tradicionales, e introducir reformas concretas y necesarias a estos. [141]

[140] Derecho en Red, “Bien jurídico” (2011), goo.gl/5R42lo.
[141] Juan José Gonzales Rus et al., *Delito e informática: algunos aspectos*, (España: Universidad de Deusto, 2017), 13-14.

4.3.1.1. Intervención penal apoyada en los bienes jurídicos "nuevos" de naturaleza informática

Según este criterio la intervención del derecho penal en Internet no se puede realizar fundamentándose en los bienes jurídicos que actualmente están protegidos por el derecho penal, porque la especialidad del medio, la extraordinaria expansión sobrepasada por Internet y las redes de transmisión de datos, la gran cantidad de usuarios y las relaciones que se crean mediante las mismas, es motivo para que necesariamente se proporcione protección a los nuevos bienes jurídicos, que implicarían el reconocimiento y protección de los intereses personales y sociales que se desarrollan por el Internet.

Gonzales Rus cita a Picotti: sostiene que por el desarrollo tecnológico han surgido nuevos intereses, que son merecedores de una especial y autónoma tutela jurídica mediante el derecho penal. Son bienes jurídicos nuevos, que la ley penal no ha protegido y no existe una correspondencia con otros bienes jurídicos preexistentes.[142] Ese es el criterio más admitido por la doctrina, y sostiene que dichos bienes serían: la seguridad informática, la información y la libertad informática. Son bienes jurídicos que manifiestan la necesidad de protección mediante el derecho penal, de forma especial y autónoma, en relación con los bienes jurídicos personales con los que se vinculan.

Asimismo, se relacionan respecto al Derecho Penal de la informática incluyen los bienes jurídicos tradicionales, que, están adheridos en el medio informático o relacionados, obteniendo una dimensión nueva que los diferencian de su sentido original en el ámbito del Derecho Penal general.[143]

[142] Ibíd., 14.
[143] Ibíd., 15.

4.3.1.1.1. La seguridad informática como nuevo bien jurídico protegido

La seguridad informática como un bien jurídico colectivo da protección anticipada a otros de naturaleza personal como la intimidad, el honor, el patrimonio, la libertad de información, el secreto y la inviolabilidad de las comunicaciones; pero no siempre se puede determinar cuáles son los derechos relacionados con ella. Este bien jurídico se transgrede cuando se utilizan el internet o sistemas informáticos, para cometer delitos, por ejemplo acceso indebido a un ordenador, atentando contra la intimidad. Se afirma que es un bien jurídico colectivo e indisponible, porque las transgresiones a la seguridad informática producen riesgos a los usuarios y no respecto de un sujeto concreto.[144]

La doctrina italiana respecto al bien jurídico que tiene protección en cuanto a la integridad y seguridad informática sostiene que tiene trascendencia práctica y autonomía por la creciente dimensión de los vínculos desarrollados mediante la informática. Asimismo afirma que es un concepto que intenta de forma anticipada y preventiva la protección, en cuanto a lesionar la integridad y posibilidad de emplear los datos, sistemas y productos informáticos, o, de un daño concreto, de todos los dispositivos, medidas, procedimientos instrumentales de protección.[145]

Este nuevo bien jurídico es criticado en el derecho español porque la seguridad informática no tiene todavía, un contenido sustancial adecuadamente elaborado y preciso para crear una tutela penal. Porque unas veces se relaciona con el honor, el patrimonio y la intimidad, asimismo, con la libertad de información, el secreto de las comunicaciones, la libertad

[144] Ibíd., 15.
[145] Ibíd., 16.

de expresión, que expresa ambigüedad del concepto, porque no se determina, que es lo que se tutela.[146] Así, González Rus, manifiesta que si no existe precisión al establecer cuál es el objeto de protección, especialmente, considerando que las acciones que se tienen que prohibir en el tipo penal, para la protección del bien jurídico seguridad informática, están incorporadas en modalidades delictivas, reguladas con la protección de bienes jurídicos tradicionales por el derecho penal.[147]

4.3.1.1.2. Libertad informática como nuevo bien jurídico protegido

La libertad informática como bien jurídico, su contenido central es dotado por el derecho del individuo a decidir qué información personal será divulgada. Es un derecho que complementa el tradicional de la intimidad. No es solamente el derecho a excluir un determinado ámbito que el titular considera reservado, ante intromisiones, es el poder positivo de control de la información personal, para su uso. Es así el denominado habeas data o derecho de autodeterminación informativa.[148]

4.3.1.1.3. La información como nuevo bien jurídico protegido

Santiago Acurio del Pino sostiene que el bien jurídico protegido,[149] es la información, pero está desde diferentes aspectos, es decir: como valor económico, como un valor intrínseco de la persona, por su movimiento y

[146] Ibíd., 21.
[147] Ibíd.
[148] Ibíd., 18.
[149] Santiago Acurio Del Pino, *Delitos Informáticos: Generalidades* (Ecuador: Pontificia Universidad Católica del Ecuador, 2007), goo.gl/2nv7gv, 20; Magaly Vázquez Gonzales, *Ciencias penales, temas actuales: homenaje al R.P. Fernando Pérez Llantada*. (Caracas: Universidad Católica Andrés Bello, 2004), 584, goo.gl/M87f1H. La utilización de sistemas tecnológicos de información ha permitido que los delitos afecten diversos bienes jurídicos en los que tales sistemas se usan como medio para su comisión, esto ha generado la aparición de un nuevo bien jurídico es decir, la información en la medida que es ilegal acceder, interceptar, modificar, divulgar, revelar, los datos contenidos en un sistema informático.

tráfico jurídico, y por último los sistemas que la procesan; este autor ha manifestado que el bien jurídico protegido incluye a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos en estos se almacena o transfiere información. En este sentido afirma que los delitos informáticos son pluriofensivos o complejos, es decir que protegen varios intereses jurídicos, sin perjuicio que uno de los bienes este independientemente tutelado por otro tipo.[150]

4.3.1.2. Intervención penal apoyada en bienes jurídicos informáticos por transformación de su sentido originario

Otra teoría de la doctrina sostiene que los bienes jurídicos tradicionales y los propios de las acciones y delitos informáticos no son diferentes. Esta teoría se fundamenta en que los bienes jurídicos tradicionales, como elementos informáticos se transforman y esta le proporciona un contenido diferente del original.[151]

Se considera que la transformación sustancial de los bienes jurídicos se generaría: en los tradicionales,[152] cuando se protegen contra nuevas formas de transgredir los bienes jurídicos mediante procedimientos informáticos; en los bienes jurídicos análogos surgidos de nuevos objetos materiales de la conducta. Cuando en la acción ejecutada se utilizan objetos, procedimientos o conductas de naturaleza informática, surgen nuevas formas de ejecutar

[150] Del Pino, *Delitos Informáticos: Generalidades,* 21 (Véase la nota 149).
[151] Ibíd.
[152] Ibíd., 20. Respecto a los delitos informáticos, en cuanto a esta teoría, sostiene lo siguiente: la protección a los bienes jurídicos, se realiza desde la perspectiva de los delitos tradicionales, mediante una interpretación teleológica de los tipos penales por que existen, para subsanar las lagunas producidas por las novedosas acciones delictivas. Así, por lo general los bienes jurídicos protegidos, son los mismos que los delitos reinterpretados teleológicamente o que se les incorpora un elemento nuevo para su persecución y sanción por parte del órgano competente.

delitos es decir se pueden transgredir los bienes jurídicos tradicionales mediante el internet.[153]

4.4. Respecto a legislación salvadoreña

El bien jurídico protegido, por la Ley Especial Contra Delitos Informáticos y Conexos, según dispone el artículo 3 d): "es la información que garantice y proteja el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros." De lo anterior, se permite determinar que el bien jurídico protegido por la Ley especial es la información, por lo que el legisferante retoma lo que plantea Von Liszt, y activa un nuevo bien jurídico, esto debido a la necesidad imperiosa de proteger la información que se maneja en las redes. Cabe destacar que los tipos penales que contiene la ley son de naturaleza pluriofensivos, es decir, que con su ejecución se transgrede más de un bien jurídico a la vez.

4.5. Problemas de persecución establecidos por la doctrina

Un tema aparte de las deficiencias en la creación de los tipos penales son las dificultades respecto a la investigación de esta forma de delincuencia; específicamente por los factores que causan dificultad en la detección y persecución del delito ejecutado mediante el internet. Así, entre los factores está el anonimato potencial de autor y la ejecución a distancia. En cuanto al anonimato, las dificultades que existen para detectar la ejecución de un delito mediante el internet, porque encontrar quien es el autor de la acción constitutiva de delito no es sencillo. Pero cada ordenador tiene asignada su propio protocolo de internet -en adelante IP-, al conectarse a internet, su rastreo y detección en la mayoría de casos, no es complejo. Sin embargo los

[153] Rus, *Delito e Informática: algunos aspectos*, 19 (Véase la nota 141).

actuales protocolos IP no garantizan en todos los casos la determinación de la dirección del emisor, porque la misma puede ser modificada.[154]

Así, un sector de la doctrina considera que los delitos informáticos son de difícil investigación porque su forma de ejecución es novedosa sobresaliendo de los medios tradicionales de investigación, porque en el medio digital es difícil detectar los rastros, siendo dificultoso imputar las acciones, así, por ejemplo: hackers de Hannover en Alemania, provocaron que durante algunos meses, los administradores de la red de computadoras del sistema informático de los laboratorios de Lawrence Berkeley de California, detectaran los rastros informáticos que dejaban los hackers, provenientes desde Hannover. El trayecto que utilizaban estos hackers fue muy extenso, de Hannover llamaban a la universidad de Bremen, mediante la red alemana Datex-P, y posteriormente tenían acceso a la red americana Tymnet, desde la cual accedían a las computadoras del laboratorio Berkely ubicadas en California. Desde allí se conectaban con la red militar, desde donde accedían a los archivos secretos para venderlos al Comité para la Seguridad del Estado, o más comúnmente KGB.[155]

4.5.1. Delitos a distancia competencia territorial

Al ser delitos a distancia, causan dificultades como parte del medio utilizado, que permite cometer el delito, así, la acción constitutiva de delito puede tener

[154] Teruelo, *Cibercrimen los delitos,* 14 (Véase la nota 124); Rus, *Delito e Informática: algunos aspectos*, 239 (Véase la nota 141). Una dirección IP (Internet Protocol, Protocolo de Internet) es un conjunto de cuatro números separados por puntos con un valor que puede oscilar entre el 0 y el 255. Los ordenadores se identifican entre sí mediante la IP, una red determinada no pueden coincidir dos IP's, porque los ordenadores remiten la información mediante paquetes y protocolos para tales fines, que anotan entre otros datos, las direcciones IP del emisor y del receptor, para que la comunicación pueda realizarse.

[155] Marcelo Huerta et al., *Delitos informáticos* (Argentina: Ed. ConoSur Ltda., 1998), 70-71. Para conocer cómo se infiltraron en las computadoras del laboratorio véase: Fernando Bonsembiante et al., "*Llaneros Solitarios" Hackers, la Guerrilla Informática* (Argentina: Espasa Calpe, 1995), 25-27.

su ejecución en uno o varios países[156] y los resultados pueden producirse, en otro u otros.[157] Es difícil determinar desde que lugar se ejecutó la acción porque la conducta se realiza mediante el internet. Un sector de la doctrina plantea un problema de jurisdiccionalidad y competencia sobre el delito.[158] Generando un problema al determinar desde que lugar se ejecutó el delito. En consecuencia la determinación del territorio o lugar en que se cometió el delito es esencial para determinar la ley que se aplicara.[159] Los delitos informáticos son denominados asimismo por la doctrina como delitos a distancia, es decir, aquellos en los cuales pueden separarse de la acción delictuosa el resultado, por la extensión espacial, así, por ejemplo un software se puede programar en cualquier lugar del mundo y puede producir sus efectos en cualquier parte del planeta, mediante la interconexión entre las computadoras por el internet, así mismo los virus informáticos son creados en otros países pero producen sus efectos en otros estados.[160] Un keylogger[161] que capta teclados, recopila la contraseña de correos electrónicos, de cuentas bancarias, desde una computadora del país la puede enviar hasta su creador en cualquier parte del mundo.

La extraterritorialidad plantea problemas para determinar quién es el juez

---

[156] Miguel Ángel Davara Rodríguez, *Manual de Derecho Informático* (España: Thomson Aranzadi, 2006), 369. Afirma que una de las características fundamentales de las acciones delictivas ejecutadas por medios informáticos es la rapidez y el acercamiento en el tiempo y espacio, que aporta el sistema informático; Rodolfo Herrera Bravo, "Reflexiones sobre la delincuencia vinculada con la tecnología digital (basadas en la experiencia chilena)", goo.gl/5OOe4H, 19. Para Herrera Bravo el Derecho Penal tiene un reto en los fraudes, los sabotajes y en el espionaje informático, cuando son ejecutados a través de la telemática, porque es lo que denomina un delito informático internacional, transfronterizo.

[157] Calonge, *Internet, Intimidad y Privacy,* 65 (Véase la nota 70). Los delitos a distancia ejecutados a través de cualquier medio de comunicación inclusive el internet, tienen su resultado en cualquier parte del mundo.

[158] Teruelo, *Cibercrimen los delitos,* 20 (Véase la nota 124).

[159] Ibíd., 21.

[160] Huerta, *Delitos Informáticos*, 72 (Véase la nota 155).

[161] Rus, *Delito e Informática: algunos aspectos*, 23 (Véase la nota 141). Keylogger es un software programa para captar las pulsaciones de un teclado permitiéndole al sujeto programador obtener claves de usuario, contraseñas o números de tarjetas de crédito o todo lo que se pulse por el teclado.

competente que tiene que sustanciar el proceso, pero la leyes resuelven en algunos casos este problema, así, en Estados Unidos que en sus leyes estaduales[162] sobre delitos informáticos, permite procesarlos en cualquier estado en este país se denomina “long arm statutes”, es decir leyes de gran alcance. Otras leyes son más extensas por ejemplo la ley de delitos informáticos de Malacia del año 1997 establece que se aplicara a cualquier individuo, independientemente, de su nacionalidad e incluso regula que tendrá efectos en el exterior.[163]

4.5.2. Competencia Territorial y Persecución Penal

En los casos cuando la conducta y el resultado se ejecutan en distintos países, trae aparejado el problema de determinar el lugar de comisión del delito, surgen problemas respecto a la aplicación de la ley penal y para solucionarlo la doctrina dispone de tres teorías: la de la voluntad, resultado y ubicuidad, a continuación se elabora un breve cometario.

4.5.2.1. La teoría de la voluntad

Esta teoría dispone como lugar de comisión en el cual el sujeto ha realizado la acción u omisión delictiva. Lo esencial es la manifestación de su voluntad, la acción, la exteriorización objetiva del querer interno. Se critica afirmando que no soluciona los problemas de los delitos a distancia, en los cuales la producción del resultado es en otro territorio al de la actividad.

4.5.2.2. Teoría del resultado

Considera que el delito es cometido en el territorio en que se produce el resultado de la acción del sujeto. Se critica porque no puede dar respuesta a

[162] Las leyes estaduales son las dictadas por cada uno de los Estados federados, con vigencia en su territorio.
[163] Huerta, *Delitos Informáticos*, 73 (Véase la nota 155).

los casos de tentativa.[164]

4.5.2.3. Teoría de la ubicuidad

Para superar las deficiencias de los criterios de la voluntad y del resultado, nació jurisprudencialmente esta teoría, de acuerdo a esta, el delito se estima cometido tanto en el lugar donde el sujeto ha realizado la acción, así como donde debiera haberse realizado, y en el lugar donde se produce su resultado.[165]

En la legislación salvadoreña se adapta a la teoría de la ubicuidad, [166] y se consagra en el artículo 12, Inciso tercero, del C.Pn, el cual establece:
"El hecho punible se considera realizado, tanto en el lugar donde se desarrolló, total o parcialmente la actividad delictuosa de los autores y participes, como en el lugar donde se produjo o debió producirse el resultado o sus efectos...".

Al igual que el código penal la Ley Especial contra Delitos Informáticos y Delitos Conexos, regula su ámbito de aplicación en el artículo 2 y expresa a letra:
"La presente Ley se aplicará a los hechos punibles cometidos total o parcialmente en el territorio nacional o en los lugares sometidos a su jurisdicción. También se aplicará a cualquier persona, natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, de sus habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador.

---

[164] Andrés José D'aussio et al., *Código Penal Comentado y Anotado Parte General* (Argentina: La Ley, 2005), 8, artículos 1° A 78 bis, goo.gl/IyjKRp.
[165] Ibid., 8.
[166] Rus, *Delito e Informática: algunos aspectos*, 181/246 (Véase la nota 141). El principio de ubicuidad sirve tanto para determinar el lugar de comisión de la acción y para decidir las jurisdicciones nacionales de diferentes territorios.

De igual forma, se aplicará la presente Ley si la ejecución del hecho, se inició en territorio extranjero y se consumó en territorio nacional o si se hubieren realizado, utilizando Tecnologías de la Información y la Comunicación instaladas en el territorio nacional y el responsable no ha sido juzgado por el mismo hecho por Tribunales extranjeros o ha evadido el juzgamiento o la condena".

4.6. Aspectos Terminológicos de delito informático

Corresponde elaborar el apartado correspondiente a los delitos informáticos previo a ello se realizará un análisis terminológico. Así, autores lo denominan "Delito Informático", sin embargo dentro del tecnicismo penal, no se puede utilizar la expresión delito, si no está tipificada la conducta como tal, algunos penalistas suprimen esa denominación. Pero otros afirman que la expresión "Delitos informáticos",[167] proviene de las expresiones inglesas, Computer Crime y Computer related crime, según lo manifiesta Alberto Landeira.[168] Aunque otro sector de la doctrina sostiene que no se admite la existencia de un delito informático, en este sentido Davara Rodríguez afirma que únicamente acepta la expresión por conveniencia para su estudio, y comenta que sirve para referirse a determinados delitos en los que para su ejecución se ha usado un servicio informático.[169]

---

[167] Alberto Alberto Maricel Lucero, "Nuevas formas de delinquir", RITS. n.3 (2009), goo.gl/RqK2Bb. Manifiesta que los delitos informáticos implica actividades criminales que los Estados intentaron evitar, como por ejemplo robos, hurtos, falsificaciones u otras, pero utilizar técnicas informáticas creo nuevas formas en las que se utiliza indebidamente las computadoras, existiendo muchas denominaciones para estas conductas y cita las siguientes: delitos informáticos propiamente dichos, delitos electrónicos, delitos computacionales, crímenes por computadora, delincuencia relacionada con el ordenador, Cyber-crimenes.

[168] Renato Alberto Landeira et al., *Diccionario jurídico de los medios de comunicación* (Madrid: Reus, 2006), 97, goo.gl/wpe1QA.

[169] Davara, *Manual de Derecho Informático*, 356-357 (Véase la nota 156). En palabras del autor: *"Ni tan siquiera admitimos que exista como tal un delito informático. Aceptamos la expresión, por conveniencia, para referirnos a determinadas acciones y omisiones dolosas*".

Gutiérrez Francés, sostiene que la expresión delitos informáticos ni siquiera da idea a la realidad tan compleja y heterogenia que se pretende englobar, por lo que expresa que no puede existir un delito informático, pero si una pluralidad de ellos en lo que se encuentran como única nota común, su relación de alguna forma con los ordenadores, pero que ni el bien jurídico protegido que se transgredió es siempre de la misma naturaleza, ni la forma de ejecución del hecho tienen características semejantes.[170]

Además, Davara Rodríguez sostiene que no es adecuada la utilización del concepto delito informático, porque no existe como tal,[171] y que considerar la necesidad de tipificar una conducta, en la legislación penal para que pueda existir un delito.[172] Sin embargo considera necesario utilizar la expresión delito informático para realizar un estudio de las acciones típicas antijurídicas y culpables y que por lo tanto es necesario definirlo.[173]

Así la realización de una acción que cumple con los elementos exigidos en la definición de delito, y con la utilización de elementos de la informática, transgrediendo derechos del titular de un elemento informático el cual podría ser hardware o software. Aquí se está refiriendo únicamente a los delitos ejecutados mediante medios informáticos o por medios telemáticos, porque la comisión de otros delitos en los que interviene un elemento informático está el área del derecho penal general, así ejemplifica, el caso de la venta con engaño de un ordenador, en el que la circunstancia de ser el ordenador el objeto de la venta no desfigura en absoluto el tipo penal aparte

[170] Gutiérrez, *Fraude Informático y Estafa, 52* (Véase la nota 118).
[171] Galán, *El fraude y la estafa*, 35 (Véase la nota 121). Afirma que por la inexistencia legal de la definición de delito informático gran parte de la doctrina niega la existencia de este concepto, considerándolo impropio y que tan solo denota unidad a una pluralidad de delitos que solo tienen en común su vinculación con los ordenadores.
[172] Davara, *Manual de Derecho Informático*, 355 (Véase la nota 156).
[173] Ibíd., 358.

absolutamente al delito informático, por tanto no tiene relación con estos.[174]

4.6.1. Definiciones de delito informático

Antes de abordar el tema de la definición, es de aclarar que en la doctrina no existe una definición absoluta aceptada, de ahí por qué existe gran variedad de estas, en cuanto a su elaboración no es fácil, debido a que su denominación se refiere a un contexto muy especial, así, los delitos son acciones típicas, antijurídicas y culpables.[175] Sin embargo, se citan las siguientes: Alberto Landeira, propone la definición de la Organización para la Cooperación y el Desarrollo Económicos, de acuerdo a esta son delitos informáticos, las conductas antijurídicas, no éticas o no autorizadas, que implican el procesamiento automático de datos y la transmisión de datos. Definición que se considera vaga e imprecisa.[176]

Galán Muñoz comenta que con la aparición de los nuevos tipos penales, particularmente aquellos que sanciona conductas, que atentan contra bienes jurídicos tradicionales[177] y los denominados de nueva creación,[178] a través de la utilización de nuevos medios tecnológicos que aporta la informática, ha causado que la doctrina debata la posibilidad de agrupar todas las figuras en

[174] Ibíd., 360.
[175] Julio Téllez Valdés, *Derecho Informático* (México: Mc Graw Hill, 2009), 188.
[176] Landeira, *Diccionario Jurídico,* 97 (Véase la nota 168).
[177] Juan José Gonzales Rus, "Protección Penal de Sistemas, Elementos, Datos, Documentos y Programas Informáticos", *Ciencia Penal y Criminología, RECPC 01-14* (1999), goo.gl/5fhRVk. Señala que el uso de la informática no supone más que un modus operandi nuevo que no plantea particularidad alguna respecto de las formas tradicionales de comisión; Gutiérrez, *Fraude Informático y Estafa, 44* (Véase la nota 118). Afirma que las modernas tecnologías incorporan una dimisión instrumental que proporciona un sin número de posibilidades para el sujeto activo, para ejecutar un delito mediante esta nueva forma, así con el ordenador se pueden ejecutar delitos patrimoniales, actos de terrorismo, espionaje, daños, sabotaje.
[178] M. Quintana Díaz, niega que se hayan desarrollado nuevos valores como consecuencia de la aparición de tales delitos, ya que todas estas nuevas figuras vendrían siempre a proteger bienes jurídicos tradicionales, citado por Galán, *El fraude y la estafa*, 35 (Véase la nota 121).

la denominación delito informático,[179] concepto que carece de sustento legal en algunas legislaciones, dotándolo de contornos difusos y controvertidos.[180]

Por lo tanto, el concepto delito informático es de naturaleza doctrinal,[181] y no legal en algunos países, asimismo existe una gran cantidad de definiciones con el fin de dar cabida a todas las actividades delictivas que tienen o pueden llegar a tener una conexión en el uso de sistemas de tratamiento de datos, considerando por ejemplo que los delitos informáticos son todas las conductas criminales que se ejecuten mediante el ordenar electrónico o que afecten el funcionamiento de los sistemas informáticos.[182]

Alberto Landeira comenta que los delitos informáticos son definidos en sentido estricto como las conductas constitutivas de delitos tradicionales que, por las particulares características de internet, han adquirido una especial trascendencia en este medio.[183]

Romina Moscoso, expresa que los delitos informáticos: “Se caracterizan por castigar conductas dirigidas en contra del soporte lógico de un sistema de tratamiento de información.” Es decir, que se utiliza un sistema de procesamiento de información, como una computadora que se constituye principalmente en dos partes: el soporte lógico o el software (los datos, la

[179] Del Pino, *Delitos Informáticos: Generalidades,* 13 (Véase la nota 149). Manifiesta que correspondiendo al legislador introducir las modificaciones legales pertinentes a fin de permitir la adecuación de los tipos tradicionales a las nuevas circunstancias.
[180] Galán, *El fraude y la estafa*, 29 (Véase la nota 121).
[181] Téllez, *Derecho Informático*, 188 (Véase la nota 175). Considera que los textos jurídico-penales, necesitan que se plasme la expresión delitos informáticos en los códigos penales. Añade el autor que los delitos informáticos son: *"actitudes ilícitas que tienen a las computadoras como instrumento o fin (concepto atípico) o las "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin" (concepto típico).*
[182] Galán, *El fraude y la estafa*, 29-30 (Véase la nota 121).
[183] Landeira, *Diccionario jurídico,* 98 (Véase la nota 168).

información contenida en el sistema); y el soporte físico o el hardware (los cables, chips, carcasa del equipo). Una acción orientada contra los datos es un delito informático, pero una orientada contra el soporte físico es un delito de daños.[184]

Möhrenschlager, propone una definición al referirse a la criminalidad informática y expresa: que cubre todo tipo de hechos donde las formas de procesamiento de datos son el medio de ejecución o el objeto de ataque u ofensa y representa las bases para la sospecha de que ha sido cometido un delito.[185]

La nota común de estas definiciones amplias es la de incluir a cualquier conducta que se hubiese ejecutado mediata o inmediata con un proceso electrónico de datos abarcando, aquellas conductas que son ejecutadas por medio de ordenadores como aquellas otras cuyo objeto material tuviese naturaleza informática.[186] Asimismo existen definiciones de carácter restringido que se limitan para los delitos que solo se pueden ejecutar porque se utilizan algunos de los medios electrónicos de datos o que no se pueden realizar sin autorización de estos, en este sentido seria delito informático todo comportamiento iniciado para ejecutar una conducta prevista en el código penal por medios informáticos.[187]

---

[184] Moscoso, "La Ley 19.223", 13-14 (Véase la nota 117). Es decir, que el objeto sobre el cual recaen las acciones tipificadas como delito de naturaleza informática, es inmaterial.
[185] Citado por Galán, *El fraude y la estafa*, 3 (Véase la nota 121).
[186] Galán, *El fraude y la estafa*, 31 (Véase la nota 121); Rus, "Protección Penal de Sistemas" (Véase la nota 177). Diferencia entre delitos contra los sistemas informáticos recaigan estos sobre sus elementos físicos o lógicos, y aquellos en los que el sistema informático es meramente el medio comisivo; Davara, *Manual de Derecho Informático*, 288 (Véase la nota 156). Se refiera solamente a los delitos ejecutados por medios de sistemas informáticos, como delito informáticos propiamente dichos.
[187] Briat. M., *La fraudeinformatique, revou de drot penal et crminologio*, n 65, 1985, 287 citado por Galán, *El fraude y la estafa*, 32 (Véase la nota 121).

Delito informático desde una perspectiva restringida contiene notas comunes como reducir la amplitud del concepto mediante la exclusión del mismo de las conductas que solo tiene de informático el hecho de recaer sobre un objeto de tal naturaleza, como por ejemplo un computador.[188]

Todas estas definiciones delimitan de forma imprecisas el concepto delito informático,[189] así por ejemplo al establecer que estos son todos aquellos delitos, incorporados bajo tal denominación se podrían agrupar atendiendo al hecho de que todos ellos vendrían a proteger o tutelar un bien jurídico de naturaleza informática, teniendo en cuenta que es difícil tutelar un bien de estos, capaz de aglutinar enorme variedad de delitos.

Se considera que el concepto delito informativo se dota de sentido, si incluye todas aquellas conductas que plantean problemas al tipificar, por el hecho de que se ejecutan por sistemas informáticos.

Galán Muñoz, sostiene que el delito informático es un término de referencia no estrictamente jurídico que se refiera a una pluralidad de delitos, protegiendo bienes jurídicos de diversa naturaleza.[190]

Fox Andina, en su obra Hacking desde cero, comenta que este término está muy presente en las leyes que se promulgaron, así añade: “Podemos afirmar que son simplemente los actos criminales en los cuales se encuentran

[188] Galán, *El fraude y la estafa*, 35 (Véase la nota 121).
[189] Además, estas definiciones de una manera u otra son vagas en cuanto no entregan una concreta delimitación de las fronteras en la que pueden producirse los delitos informáticos, desde un punto de vista estrictamente jurídico, también no establecen con claridad los efectos susceptibles de punibilidad de los delitos informáticos, toda vez que se establecen conductas del agente sin referencia precisa a la necesidad o no de resultados y cuáles serían éstos. Del Pino, *Delitos Informáticos: Generalidades,* 12 (Véase la nota 149).
[190] Galán, *El fraude y la estafa*, 35-36 (Véase la nota 121).

involucradas las computadoras".[191] Esta es una definición muy restringida porque el ordenador, no es el único medio, además interviene el internet, los programas utilizados como los spyware, troyanos, gusanos.

Respecto a la Ley Especial contra delitos informáticos y delitos conexos establece la definición legal, en el artículo 3. a) a la letra expresa: "Delito Informático: se considerará la comisión de este delito, cuando se haga uso de las Tecnologías de la Información y la Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información."

Por último se cita a Téllez que sostiene que los delitos informáticos son los que utilizan computadoras como instrumento o fin,[192] al contrario otro sector de la doctrina afirma que se ejecutan por medios informáticos o telemáticos y que tiene una característica especial, que los convierte en "sui generis", respecto a su forma especial de ejecución, entre ellos Davara Rodríguez que considera propias las características comunes y especiales de este tipo de acciones constitutivas de delitos que se mencionan a continuación.

1. Rapidez y acercamiento, en tiempo y espacio, su comisión. El tratamiento y proceso de información y las posibilidades de crear programas que ejecuten acciones que retrasen y controlen el tiempo, aprovechando las

[191] Fox Andina, *Hacking desde cero,* (Buenos Aires: Banfield-Lomas de Zamora Gradi, 2011), 38.

[192] Téllez, *Derecho Informático*, 188 (Véase la nota 175). A diferencia de la propuesta por Téllez, este sostiene que las principales características de los delitos informáticos son las siguientes: "*1. Son conductas criminales de cuello blanco; 2. Son acciones de oportunidad; 3. Provocan serias pérdidas económicas; 4. Ofrecen facilidades de tiempo y espacio; 5. Son muchos los casos y pocas las denuncias; 6. Son muy sofisticados y relativamente frecuentes en el ámbito militar; 7. Presentan grandes dificultades para su comprobación; 8. En su mayoría son dolosos o intencionales; 9. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional.";* Gutiérrez, *Fraude Informático y Estafa,* 52 (Véase la nota 118). Al contrario como se manifestó sostiene que la única nota común, es su vínculo de alguna forma con los ordenadores, y que ni siquiera la forma de ejecución del hecho tienen características semejantes.

funciones del sistema operativo del ordenador, que permite activar o desactivar acciones en las máquinas de forma dinámica y flexible, asimismo se pueden utilizar las comunicaciones en tiempo real y fuera del alcance del operador y del ordenador atacado, realizar las acciones que disponga en tiempo y espacio retirados es decir se ejecutan delitos por una persona desde lugares distantes, por el acercamiento en espacio y permiten que las comunicaciones por internet y la potente posibilidad de utilizar como medio para ejecutar las acciones por programas que se pueden activar para funcionar en un momento determinado, hasta meses después del momento en que se creó y desde muy lejos.

2. Facilidad para ocultar el hecho. Se considera que existe la posibilidad de utilizar un programa,[193] para que ejecute una actividad delictiva para beneficiar al sujeto activo y establecer que se vuelva a utilizar un software es decir de forma automatizada, después de ejecutar la acción delictiva dejándolo tal como estaba en un inicio. De esta forma ni con el análisis del programa ni del proceso es posible determinar el hecho que se desarrolló, solo detectar el resultado de la acción.

3. Facilidad para borrar prueba. Existe una gran facilidad para eliminar todos los rastros que prueba que podría ser imposible detectar las acciones ejecutadas. Esta facilidad proviene, a veces, de la calidad de profesional del delincuente.[194]

Asimismo este autor señala las características comunes a todas las acciones catalogadas como delitos informáticos, permitiendo una clasificación según la

[193] Galán, *El fraude y la estafa*, 27 (Véase la nota 121). Sostiene que se puede decidir en qué momento tiene que producir efectos que se pretende obtener.
[194] Davara, *Manual de Derecho Informático*, 371 (Véase la nota 156).

función y la actividad en que se ejecutan. Así, en estos delitos su núcleo está en que la acción por lo general, es el acceso o la manipulación de datos que están en soportes informáticos o programas de ordenador, utilizados en su procesamiento y por la naturaleza de las acciones pueden ser eliminados los rastros de las acciones delictivas. Sin embargo esta es una tarea de la informática forense, es decir la disciplina de la criminalística que tiene como objeto la investigación en sistemas informáticos de hechos de relevancia jurídica o para la simple investigación privada.[195]

4.7. Clasificación de los delitos informáticos

Las nuevas tecnologías informáticas se han desarrollado rápidamente, y llevan a cabo diversas conductas que transgreden los bienes jurídicos protegidos penalmente por lo tanto es necesario establecer los diferentes delitos informáticos.

Respeto a la clasificación Ricardo Martin, al referirse al concepto de criminalidad informática diferencia dos grandes grupos, el primero de ellos recae sobre la informática o los sistemas informáticos es decir son el medio para ejecutar los hechos previstos y sancionados en la ley penal, y lesionar así un bien jurídico.

Por otra parte los grupos en que el hecho delictivo incide en algún elemento informático, el objeto material lo constituyen los propios soportes o sistemas informáticos. En este grupo se completan, por ejemplo, los ataques de denegación de servicio a un servidor (delito de daños), la descarga o la copia de una obra protegida (delitos contra la propiedad intelectual) la alteración de

[195] Javier Pages, *Informática Forense* (Madrid: Universidad Politécnica de Madrid, 2013), 8, goo.gl/snbz93. Para conseguir sus objetivos, la Informática Forense desarrolla técnicas idóneas para ubicar, reproducir y analizar evidencias digitales con fines legales.

datos reservados incluidos en algún tipo de archivo informático en los delitos contra la intimidad.[196]

Por otro lado Davara Rodríguez, considera determinadas acciones, como las que se encuadran en un delito informático, clasificándolo según el fin que persiguen en seis apartados que desarrollaremos posteriormente, explica que en todo delito que se quiera denominar informático, se tiene que distinguir el medio y el fin, para encuadrar una acción dolosa o culposa en esta clase de delitos. Por lo tanto el medio con el que se ejecuta tiene que ser un elemento, bien o servicio, patrimonial,[197] del ámbito de responsabilidad de la informática, y el fin que se persigue, tiene que ser la producción de un beneficio al sujeto activo del delito, con el fin de causar perjuicio a un tercero.[198]

4.7.1. La informática como instrumento en la ejecución de un delito

Se refiere a la posibilidad de utilizar la informática como medio de la ejecución de determinadas acciones dolosas o culpables que se pueden considerar como delitos. La forma de ejecutar un delito y sus muchas fases por los medios informáticos permiten, hacer aplicable una clasificación cerrada[199] de forma que se puede entender todas las posibilidades que en

[196] Rus, *Delito e Informática: Algunos Aspectos*, 131 (Véase la nota 141). Asimismo, sostiene que en este grupo se incorporan, entre otros, las estafas electrónica, la difusión de ciertos materiales pornográficos y el ciberterrorismo.
[197] Galán, *El fraude y la estafa*, 35 (Véase la nota 121). Pero esta es criticada por la doctrina porque el término se refiere a una pluralidad de delitos y bienes jurídicos de diversa naturaleza no solo patrimoniales.
[198] Davara, *Manual de Derecho Informático*, 360 (Véase la nota 156).
[199] Rus, Protección Penal de Sistemas (Véase la nota 177). Elabora una clasificación, para los delitos que se ejecutan por medio del sistema informático o utilizando elementos de naturaleza informática, que funciona como el instrumento utilizado para la ejecución del delito.

este sentido existen.[200]

Sin embargo, existen determinadas características comunes a todas las conductas catalogas como delitos informáticos que permiten clasificar de acuerdo con su función y actividad que se realizan para ejecutarla. Estos delitos tienen especiales características que les hacen en ocasiones, más difíciles de detectar, son de difícil persecución. Todas centran su actividad principal en el acceso o la manipulación de datos que se encuentran en soportes informáticos, o de programas de ordenadores utilizados en su procesamiento. En principio, la manipulación mediante la informática puede venir por dos medios diferentes uno como acceso y manipulación de los datos y el otro como manipulación de los programas.

Davara Rodríguez considera, que determinadas acciones, se pueden encuadrar dentro de lo que se llama delito informático, y para su estudio los clasifica, de acuerdo con el fin que persiguen, en seis apartados:

1. Manipulación en los datos e información contenida en los archivos o soportes físicos informáticos ajenos: Para que encuadre la acción en esté se necesita que se persiga obtener un beneficio económico de otra clase, para la persona que la ejecuta, o para quien se realiza afectando a otra persona, sin autorización, suprimiéndolos o modificándolos destruyéndolos o inutilizándolos para otras actividades diferentes logrando con ellos un beneficio ilícito para el sujeto activo.

2. Acceso a los datos o utilización de los mismos por qué no está autorizado para ello: Acá, se refiere al acceso que una persona no autorizada, a datos que están en soportes informáticos, por lo general de

[200] Davara, *Manual de Derecho Informático*, 360-361 (Véase la nota 156).

grandes bases de datos, de empresas e instituciones, secretos industriales, espionaje industrial.

3. Introducción de programas o rutinas en otros ordenadores para destruir información datos o programas: Es el caso de los virus informáticos, que se introducen mediante un soporte físico que los contiene o a través del internet, destruyendo los datos, información o programas contenidos en un ordenador.

4. Utilizar el ordenador o los programas de otras personas, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otros: En este caso se acede a los datos mediante programas o un ordenador de otra persona, así como mediante abuso de la confianza, en una relación laboral, personal, tiene el acceso y utilización de los mismos. Así, la acción consiste en utilizar programas u ordenador, sin autorización con el fin de la obtención de beneficios propios en perjuicio de terceros por ejemplo empleados utilizan los programas y la información de una empresa para realizar trabajos a terceros, los accesos no autorizados como posible delito se ejecutan a través, del internet, así la información y los programas están en soporte informático o que por la red se transportan a través de impulsos electrónicos.

5. Utilizar el ordenador con fines fraudulentos: Se refiere a la utilización para fines fraudulentos el ordenador así, ofrecer servicios, como pueden ser enmascaramiento de datos, cálculos complejos para evadir impuestos, escondiendo información entre otras acciones.

6. Intrusión a la intimidad mediante la utilización y procesamiento de datos personales con fin distinto al autorizado: Mediante la utilización y

procesamiento de datos personales utilizando para un fin distinto del que se está autorizado, así como utilizar el producto de los datos personales, con fines y actividades distintas a las que se fundamentan para su obtención, es lo que las legislaciones previenen y protegen, cuando se refieren a conductas que transgreden la intimidad mediante el uso de medios informáticos.[201]

López Ortega, identifica ámbitos de riesgo para la intimidad para salvaguardar este bien jurídico entre ellos están:

1. El problema de los denominados "archivos logs" los proveedores de acceso a la Red ostentan la posibilidad de registrar las conexiones de los usuarios, el tiempo de la conexión, la localización de la conexión, los servicios visitados, la identidad del emisor del mensaje y del destinatario, todos estos datos e informaciones son almacenados o consignados por el proveedor de acceso, lo que le permite configurar un primer y amplio perfil digital del usuario.

2. El problema de las denominadas "cookies", archivos que son emitidos por los web servidores visitados o consultados por el internauta y que se graban en el disco duro de éste. Esta técnica permite al web servidor memorizar las consultas efectuadas anteriormente por el internauta a ese mismo web. El envió sucesivo de cookies y su conservación permite al web emisor de las mismas obtener una fotografía digital del usuario, rastreando sus gustos o preferencias, costumbres, entretenimiento, etc.

3. El problema de los "virus informáticos" es que son comportamientos que atacan los elementos lógicos de sistemas informáticos que pueden

[201] Ibíd., 363-368.

llevarse a cabo a través de procedimientos de naturaleza informática mediante programas de destrucción progresiva, las llamadas rutinas cancerígenas, virus que dejen inoperante un programa o destruyen datos almacenados o bien mediante otras formas como las bombas lógicas o Caballo de Troya.

4. El problema del "hacking o acceso no autorizado".[202] El acceso y uso de banco de datos y archivos electrónicos ajenos, constituye la superación de medidas de protección al sistema mismo, donde el sujeto involucrado mejor conocido como hacker puede modificar, destruir, copiar todo tipo de información de algún sistema informático. Los medios de acceso son variados pero podríamos mencionar los siguientes; Las Puertas Falsas (Trap Doors), La Llave Maestra (Superzapping), Pinchado de Líneas (Wiretapping).[203] Entre las acciones ejecutadas en internet, expandidas son estos accesos a datos reservados con el fin de obtener información personal, o profesional ajena.[204] Se considera que algunas de las conductas se podrían subsumir a los delitos contra la intimidad, cuando el bien transgredido a través de las mismas, es la intimidad personal (el secreto a las comunicaciones).

[202] Lucero, "Nuevas formas de delinquir" (Véase la nota 167). Afirma que esta es una expresión anglosajona.
[203] Juan José López Ortega, *Internet y derecho penal* (Madrid: Consejo General del Poder Judicial, 2001); Faustino Gudín Rodríguez-Magariños, *Nuevos Delitos Informáticos: Phising, Pharming, Hacking y Cracking,* 7, goo.gl/GHKKHF. El hacking o intrusismo informático, consiste en el acceso no autorizado, por lo general violando los medios de seguridad de los soportes que contienen los archivos y bases de datos contenidos en los sistemas informáticos ajenos.
[204] Teruelo, *Cibercrimen los delitos,* 121 (Véase la nota 124).

CAPÍTULO V
COMENTARIOS JURÍDICOS Y DOCTRINAL A LOS DELITOS TIPIFICADOS EN LA LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS QUE PROTEGEN EL DERECHO A LA INTIMIDAD DE LA INTRUSIÓN INFORMÁTICA

El propósito de este capítulo es realizar un análisis del tipo penal del delito acceso Indebido a Sistemas Informáticos y Espionaje Informático, tipificados en la Ley Especial contra los Delitos Informáticos y Conexos que protegen el derecho a la intimidad de la intrusión informática.

5. Delitos Regulados respecto al intrusismo informático

Antes de realizar el análisis de los tipos penales que protegen la intimidad mediante la regulación del intrusismo informático, es necesario elaborar un breve cometario de lo que en doctrina se conoce como delito de hacking.[205] Huerta sostiene que este se constituye por un acceso indebido o lo que es lo mismo un acceso no autorizado, sirve de medio para la comisión de otros delitos, como la estafa informática, el espionaje informático, la piratería de software,[206] se ejecutan mediante el acceso indebido, a los Sistemas Informáticos, así, este autor estima que el hacking, es un delito que puede ser utilizado como medio necesario para la ejecución de otro delito.[207]

---

[205] Eduardo E. Rosende, *El Intrusismo Informático. Reflexiones sobre su inclusión al código penal*, 3, goo.gl/Go38Va; Huerta, Delitos Informáticos, 168 (Véase la nota 155). También denominado acceso no autorizado a datos y programas.

[206] Rus, *Delito e Informática: Algunos Aspectos*, 408 (Véase la nota 141). Conjunto de programas y aplicaciones informáticas que hacen funcionar a un ordenador o que se ejecutan en él.

[207] Huerta, *Delitos Informáticos*, 169 (Véase la nota 155). El hacker, es la persona que ejecuta el delito de hacking con el objetivo de ejecutar un fraude informático, un espionaje informático o sabotaje, mediante la trasgresión a la prohibición de acceso.

Los accesos no autorizados se denominan Intrusismo informático o "hacking" entendiéndose como una conducta de acceso o permanencia no autorizados a sistemas informáticos, una interferencia en redes de telecomunicación electrónicas protegidas.[208] Para el caso en la legislación del país se ubica el intrusismo informático en el artículo 4 de la Ley Especial Contra Delitos Informáticos y Delitos Conexos que regula el acceso indebido a Sistemas Informáticos.

Corresponde abocarse al análisis de los elementos del tipo penal antes citado, aplicando la teoría general de delito[209] a los diversos tipos penales que protegen la intimidad del intrusismo informático en la LECDIDC, para lo cual previo a ello se elabora un breve comentario respeto al análisis doctrinal y jurídico del tipo penal.

5.1. Tipo penal y Tipicidad

Huerta, comenta que el tipo penal[210] es la descripción de una conducta prohibida por la norma jurídica, la tipicidad, es la adecuación de una conducta al tipo penal.[211] El tipo contiene la acción mediante los diversos verbos rectores, de acuerdo a ellos los tipos penales podrían ser de mera

[208] Asunción Colás Turégano, "El delito de intrusismo informático tras la reforma del CP español de 2015", *Iuris Tantum,* Nº 21 (2016), goo.gl/yszX5M.

[209] Eduardo Germán Bauché, *Lavado de Dinero Encubrimiento y Lavado de Activos* (Argentina), 236. "La teoría del delito se estructura como un método de análisis de distintos niveles. Cada uno de estos niveles presupone el anterior y todos tienen la finalidad de ir descartando las causas que impedirían la aplicación de una pena y comprobando (positivamente) si se dan las que condicionan esa aplicación. Gráficamente podría decirse que se trata de una serie de filtros cuyos orificios son más estrechos en cada nivel".

[210] Raúl Eugenio Zaffaroni, *Tratado de Derecho Penal: Parte General,* Tomo III (Argentina: Ediar, 1981), 168. El tipo penal es un instrumento legal, lógicamente necesario y de naturaleza descriptiva.

[211] Huerta, *Delitos informáticos*, 181 (Véase la nota 155). La función del tipo es que la norma controle una conducta determinada, así los elementos objetivos del tipo recaen, en la protección del bien jurídico y las modalidades de acción; Zaffaroni, *Tratado de Derecho Penal*, 167 (Véase la nota 210). El tipo penal tiene por función la individualización de conductas humanas penalmente relevantes (por penalmente prohibidas).

actividad[212] o de resultado[213] De acuerdo con Bacigalupo, el tipo penal en sentido estricto es la descripción de la conducta prohibida por una norma jurídica, es decir que es la descripción de acciones que transgreden la norma jurídica.[214] Claus Roxin expresa lo siguiente: "El tipo penal es un juicio por el cual se establece que la acción subsumida en él constituye un injusto mientras no se demuestre lo contrario."[215] Es la determinada descripción de una acción prevista en una ley.[216] La dogmática penal establece que el tipo penal en sentido amplio tiene supuestos y elementos objetivos, referencias de tiempo, espacio e instrumentales, datos subjetivos normativos, y precisiones en cuanto a los sujetos activos y pasivos y sobre el objeto.[217]

El tipo de acuerdo a Muñoz Conde como imagen conceptual, tiene una

[212] Huerta, *Delitos informáticos*, 181 (Véase la nota 155). Son aquellos que se consuman por una simple acción del sujeto activo para transgredir la ley; Bacigalupo, *Manual Derecho Penal*, 80 (Véase la nota 131). Sostiene que la teoría del tipo penal es un medio conceptual para determinar el comportamiento prohibido, así, la acción ejecutada por el sujeto activo es la prohibida por la norma cuando se subsume bajo un tipo penal; Raimundo Del Rio C', *Explicaciones de Derecho Penal Tomo I,* Generalidades (Chile, Nascimento), 259. Afirma que la teoría del tipo o de la tipicidad se toman como sinónimos, por tanto existen en la doctrina controversias, esta, fue creada originariamente por Beling, en 1906.

[213] Huerta, *Delitos informáticos*, 181 (Véase la nota 155). Los tipos de resultado son los que para su consumación la ley requiere que se verifique el resultado dado por el sujeto activo, es decir la transgresión al bien jurídico protegido por la norma penal.

[214] Bacigalupo, *Manual Derecho Penal,*80 (Véase la nota 131). Asimismo, comenta que en general el tipo es una expresión que sirve para designar a un conjunto de elementos anexados por una misma significación, y añade que "*el tipo penal es el conjunto de elementos que caracteriza a un comportamiento como contrario a la norma"*. Distingue dos conceptos de tipo según su contenido y son los siguientes: Tipo garantía: contiene los presupuestos que determinan aplicar una pena; Tipo sistemático: es el tipo en sentido estricto, que describe la acción prohibida por la norma jurídica, este, coincide con el error de tipo: así, los elementos objetivos de este son los que debe haber conocido y querido el sujeto activo, para poder determinar que ejecuto la acción con dolo; el error en uno de los elementos excluye el dolo; Carlos Julio Lascano, *Derecho Penal: Parte General* (Argentina: Duarte Quirós, 2005) 262-263. Distingue también en el mismo sentido que Bacigalupo, dos conceptos de tipo a saber; Tipo garantía: Tipo sistemático o en sentido estricto.

[215] Claus Roxin, *Teoría del Tipo Penal* (Argentina: De palma, 1979), 65.

[216] Sergio García Ramírez, *Derecho Penal Colección Panorama del Derecho Mexicano* (México: Porrúa, 2007), 82.

[217] Ibíd., 83; Francisco Muñoz Conde, *Derecho Penal: Parte General* (España, Tirant lo Blanch, 2010), 79. Los tipos penales, cumplen la misión de indicar la materia de prohibición, es decir lo que el legislador considera que debe ser prohibido.

formulación con expresiones lingüísticas que, pretenden describir, con notas de abstracción y generalidad, la acción prohibida, y así, cumplir la función de garantía, por lo tanto el tipo tiene que estar redactado, así, del texto se podrá deducir con claridad la acción prohibida. Por lo tanto se tiene que utilizar un lenguaje claro y preciso, añade que se debe usar de forma moderada elementos normativos (por ejemplo acreedor, insolvencia, ajenidad, datos informáticos, sistemas informáticos), que envuelven una valoración y, por lo tanto, un grado de subjetivismo, y utilizar, más que todo, elementos lingüísticos descriptivos que cualquier sujeto conozca su significado sin complicaciones (por ejemplo: matar, daños, lesiones). Pero, es imposible, sacar absolutamente los elementos normativos, así como también los puramente descriptivos, como por ejemplo el de morada (utilizado en la descripción del delito de allanamiento de morada), que se necesita para valorar al momento de aplicar.[218]

Muñoz Conde sostiene que el tipo es la descripción de la conducta prohibida que establece el legislador en el supuesto de hecho de una norma penal, [219] menciona que el tipo tiene una triple función y son las siguientes: a) función de selección de las acciones humanas penalmente relevantes; b) función de garantía, porque únicamente los comportamientos que se subsumen en él se pueden sancionar penalmente; c) función motivadora general, porque, con la descripción de los comportamientos en el tipo penal, el legislador determina a los ciudadanos las acciones que tienen prohibidas y con la advertencia penal de los tipos, se espera que los ciudadanos se abstengan de ejecutar la conducta prohibida por la norma penal.[220]

[218] Muñoz, *Derecho Penal: Parte General,* 256 (Véase la nota 217).
[219] Ibíd., 252,253.
[220] Ibíd., 252

Respecto a la tipicidad García Ramírez, sostiene que la tipicidad es la adecuación de la conducta a un tipo penal.[221] La tipicidad es la adecuación de un hecho ejecutado a lo descrito en la ley penal como delito.[222] Para Conde la tipicidad es la cualidad de un comportamiento cuando se subsume en el supuesto de hecho de una norma penal.[223] Respecto a la tipicidad Villavicencio Terreros, sostiene que es el resultado de la verificación que coincide la conducta con lo descrito en el tipo penal, además nos dice que a este proceso de verificación es denominado juicio de tipicidad.[224]

5.1.1. Tipo Objetivo y Tipo subjetivo

Bacigalupo comenta que este tipo contiene los aspectos objetivos del hecho.[225] De acuerdo con Lascano el tipo objetivo es lo externo del comportamiento humano prohibido por la norma penal.[226] Respecto al tipo subjetivo dice Bacigalupo que la tipicidad del delito doloso depende no sólo de ejecutar el tipo objetivo, también, de realizar el tipo subjetivo, es decir, el dolo, este se caracteriza porque en él concuerdan el hecho (tipo objetivo) con lo querido (tipo subjetivo).[227] El dolo, añade; es la realización del tipo

---

[221] Sergio Ramírez, *Derecho. Penal Colección Panorama del Derecho Mexicano,* México, 82. Asimismo, expresa que para la exclusión de la tipicidad se tiene que distinguir entre la falta de tipo (ausencia de fórmula legal incriminatoria) y la falta de adecuación típica de la conducta al supuesto penal (atipicidad) por lo tanto no hay delito, no hay sanción.

[222] Muñoz, *Derecho Penal: Parte General,* 251 (Véase la nota 217). Asimismo, añade que por imperativo del principio de legalidad, en su ramificación del nullum crimen sine lege, únicamente los hechos tipificados en la ley penal como delitos son considerados como tales.

[223] Ibíd., 252. La tipicidad de una acción no implica, su antijuricidad pero si, un indicio de que la conducta puede ser antijurídica (función indiciaria del tipo); Del Rio, *Explicaciones de Derecho Penal*, 253 (Véase la nota 212). La tipicidad como elemento genérico del delito, supone que la acción (asimismo con el resultado) se subsuma en el tipo.

[224] Felipe Villavicencio Terreros, *Derecho penal: parte general* (Perú: Grijley, 2006), 295; Eduardo Bauché, *Lavado de Dinero Encubrimiento y Lavado de Activos*, 237. La "tipicidad" consiste en que la conducta se adecúe a un tipo penal.

[225] Bacigalupo, *Manual Derecho Penal*, 83 (Véase la nota 131).

[226] Lascano, *Derecho Penal: Parte General*, 266 (Véase la nota 214).

[227] Bacigalupo, *Manual Derecho Penal*, 103 (Véase la nota 131). Precisamente esta coincidencia diferencia al delito doloso del delito culposo, en el que esta coincidencia no existe.

objetivo, así, el dolo es el conocimiento y la voluntad de la realización del tipo.[228]

Garrido Montt comenta que el dolo exige dos momentos, el primero de ellos es el intelectual, es decir el conocimiento de la acción que se va a ejecutar, y otro la naturaleza volitiva, es decir es el querer realizarlo.[229] Asimismo se exige que el sujeto activo conozca todas las características materiales de la acción descrita por el tipo objetivo, es decir las descriptivas y las normativas, es lo que se denomina elemento cognoscitivo (intelectual). El segundo elemento para configuración del dolo es la voluntad de materializar el tipo objetivo, es decir la voluntad de realizar la actividad típica, es denominado elemento voluntad del dolo (momento volitivo).[230]

5.1.2. Sujeto de la acción

De acuerdo a Garrido Montt el sujeto activo es quien realiza toda o una parte de la acción descrita por el tipo, sólo puede ser un individuo de la especie humana, hombre o mujer.[231] Empero el tipo penal restringe la posibilidad de ejecución a determinadas personas, como se hace en delitos que solamente los empleados públicos son sujetos activos, en este caso es lo que en doctrina se denomina tipos especiales,[232] que exigen de un sujeto calificado,

[228] Ibíd.
[229] Mario Garrido Montt, *Derecho Penal: Parte General*, Tomo II (Chile: Editorial jurídica de Chile, 2010), 76.
[230] Ibíd., 77.
[231] Juan Busto Ramírez et al., *Lecciones de Derecho Penal Volumen II Teoría del delito, Teoría del Sujeto Responsable y Circunstancias del Delito* (Madrid: Trotta, 1999), 50. En el derecho penal actual, únicamente una persona natural puede ser considerada como sujeto activo del delito. Sujeto activo es quien lleva a cabo la actividad descrita en el tipo legal
[232] Ibíd., 40. Establece una división entre los sujetos comunes que son aquellos que tienen un sujeto activo y pasivo innominado, son la mayoría de los tipos penales. En la estructura típica, queda el sujeto activo determinado por expresiones como: el que o quien; el pasivo, por la voz otro. Respecto a los delitos especiales, el sujeto activo es identificado los autores potenciales del delito están restringidos a personas que cumplen las cualidades exigidas por el tipo penal.

y la calidad especial que deben tener es un elemento del tipo objetivo, lo que añade tiene relevancia para los casos del error.[233]

Así en cuanto al sujeto activo, en la descripción de los diversos delitos regulados en la ley especial, no se hace mención alguna respecto a la calidad de este. En cuanto al sujeto pasivo es el destinatario de la protección del bien jurídico, es decir cualquier persona puede ser sujeto pasivo de un delito, ya sea natural o jurídica.[234] Para el caso de los delitos informáticos pueden ser una o varias personas sean naturales o jurídicas, podrían ser empresas u organización, así como los Estados y toda la sociedad dependiendo del delito.[235]

5.2. Delitos tipificados en la ley especial contra los delitos informáticos y conexos que protegen el derecho a la intimidad de la intrusión informática

El capítulo III de la ley especial, denominado delitos informáticos relacionados con el contenido de los datos regula un catálogo sin embargo por el objeto de la investigación se analizarán unicamente los delitos informáticos, que engloban conductas de acceso no autorizado a los sistemas de información. No obstante la ley especial no regula un tipo penal que se denomine intrusismo informático, pero si, el Acceso Indebido a Sistemas Informáticos, que constituye intrusismo.

5.2.1. Análisis del tipo penal del delito acceso Indebido a Sistemas Informáticos

El Acceso Indebido a Sistemas Informáticos, se regula en el artículo 4 de la

[233] Montt, *Derecho Penal: Parte General*, 56 (Véase la nota 229).
[234] Busto, *Lecciones de Derecho Penal,* 50 (Véase la nota 231).
[235] Huerta, *Delitos Informáticos*, 186 (Véase la nota 155).

ley especial a la letra expresa: El que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o utilice parcial o totalmente un sistema informático que utilice las Tecnologías de la Información o la Comunicación, será sancionado con prisión de uno a cuatro años.

5.2.1.1. Análisis de la Conducta típica

5.2.1.1.1. Tipo objetivo

La conducta se caracteriza por la realización de cualquiera de los verbos rectores alternativos, es decir, accesar, interceptar o utilizar parcial o totalmente un sistema informático[236] que utilice las Tecnologías de la Información o la Comunicación, siempre que lo realice sin autorización o excediendo la que tiene. Para el caso de realizar la conducta sin autorización,[237] acceda,[238] intercepte utilizándolos total o parcialmente en contra de la voluntad de quien tuviera el derecho a decidir si puede o no.[239] Así el acceso típico no dice nada sobre la vulneración de las medidas de seguridad establecidas, porque existen sistemas no protegidos. De la

[236] Sistema Informático: es un elemento o grupo de elementos interconectados o relacionados, pudiendo ser electrónicos, programas informáticos, enlaces de comunicación o la tecnología que en el futuro los reemplace, orientados al tratamiento y administración de datos e información; Tecnologías de la Información y la Comunicación: es el conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros.

[237] Fernando Pérez Alvares, *Moderno Discurso Penal y Nuevas Tecnologías* (España: universidad de Salamanca, 2013), 252, goo.gl/76MKjo. Respecto a la expresión sin autorización, comenta que deberá de ser sustituida por ilícitamente o por la especificación sin amparo legal.

[238] Moscoso, "La Ley 19.223", 32 (Véase la nota 117). La acción de ingresar al sistema informático, la voz acceder tipifica el denominado hacking blanco (o hacking a secas, en oposición a cracking), para significar un acceso indebido sin la intención de producir un resultado dañoso.

[239] Se está en presencia de lo que se denomina intrusismo informático de hacker blanco, es decir acceder e interferir sin autorización a un sistema informático o red de comunicaciones electrónica de datos, u utilizar excediendo las facultadas dadas.

literalidad del tipo penal[240] se desprende que los verbos rectores regulan los supuestos en que el acceso es sin la autorización del titular[241] y cuando han sido autorizado pero el sujeto extiende los limites por lo tanto constituye delito, asimismo existe ilicitud cuando al sujeto se le dice que salga del sistema, este se niega y manteniéndose en el mismo, extendiendo las facultades autorizadas.[242] El acceso tiene que ser informático, es decir, virtual, no puede ser físico, la acción de accesar se lleva a cabo mediante la digitación de una serie de comandos con los cuales se ordena a un sistema informático ejecutar una determinada operación utilizando software denominados coloquialmente como virus, que, permiten al sujeto ingresar o utilizar el sistema de tecnología.

El caso de realizar el verbo rector de interceptar,[243] es decir apoderarse de información o datos que circulan por la red, por ejemplo de mensajes de email ajenos o de los que circulan por el internet el denominado sniffing que se diferencia del hacking, porque el primero supone, utilizar los sniffers, es decir, rastreadores, software que se ponen en la red para interceptar mensajes enviados, como por ejemplo los correos email, accediendo a su lectura. Sin embargo la interceptación es para cualquier mensajería instantánea como los chats, WhatsApp, oral, visual, escrita o combinada (voz

[240] Pérez, *Moderno Discurso Penal*, 252 (Véase la nota 237). La vulneración de la medida de seguridad tiene que asociarse con la conducta de acceso y no a la de mantenerse en el sistema de información.
[241] Ricardo Posada Maya, "El delito de acceso abusivo a sistema informático: a propósito del art. 269ª del CP de 2000", *Universidad de los Andes: Facultad de Derecho N. 9* (2013), 14, goo.gl/j6OCsf. Respecto al acceso puede ser directa, indirectamente o remota a un sistema informático, el sujeto activo traba un diálogo lógico no autorizado. Esta modalidad típica es de mera conducta o pura actividad, y se consuma instantáneamente con la mera introducción o acceso.
[242] Colás, "El delito de intrusismo informático" (Véase la nota 208).
[243] Al interceptar un sistema informático, se apodera de los datos e información, la ley en cometo en su artículo 3 literal h define que es Interceptar: es la acción de apropiarse, interrumpir, escuchar o grabar datos informáticos contenidos o transmitidos en cualquier medio informático antes de llegar a su destino.

e imagen, imagen e información o texto).[244]

Por la naturaleza activa del verbo interceptar se excluye la tipicidad de la conducta en el supuesto de retener la información si esta es recibida por error.[245] Asimismo agrega que en el ámbito del internet, existen múltiples medios de apoderamiento e interceptación desde el acceso material desde la PC, ajena para aprovecharse del descuido del titular, o mediante engaño al mismo, la sustracción de claves. Hasta los ya mencionados snifffers a los que denomina como capturadores de correo, además menciona la utilización de los spyware,[246] es decir programas espías, que permite accesar a la información del titular de la PC.[247] Esta conducta no exige revelar los secretos solo la intercepción de la información en caso se revelara los secretos contenidos en la información interceptada, constituiría otro delito como por ejemplo; Revelación Indebida de Datos o Información de Carácter Personal artículo 26 y la diferencia esencial; o la agravación en el caso del Espionaje Informático, párrafo segundo, articulo 12. Así, en el sniffing lo que se lleva cabo es la interceptación de los mensajes, información.[248]

Respecto a la utilización parcial o total de un sistema informático, que utilice las Tecnologías de la Información o la Comunicación, se refiere a los

[244] Fátima Flores Mendoza, "Delincuencia económica. Respuesta Penal Al Denominado Robo de Identidad en las Conductas de Phishing Bancario, Nuevos instrumentos jurídicos y tecnológicos", Estudios Penales y Criminológicos*, vol. XXXIV* (2014), 323, goo.gl/fTqI6Y.
[245] Teruelo, *Cibercrimen los delitos,* 124 (Véase la nota 124).
[246] Ibíd., 315-318. El pharming y spyware son métodos que se emplean para ejecutar las conductas intrusismo informático. Ambos consisten en un acceso no consentido a un sistema informático de un tercero, realizado remotamente mediante el internet, modifica las direcciones IPs o configuración DNS de un sistema informático, en el primero, e introduciendo programas espía en el sistema, en el segundo.
[247] Ibíd., 125.
[248] Manuel Sánchez Bercedo, *El delito de intrusismo informático o Hacking Artículo 197.3 CP*., 8, goo.gl/QXktuK; Rus, *Delito e informática: algunos aspectos*, 408 (Véase la nota 141). Sniffer. (Husmeador). Es un dispositivo que intercepta la información que circula por una red informática por medio de una cadena numérica o de caracteres es, por tanto, un ataque informático en el que el objetivo es obtener información sin manipularla.

supuestos que se pretende es la obtención de un beneficio derivado directamente de la utilización sin embargo la ley no regula respeto a la finalidad de la utilización total o parcialmente de un sistema informático que utilice las Tecnologías de la Información o la Comunicación. Para el caso esta conducta se ejecuta al utilizar por ejemplo una terminal a distancia, mediante troyanos[249] que controla el ordenador. No es una intromisión ilícita a un área ajena, es una actuación sin permiso usando un servicio que el titular recibió un precio por su uso. No se sanciona, el acceso doloso y sin autorización total o parcialmente, si no la utilización del sistema.[250]

Tal como está redactado el tipo penal, sólo sanciona las conductas de utilización parcial o totalmente de un sistema informático que utilice las Tecnologías de la Información o la Comunicación, no establece el tipo penal si, tal utilización, causa un perjuicio patrimonial al titular del servicio, por ejemplo, cuando se usa un teléfono de pago para acceder a redes informáticas, por lo que se paga al titular. Asimismo se adaptan las conductas a la captación de señales de un router inalámbrico.[251]

5.2.1.1.2. Tipo subjetivo

De la redacción del tipo penal para la ejecución del delito se exige dolo, porque el sujeto ejecuta la acción con la voluntad de intromisión al sistema tecnológico de información, lleva cabo los verbos rectores: acceder, interceptar o utilizar parcial o totalmente un sistema informático que utilice las Tecnologías de la Información o la Comunicación, así al realizar esta

[249] Rus, *Delito e informática: algunos aspectos,* 395 (Véase la nota 141). Caballo de Troya o troyanos: Son programas que se ocultan dentro de otros, para no ser descubiertos, y se instalan en el sistema, de forma que al actuar producen un auténtico sabotaje contra el sistema informático. Los troyanos no se replican a sí mismos lo que les diferencia de los virus puros aunque algunos sí son capaces de enviarse como adjuntos.
[250] Ibíd., 57
[251] Ibíd.

conducta con el conocimiento de que es ilícita, es decir, que no tiene, permiso, autorización o consentimiento del titular para hacerlo. Por lo tanto si el acceso es por un descuido o negligencia sin la intencionalidad que exige el tipo penal, el hecho es atípico.[252] Es decir que se trata de un tipo que solo dolosamente, puede ejecutarse, y el dolo tiene que ser directo, excluyendo al eventual, por expresar el tipo penal como elemento subjetivo distinto al dolo la palabra "intencionalidad".[253]

5.2.1.2. Sujeto activo

EL sujeto activo de la acción regulada en el tipo penal, únicamente la puede ejecutar un sujeto con práctica y conocimientos especiales de la informática para trasgredir los medios de seguridad del sistema de información. Sin embargo de la redacción del tipo penal, permite determinar que es un delito común al expresar "El que" es decir no establece calidad especial para el que realiza los verbos rectores, en otras palabras, el sujeto no tiene por qué ser un hacker o un cracker, basta que sea una persona común.

La Revista Boliviana de Derecho, dice que en principio, no se requiere ninguna condición especial, formalmente, sin embargo en la práctica la autoría se limita para personas que tienen conocimientos especiales de la informática, asimismo afirman que el usuario medio ni siquiera tiene habilidad para ejecutar la conducta típica.[254] Lo que permite determinar que es un delito en el que el sujeto activo tiene que ser un especialista informático o por lo menos tener conocimientos de lenguajes de programación.

---

[252] Colás, "El Delito de Intrusismo Informático" (Véase la nota 208).
[253] Montt, *Derecho Penal: Parte General*, 85 (Véase la nota 229). La intencionalidad es un elemento subjetivo distinto del dolo del tipo, al que Garrido lo define como: "*todos aquellos requisitos de carácter subjetivo distintos del dolo que el tipo exige, además de éste, para su realización",* lo que implícitamente excluye al delito culposo.
[254] Colás, "El Delito de Intrusismo Informático", 221 (Véase la nota 208).

5.2.1.3. Sujeto pasivo

Para el caso puede ser una o varias personas naturales o jurídicas, El sujeto pasivo es el titular o parte de un sistema informático que utilice las Tecnologías de la Información o la Comunicación. Por lo tanto podría ser un organismo público o un proveedor de servicios públicos o financieros,[255] también la persona a quien se le ha interceptado o accesado ilegalmente.

5.2.1.4. Bien jurídico protegido

Existe la dificultad en determinar cuál es el bien jurídico que se tutela, no hay un acuerdo consensado por la doctrina. Un sector considera como bien jurídico protegido por el intrusismo informático, la confidencialidad de los datos reservados y no la intimidad de las personas físicas relacionadas con aquellas.[256] Un sector de la doctrina considera, según la ubicación establecida por el legislador se considera que lo que se pretende tutelar es la información, que se sitúa en estos ámbitos de reserva de dicho espacio en términos de intimidad. El intrusismo informático se encuadra la tutela de la intimidad y seguridad de los sistemas informáticos. Porque se sancionan conductas en las que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, se accede, intercepta o la utilización parcial o totalmente de un sistema informático que utilice las Tecnologías de la Información o la Comunicación, en los que hay según el caso información

[255] Huerta, *Delitos Informáticos,* 186 (Véase la nota 155).

[256] Fátima Mendoza, "Delincuencia económica. Respuesta Penal al Denominado Robo de Identidad en las Conductas de Phishing Bancario", 320; Moscoso "La Ley 19.223", 7 (Véase la nota 117). La afectación a la confidencialidad de los datos de un sistema informático es la condición necesaria, para admitir la afectación a los bienes jurídicos tradicionales. Así, los delitos informáticos son pluriofensivos, porque no sólo la confidencialidad del soporte lógico, sino que se transgreden más intereses es decir delito informático atento contra la intimidad, el patrimonio, la fe pública, el orden económico, entre otros. Posada, *El delito de acceso,* 10 (Véase la nota 241). Este tipo penal es pluriofensivo porque afecta varios bines jurídicos exige, asimismo la vulneración del bien jurídico intermedio, público y autónomo de la seguridad de la información y los datos informáticos, sancionando la transgresión a la confiabilidad, integridad y la libre disponibilidad directa de los sistemas informáticos y el peligro indirecto de los datos y la información recogida en ellos.

relacionada a la intimidad, por ejemplo en los mensajes, correo electrónicos cuando se interceptan, o se tiene acceso a ellos, o al mantenerse en los sistemas informáticos. Así las conductas transgreden la intimidad de personas, y de entidades, porque se tiene acceso a información privadas resguardas en los sistemas, por lo tanto son conductas que transgreden la intimidad.[257]

Sánchez Bercedo sostiene que el bien jurídico protegido por el intrusismo informático es el derecho a la intimidad y establece los siguientes motivos: El Convenio de Budapest, porque este expresa que el acceso ilícito es un peligro para la intimidad personal y familiar; Asimismo sostiene que no hay otro bien jurídico que es transgredido por el acceso a una red de información, porque el hacking no supone revelar información alguna. Ni transgrede al patrimonio, e igualmente no extrae un beneficio por la utilización de información o de los sistemas informáticos.[258] Sin embargo al estar regulado en los delitos contra los sistemas tecnológicos de información, de esta manera la misma ley lo pone al margen de la protección a la intimidad, pero al acceder el tercero a información que por naturaleza es confidencialidad y de exclusivo conocimiento de determinadas personas, lo que transgrede es, por tanto el ámbito de su intimidad como derecho fundamental.

El capítulo II denominado de los delitos informáticos de la ley especial, regula un amplio catálogo de conductas que transgreden el derecho a la intimidad, sin embargo,[259] teniendo en cuenta que se están analizando los delitos

[257] Colás, "El Delito de Intrusismo Informático" (Véase la nota 208).
[258] Sánchez, *El delito de intrusismo informático,* 11 (Véase la nota 248).
[259] Lucero, "Nuevas formas de delinquir" (Véase la nota 167). Sostiene que el espionaje informático puede ser utilizado para producir considerables pérdidas de información a una empresa u organización, asimismo se puede atentar contra la seguridad exterior del Estado. Añade que El espionaje informático es considerado una conducta atentatorio al interés nacional en muchos Estados.

relativos al intrusismo informático, en este sentido se analizan aquellos delitos en los que se enjutan acciones de naturaleza instructiva. Así, se tipifica el delito de Espionaje Informático, el cual previo a realizar el análisis del tipo penal, se hace un breve comentario respecto al espionaje informático.

5.2.2. Espionaje Informático

Huerta, sostiene que el Espionaje Informático es toda acción típica, antijurídica y culpable que tiene por finalidad la violación de la reserva u obligación de secreto de la información contenida en un sistema de tratamiento de la información.[260] Asimismo sostiene que el fundamento de este delito es obtener de forma maliciosa la información que está en poder de la competencia, el enemigo, entre otras, por lo tanto los interesados de tales acciones están dispuestos a pagar mucho dinero. Añade que el espionaje informático es el delito consistente en obtener una información de forma no autorizada, sea por motivo de lucro o de simple curiosidad hecho que implica espiar y procurar una comunicación o bien una utilización de un sistema de tratamiento de la información en forma desleal, no autorizada.[261]

Herrera Bravo respecto al espionaje informático sostiene que consiste en la

[260] Huerta, *Delitos Informáticos,* 132 (Véase la nota 155). Otros autores consideran que este delito consiste en sustraer información confidencial o su divulgación no autorizada de datos reservados, asimismo para el derecho comparado consiste en la obtención no autorizada de datos almacenados en un fichero automatizado por lo que se produce una vulneración de la reserva o secreto de información de un sistema de tratamiento de la misma; Lucero, *"Nuevas formas de delinquir"* (Véase la nota 167)*.* Al referirse a la criminalidad informática también denominada de cybercriminalidad, sostiene que esta puede afectar a bienes jurídicos diversos, por ejemplo delitos en los que se utiliza el computador para atentar contra la fe pública, la seguridad nacional. En el caso de los Bienes Informáticos, consiste de acuerdo a esté, autor "*en dar facilidad al acceso de datos a ingresar a la información computarizada, archivos y programas insertos en el soporte lógico del ordenador"*. Así, en estas conductas se encuentra encuadrada el espionaje, fraude y el sabotaje informático.

[261] Huerta, *Delitos Informáticos*, 133 (Véase la nota 155)*;* Herrera*, Reflexiones sobre la delincuencia*, 20 (Véase la nota 156). Consideran que, puede o no ser el lucro, el fin de ejecutar esta conducta pero por lo general, son las grandes sumas de dinero.

obtención no autorizada de datos almacenados en un fichero automatizado, por medio del cual se produce la violación de la reserva o secreto de información de un sistema de tratamiento de la misma.[262] Téllez lo define como el acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas asimismo la interceptación de correos electrónicos.[263]

Maricel Lucero comenta que entre las formas maliciosas de obtener la información se encuentra la utilización de programas spyware[264] un vez instalados en el computador constantemente monitorean los movimientos del usuario conectado a Internet, en algunos casos su fin es crear un perfil comercial.[265] Tiene capacidad para monitorear el teclado. Su forma de operación se manifiesta en línea o en Internet así, cuando un usuario, descarga algún programa, que tiene incorporado un archivo ejecutable spyware; por lo general el usuario no sabe sobre su presencia y lo instala y comienza el espionaje. Asimismo hace referencia al intrusismo informático como una forma de ejecutar el espionaje informático, así el intrusismo de acuerdo a este autor, es un conjunto de comportamientos mediante los cuales se accede de manera secreta y reservada a un sistema informático,

[262] Ibíd., 20.
[263] Téllez, *Derecho Informático*, 204 (Véase la nota 175). Asimismo, lo categoriza como un Acceso no autorizado a un sistema de servicios, 195; Santiago Acurio Del Pino, *La Delincuencia Informática Transnacional y la UDIMP* (Ecuador: Ministerio Fiscal General del Ecuador, 2012), goo.gl/ucxSSk. Denomina al espionaje informático como: fuga de datos (data leakage), o divulgación no autorizada de datos reservados, y cometa que es una clase de espionaje industrial que consiste en sustraer información confidencial de una empresa.
[264] Andina, *Hacking desde cero,* 32 (Véase la nota 191). Como cada vez más las computadoras están conectadas por Internet en todo el tiempo, facilita que otras personas tengan acceso a información que no deberían, mediante programas malicioso como el malware o software malicioso.
[265] Lucero, "Nuevas formas de delinquir" (Véase la nota 167). El spyware tienen la capacidad de apoderarse de información personal del usuario, las transfiriere electrónicamente para según el caso a una empresa o a una persona que podría tener como objetivos comercializar la información. Este programa obtiene la información que está en el ordenador, así como también la que pasa por él. Mediante la utilización de un método de conexión entre el usuario y servidor directa e instantáneamente. La información está almacenada en un pequeño espacio que es transferida a otro soporte parecido.

con el fin de causar un perjuicio al titular del bien o a terceros.[266] Los métodos más frecuentes para la comisión del espionaje informático son los siguientes:

5.2.2.1. Pinchado de líneas o Wiretapping

Consiste en interceptar de forma programada las comunicaciones de las líneas telefónicas, con la finalidad de obtener licitante la información, pero permitiendo, la recepción normal de la comunicación por parte de los destinatarios. Asimismo añade que por esto último, es imposible detectar si la información fue interceptada por un tercero ajeno. Además consiste en la intercepción programada de las comunicaciones que se mueven a través de los cables telefónicos, con el fin de obtener de forma ilícita la información y los datos desplazados por ese medio, sin que el procedimiento interrumpa la recepción normal de la comunicación.[267] Así, al interferir las líneas telefónicas con el fin de obtener la información que se mueve por ellas, a través de un radio, un módem y una impresora.[268]

5.2.2.2. Recogida de información residual o Electronic Scavenging

Esta modalidad es producida exclusivamente por el descuido del propio usuario por tener pocas medidas de seguridad,[269] porque puede ser ejecutado por personas sin ninguna especialidad informática. Es así, que una persona obtiene sin autorización, la información que fue dejada sin protección como restos de trabajo. La información residual que queda precedentemente instalada en la memoria secundaria (porque la información

[266] Lucero, “Nuevas formas de delinquir” (Véase la nota 167).
[267] Huerta, *Delitos Informáticos*, 136 (Véase la nota 155).
[268] Del Pino, *La Delincuencia Informática Transnacional,* 29 (Véase la nota 263).
[269] Huerta, *Delitos Informáticos*, 138 (Véase la nota 155). Comenta que una medida de protección más simple es borrar la información del computador.

que se encuentra en memoria RAM, se borra al apagar el sistema por ser volátil) que no la borro el usuario, así, un tercero accede a la información y copia.[270] El termino scavenging es anglosajón y que implica recoger los desperdicios, desde un computador es decir la información residual que se queda instalada en la memoria o en el disco duro que no fue borrada por el usuario.[271] Se encuadra en esta descripción del espionaje informático: La fuga de datos (Data leakage), esta consiste en la divulgación de información confidencial por lucro;[272] Otra forma de espionaje informático es el uso de las denominadas "llaves maestras" (Superzapping), es un ataque a un programa para cambiarlo, destruirlo, copiarlo, introducir datos, o impedir su uso correcto.[273]

5.2.2.3. Análisis de la Conducta típica

5.2.2.3.1. Tipología del espionaje informático

Para el caso la Ley Especial contra Delitos Informáticos y Delitos Conexos, regula el Espionaje Informático, en su artículo 12 a la letra expresa:

"El que con fines indebidos obtenga[274] datos, información reservada o confidencial contenidas en un sistema que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, será sancionado con prisión de cinco a ocho años. Si alguna de las conductas descritas en el inciso anterior se cometieren con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad del Estado, la

[270] Herrera, *Reflexiones sobre la delincuencia,* 21 (Véase la nota 156).
[271] Huerta, *Delitos Informáticos*, 138 (Véase la nota 155).
[272] José Soler de Arespacochaga, *El Delito Informática*, 19, goo.gl/GNgkj8.
[273] Rus, *Delito e informática: algunos aspectos*, 409 (Véase la nota 141).
[274] Lucero, "Nuevas formas de delinquir" (Véase la nota 167), comenta que en el Espionaje informático el sujeto activo busca información de forma sigilosa que tenga valor económico. Así, menciona entre algunas de los programas que realizan esas operaciones: los spywares; Rus, *Delito e informática: algunos aspectos* (Véase la nota 141). Spywares, son un programa o software que tiene por objeto registrar los hábitos y costumbres del usuario, sustrayendo información confidencial de los computadores.

confiabilidad de la operación de las instituciones afectadas, resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de la información de carácter reservada, confidencial o sujeta a secreto bancario, la sanción será de seis a diez años de prisión."

5.2.2.3.2. Tipo objetivo

El tipo penal básico de espionaje informático, lo da el inciso primero artículo 12 donde se establece la descripción de la conducta típica, se tiene como elementos objetivos la obtención de datos, información reservada[275] o confidencial, contenidas en un sistema que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, así, su modalidad verbal consiste en "obtención" esta evoca la acción de sustraer tanto físico como virtualmente.[276] La sanción según el tipo penal básico será de seis a diez años de prisión.

5.2.2.3.3. Tipo subjetivo

Para el caso como elemento subjetivo, es la existencia de un dolo y como elemento subjetivo distinto al dolo se encontró "fines indebidos" el párrafo primero al apoderarse la información, el elemento indebido, es parte integrante del ánimo, así, la persona, tiene como fines por ejemplo ejecutar otros delitos como el fraude, la revelación de secretos.

El mismo artículo en el párrafo segundo establece un tipo agravado y a la letra expresa: "Si alguna de las conductas descritas en el inciso anterior se cometieren con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las

[275] Teruelo, *Cibercrimen los delitos,* 136 (Véase la nota 124). Se entiende por información reservada, aquellas de acceso o conocimiento limitado, para terceros ajenos.
[276] Ibíd., *1*35.

instituciones afectadas,[277] resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de la información de carácter reservada, confidencial o sujeta a secreto bancario, la sanción será de seis a diez años de prisión."

El tipo agravado contiene como un elemento subjetivo distinto al dolo al ejecutar los verbos rectores del párrafo primero con el fin de obtener beneficio para sí o para otros. Asimismo cuando por revelar la información de carácter reservada, confidencial o de secreto bancario, poniendo en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas, o resultare algún daño para las personas naturales o jurídicas, así, la información respecto a los secretos de estado tales como de cooperación militar, pueden estar en peligro particularmente respecto a la defensa y seguridad nacional, también podrían ser los casos de espionaje informático industrial o comercial, al establecer el tipo penal el elemento subjetivo distinto al dolo, es decir: con el fin de obtener beneficio para sí o para otros, en otras palabras es la obtención, con ánimo de lucro y sin autorización, de información con un valor en el tráfico económico o de seguridad nacional.

5.2.2.4. Sujeto de la acción

En cuanto al sujeto activo, en la descripción del delito no se hace mención alguna respecto a la calidad de este, sin embargo la doctrina al referirse a los delitos en los que existe acceso a datos reservados con el fin de obtener información ajena, expresa que son conductas propias de un Hacker. Pero para el caso en la legislación del país puede ejecutarlo cualquier persona

[277] Como por ejemplo información reservada de carácter personal o familiar, que está en sistemas tecnológicos o soporte informáticos resguardados. Es decir, información de personas físicas, con las que pueden ser identificadas.

según se establece en el tipo penal, al utilizar la expresión: “El que” es decir que no requiere calidad especial.[278]

Sin embargo el espionaje informático se ejecuta mediante programas que no cualquier sujeto puede utilizar, estos facilitan la compilación de información, así como software que reconfiguran a los ordenadores sin el consentimiento de sus titulares, en este sentido existen por ejemplos los siguientes:

a. Dialers: Consiste en instalar un marcado telefónico, que genera conexiones telefónicas no solicitadas, por lo general mediante tarifas especiales, y operan solo por conexiones de modem.[279]

b. Adware: Son programas que recopilan información de los hábitos de navegación del usuario.[280]

c. spyware: Este tipo de programas compilan todo lo que se realiza en un pc, se oculta en otro que se instala al mismo tiempo que éste, remitiendo datos, costumbres, aficiones o historiales de navegación, a terceros.[281] Respecto al sujeto pasivo para el caso del espionaje informático es el titular de las Tecnologías de la Información y la Comunicación.[282]

5.2.2.5. Bien jurídico protegido

En cuanto al bien jurídico en el espionaje informático las conductas lesivas son contra la intimidad, como intermedio para evitar la transgresión mediata o inmediata de otros bienes, así, cuando se apoderan de información

[278] Teruelo, *Cibercrimen los delitos,* 121 (Véase la nota 124); Téllez, *Derecho Informático*, 595 (Véase la nota 175). Hacker o pirata informático es la persona que accede a una computadora de forma no autorizada e ilegal.
[279] Luis Aranton, *Sobre virus y virus*, 39, goo.gl/mF1ReS.
[280] Portaley.com, *El Delito de Espionaje por medios Informáticos*, goo.gl/FMEUxs.
[281] Aranton, *Sobre virus y virus*, 39. (Véase la nota 279).
[282] Huerta, *Delitos informáticos*, 134 (Véase la nota 155). En cuanto al sujeto pasivo, en la actualidad este delito tiene especial relevancia respecto a las empresas por las percepciones de la competición para la obtención de información. Así, se han dado casos de espionaje al venderse al mejor postor la información financiera.

reservada no forma parte de un acto de comunicación, pero transgrede la intimidad al ser información de carácter reservado de personas.[283]

Asimismo al trastocar la reserva de la información y la confidencialidad de los datos, en el caso de las agresiones informáticas a la esfera de la intimidad, especialmente en el caso de los bancos de datos el bien jurídico protegido es el derecho a la intimidad en relación al secreto de las telecomunicaciones.

El secreto empresarial, es transgredido respecto a la información almacenada informáticamente que supone un valor económico para la empresa, así, un sector de la doctrina sostiene que las conductas de espionaje informático transgrede la confidencialidad. Sin embargo inclusive dependido de la naturaleza de la información podría a ser la seguridad del estado, al revelarse secretos de Estado.

[283] Teruelo, *Cibercrimen los delitos,* 134 (Véase la nota 124). La doctrina asimismo establece que se transgrede la lesión de la libertad informática.

CONCLUSIONES

El derecho a la intimidad se ve amenazado con el surgimiento de las nuevas tecnologías, esto debido a la novedosa forma de almacenar, procesar y distribuir la información, consecuentemente al haber finalizado este trabajo de investigación correspondiente al tema El Intrusismo Informático y la Utilización del Derecho Penal Como Mecanismo de Tutela del Derecho a la Intimidad, es posible concluir lo siguiente:

En un principio el reconocimiento del derecho a la intimidad tuvo varias facetas hasta convertirse en el derecho personalísimo que conocemos, esto debido a que en las antiguas civilizaciones de Roma y Grecia dicho derecho carecía de relevancia, en razón de que se consideraba la vida de los ciudadanos publica, posteriormente se reconoce como una extensión del derecho a la propiedad y no como garantía del ser humano, teniendo principal relevancia en la protección a la vivienda, con la que restringen accesos indeseados, empero el Derecho a la Intimidad en su sentido moderno inicia con el articulo The right to privacy, escrito por los abogados estadounidenses Samuel Warren y Louis Brandeis, donde nace no solo como un reconocimiento de algo que le pertenece a la persona humana, sino que además se reconoce la necesidad de protegerlo frente a los abusos de terceros e inclusive del mismo Estado. En cualquiera de sus diversas concreciones el término intimidad es de aquellos conceptos indeterminados puesto que cada autor lo define según su criterio y conveniencia de estudio, así mismo se le acuñan diferentes sinónimos sin embargo este derecho como todo derecho fundamental se protege a través de la tutela de la administración pública usando como mecanismo y bajo el principio de mínima intervención el Derecho Penal esto con el fin de la pacífica convivencia en la sociedad.

En derecho comparado la protección a la intimidad, se entiende como sinónimo de privacidad, asimismo se protegen los datos personales, desde la Constitución desarrollándolo en las leyes secundaria, en algunas legislaciones se utilizan términos como vida privada, la confidencialidad, los datos personales, incluso la libertad, como dimensiones del derecho fundamental a la intimidad, lo que nos permite determinar que en la legislación comparada no existe un término preciso para referirse al derecho de intimidad, pero que sin duda tratan de proteger este derecho de instrucciones de terceras personas, se ha observado que la dualidad -intimidad y tecnología- que se ha establecido por el creciente aumento de las tecnologías de la información y la comunicación, hace que en legislaciones de otros países generen nuevos tipos penales acorde al contexto que ellos experimentan, a tal grado que regulen la protección del domicilio, las comunicaciones, la divulgación de información reservada, los accesos no autorizados a sistemas informáticos, como verdaderas invasiones a la privacidad de la personas, sancionándolos con penas de prisión acordes a la actividad ilícita que se está cometiendo.

El Estado debe intervenir en internet, se sabe que la red informática mundial surgió como un elemento de comunicación que permitiría crear una sociedad globalizada, no obstante al navegar pueden encontrarse contenidos nocivos, irrespetuosos o ilegales, como por ejemplo lo que se encuentra en una parte del ciberespacio denominada por los especialistas como deep web, dada esta situación los gobiernos deben establecer al igual que en la vida diaria reglas, siendo competencia del Estado por mandato constitucional el ejercicio de la función punitiva, sin perder de vista el principio de minina intervención, utilizando el derecho penal como ultima ratio, para así poder garantizar los bienes jurídicos como la seguridad informática, la información, la libertad informática entre otros.

Las relaciones en Internet son muchas veces de carácter transfronterizo lo que implica que algunos delitos informáticos, al operar mediante el Internet provoquen problemas de investigación, por la facilidad de traspasar las fronteras mediante la Red, desde un país remoto, el sujeto activo puede vulnerar la intimidad de otro sujeto que, a su vez, está en otro país dando lugar a problemas de competencia territorial, por lo que es necesario aplicar el principio de ubicuidad y así perseguir conductas delictivas sin tener el país de comisión del hecho y el del resultado, existiendo así una persecución extraterritorial, por la utilización de la internet como medio ejecución.

Existe una confusión terminológica y conceptual cuando se habla de delito informático, esto lleva a decir a algunos autores, juristas, catedráticos, técnicos, estudiantes que no existen delitos informáticos, por no estar tipificados como tal, y otros dicen que por su complejidad no puede existir un delito informático pero si una pluralidad de ellos, en esta investigación se afirma que el delito informático es toda acción típica, antijurídica y culpable, que tiene como fin obtener, manipular o perjudicar información contenida en sistemas informáticos, dañando bienes jurídicos. Así mismo son de naturaleza pluriofensivo, porque protegen: la información que garantiza el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública el orden económico.

Como suele suceder en el país, las leyes son promulgadas como una especie de moda, la creación de la Ley Especial Contra los Delitos Informáticos y Conexos no fue la excepción, esta fue festejada como un triunfo en todas las gestiones, sin embargo nunca se tomó en cuenta una verdadera política criminal, colocando nuevamente a El Salvador como uno de los países más atrasados en estos temas de fomento de las Tecnologías

de la Comunicación y la Información, y de castigar los delitos que conllevan a su uso inapropiado, otro apartado es que esta ley carece de herramientas procesales que investiguen el delito, perfilando a este instrumento con escasas posibilidades de volverse efectivas con los sujetos activos del delito.

El acceso indebido a sistemas informáticos, tipificado en Ley Especial Contra los Delitos Informáticos y Conexo, determina: 1. Que puede configurarse de dos formas, la primera como una conducta delictiva, y la segunda como instrumento para la comisión de otros delitos, como la Estafa Informática, El Espionaje Informático, La Piratería de Software, Acceso Indebido a los Programas o Datos Informáticos, Pornografía, Hurto de identidad, entre otros siempre regulados en la misma norma penal. 2. Que es un tipo penal especial, de mera actividad, porque se consuma en el instante en que se accede, se intercepta o se utiliza parcial o totalmente un sistema informático que utilice las Tecnologías de la Información o la Comunicación, ya sea de manera intencional y sin autorización o excediendo la que se le hubiera concedido. 3. Que tiene como elemento subjetivo el dolo directo, porque se realiza con el conocimiento que la acción es ilícita, por no tener autorización o exceder la que tiene. 4. Que el sujeto activo tiene conocimientos especiales de la informática para poder ejecutar la conducta típica, no obstante no se precisa que sea un perito en materia informática; y que el sujeto pasivo puede ser cualquier persona natural o jurídica que sea titular o parte de un sistema informático que utilice las Tecnologías de la Información o la Comunicación. 5. Que el bien jurídico protegido en este nuevo delito a prima facie es la información, sin embargo siempre está al margen de la protección a la intimidad, porque es la intimidad la que se ve transgredida por el acceso, interceptación o utilización parcial o total a un sistema informático que utilice las Tecnologías de la Información o la Comunicación, ya que en estos sistemas es donde las personas y entidades resguardan información

confidencial y de exclusivo conocimiento.

Como es sabido y sin entrar en mayores detalles, la misión fundamental del Derecho penal es la protección de aquellos intereses que son estimados esenciales para la sociedad y que permiten mantener la paz social. Sin embargo, la cuestión es de qué forma el Estado orienta dicha misión en el derecho a la intimidad frente al intrusismo informático, en esta investigación no se encontró un tipo que se adecue perfectamente a la protección de la intimidad frente a los usos inadecuados de los avances tecnológicos, no obstante se encontró tipificado en la Ley Especial Contra los Delitos Informáticos y Conexos el acceso indebido a sistema informáticos, abordado desde la protección del bien jurídico información, aunque este lleva aparejado derechos fundamentales como lo es la intimidad dicha tipificación se encuentra dentro del catálogo de delitos contra los sistemas informáticos, por lo que no se considera en una totalidad dirigido a la protección de la persona; en este caso la intimidad familiar y personal en todas sus concreciones queda sin protección del código penal ni de tratados o convenios internacionales, y se puede decir que raquíticamente está protegida por leyes especiales.

RECOMENDACIONES

Al estado de El Salvador, se le insta a que desarrolle estrategias nacionales como la creación de juzgados, fiscalías y defensorías especializadas en materia de criminalidad informática o delitos de alta tecnología acompañada por una amplia reforma legislativa a nivel procesal, actualizadora de las normas sobre investigación en esta materia, así mismo la capacitación del personal para afrontar el gran desafío que implica la implementación de la seguridad informática como bien jurídico colectivo, macrosocial o supraindividual, que contemplen por una parte campañas de concientización sobre los peligros en la red y las formas de poder denunciar un ataque a su intimidad, por otro lado mecanismos de coordinación con el sector privado y con otros países, para combatir estos delitos, de igual forma es necesario que el Código Penal, el Código Procesal Penal sea revisado para adecuarse a la realidad de la creciente prevalencia de actividades, documentación y pruebas electrónicas, y la necesidad de disposiciones, herramientas y entrenamientos adecuados.

En los delitos informáticos, el lugar de comisión y el de los efectos puede involucrar diferentes regímenes jurídicos. Por lo tanto, para una prevención, investigación, y persecución penal exitosa, será indispensable una fuerte cooperación y colaboración internacional en materia probatoria. Para ello es imprescindible que los países suscriban y ratifiquen las convenciones apropiadas, especialmente la llamada Convención de Budapest y sus Protocolos adicionales, aprobado por el consejo de Ministros de Europa en el año 2001. Esto le permitiría a El Salvador establecer un régimen rápido y eficaz de cooperación internacional; Intercambio de información sobre las novedades jurídicas, políticas o técnicas en el ámbito de delincuencia informática y la obtención de pruebas en formato electrónico; Obtención de

fondos como los del proyecto Global Action on Cybercrime Extended o por sus siglas en ingles GLACY -Acción Global Contra el Cibercrimen Extendido-.

A la Fiscalía General de la República, de gestionar instrumentos investigativos, métodos, software adecuados para la persecución de los delitos informáticos a fin de realizar los diferentes análisis de la investigación, es decir para llevar a cabo todas las diligencias necesarias y así, llegar a la verdad real de los hechos.

Reconociendo la necesidad de una cooperación entre el Estado y la industria privada en la lucha contra la cibercriminalidad y la necesidad de proteger los intereses legítimos vinculados al desarrollo y a la utilización de las tecnologías de la información y sabiendo que, una de las principales dificultades de la persecución de la cibercriminalidad, consiste en la dificultad para identificar a su autor, que fácilmente puede ocultarse tras el anonimato y opacidad que ofrecen las modernas y universales redes informáticas, altamente complejas, e intervenidas por múltiples operadores privados se le recomienda a la Asamblea Legislativa una reforma penal en el que se incluya la responsabilidad a proveedores de servicios informáticos y electrónicos mejor conocidos como ISP de internet, de conservar datos electrónicos específicos, incluyendo datos relativos al tráfico, almacenados por medio de sistema informático.

A la Biblioteca de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad de El Salvador, que surta sus anaqueles de libros sobre derecho informático, delitos informáticos, para que los miembros de la comunidad universitaria, consulten la bibliografía para elaborar trabajos investigativos del tema.

A la Facultad de Jurisprudencia y Ciencias Sociales, que actualice su pensum universitario e incluya cátedras respecto a delitos informáticos, investigación forense de delitos informáticos, derecho informático, con el fin de estudiar los problemas en materia de criminalidad informática para asegurar la frecuente puesta al día de las actividades ilícitas en la red.

BIBLIOGRAFÍA

LIBROS

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

Álvarez Caro, María. *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital.* Madrid: editorial Reus, 2015.

Álvarez Martínez, Joaquín. *La inviolabilidad del domicilio ante la inspección de tributos.* España: La Ley, 2007.

Amaya Amaya, Jairo. *Sistemas de Información Gerencial, Hardware, Software, Redes, Internet, Diseño.* Bogotá: Ecoe Ediciones 2010.

Andina, Fox. *Hacking desde cero*. Buenos Aires: Banfield-Lomas de Zamora Gradi, 2011.

Arévalo Silva, José Raúl. *La Normativa del Domicilio Civil en El Salvador.* El Salvador: Instituto de Investigación Jurídica, Univ. Dr. José Matías Delgado, 2012.

Avilés Gómez, Manuel, y otros. *Delitos y delincuentes: Cómo son, cómo actúan.* España: club universitario, 2010.

Bacigalupo, Enrique. *Manual Derecho Penal: Parte General.* Colombia: Temis, 1996.

Bonsembiante, Fernando, y otros. *"Llaneros Solitarios" Hackers, la Guerrilla*

Informática. Argentina: Espasa Calpe, 1995.

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

Creus, Carlos. *Derecho Penal: Parte Especial*. Tomo I. 6 Ed. Buenos Aires: Edit. Astrea, 1999.

Davara Rodríguez, Miguel Ángel. *Manual de Derecho Informático.* España: Thomson Aranzadi, 2006.

Del Rio, Raimundo. *Explicaciones de Derecho Penal Tomo I, Generalidades.* Chile, Nascimento.

Ekmekdijian, Miguel Ángel. *Hábeas Data: El Derecho a la Intimidad frente a la Revolución informática*. Buenos Aires: Desalma, 1996.

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

Fernández Teruelo, Javier Gustavo. *Cibercrimen los delitos cometidos a través de internet.* España: edit. Constitutio Criminalis Carolina, 2007.

Fontan Balestra, Carlos. *Derecho Penal: Introducción y parte general.* Argentina: Abeledo-perrot, 1998.

Galán Muñoz, Alfonso. *El fraude y la estafa mediante sistemas informáticos.* Valencia: edit. Tirant lo Blanch, 2005.

Gallardo, Miguel Ángel. *Cuatro Constituciones Federales de Centro América*

y las Constituciones Políticas de El Salvador. San Salvador: Trip. La Union, 1945.

García Ramírez, Sergio. *Derecho Penal Colección Panorama del Derecho Mexicano.* México: Porrúa, 2007.

Garrido Montt, Mario. *Derecho penal: parte general.* Tomo I. Chile: Editorial jurídica de Chile, 2010.

Garrido Montt, Mario. *Derecho penal: parte general.* Tomo II. Chile: Editorial jurídica de Chile, 2010.

Germán Bauché, Eduardo. *Lavado de Dinero Encubrimiento y Lavado de Activos.* Argentina.

Gonzales Rus, Juan José, y otros. *Delito e informática: algunos aspectos.* España: Universidad de Deusto, 2017.

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

Guibourg, Ricardo. *Manual de Informática Jurídica.* Argentina: edit. Astrea 1996.

Gutiérrez Francés, Luz. *Fraude Informático y Estafa*. Madrid: Ministerio de Justicia, 1991.

Heredero, Carmen de Pablos. *Informática y Comunicaciones en la Empresa.* Madrid: edit. ESIC, 2004.

Herrán Ortiz, Ana Isabel. *El derecho a la intimidad en la Nueva Ley Orgánica de Protección de datos personales.* Madrid: edit. Dykinson, 2002.

Herrera, Francisco José. *El Derecho a la Vida y el Aborto*. Colombia: Colección de Textos Jurídicos, 1999.

Huerta, Marcelo, y otros. *Delitos informáticos*. Argentina: Ed. ConoSur Ltda., 1998.

Krol, Ed. *Conéctate al mundo de Internet: Guía y Catálogo.* México: McGraw-Hill, 1995.

Lara, Carlos. *La privacidad en el sistema legal chileno.* Chile: ONG Derechos Digitales, 2005.

Lascano, Carlos Julio. *Derecho Penal: Parte General.* Argentina; Duarte Quirós, 2005.

López Ortega, Juan José. *Internet y derecho penal.* Madrid: Consejo General del Poder Judicial, 2001.

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

Martínez, Matilde Susana. *Protección de datos y habeas data: una visión desde Iberoamérica*. Madrid: Agencia española de protección de datos, 2015.

Mir Puig, Santiago. *Introducción a las bases del Derecho Penal*. Argentina: Julio César Faira, 2003.

Muñoz Conde, Francisco. *Derecho Penal Parte General*. España: Tirant lo Blanch, 2010.

Novoa Monreal, Eduardo. *Derecho a la Vida Privada y Libertad de Información: un Conflicto de Derechos*. Argentina: siglo veintiuno, 2001.

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

Petrino, Romina. *Convención Americana sobre Derechos Humanos y su Proyección en el derecho argentino.* Argentina: Universidad de Buenos Aires, 2013.

Prieto Espinosa, Alberto, y otros. *Introducción a la Informática.* Madrid: McGraw-Hill/ interamericana de España, 2002.

Ramírez, Juan Busto, y otros. *Lecciones de derecho penal Volumen II Teoría del delito, teoría del sujeto responsable y circunstancias del delito*. Madrid: Trotta, 1999.

Rodríguez Mourullo, Gonzalo. *Derecho Penal: Parte General*. 1a. ed. Madrid: Edit. Civitas, 1978.

Roxin, Claus. *Teoría del Tipo Penal.* Argentina: De palma, 1979.

Téllez Valdés, Julio. *Derecho Informático.* México: Mc Graw Hill, 2009.

Ureña López, Luis Alfonso. *Fundamento de Informática*. México: edit. Alfaomega, 2005.

Villavicencio Terreros, Felipe. *Derecho penal: parte general.* Perú: Grijley, 2006.

Zaffaroni, Raúl Eugenio, y otros. *Derecho penal: Parte general*. 2° edi. Buenos Aires: Ediar, 1977.

Zaffaroni, Raúl Eugenio. *Tratado de Derecho Penal: Parte General*. Tomo III. Argentina: Ediar 1981.

TESIS

Cabrera Moreira, José Pablo. “Los límites de la actuación de la prensa en relación con la administración de justicia en el ámbito penal”. Tesis Doctoral, Universidad Nacional de Loja, Ecuador. 2013. goo.gl/enl7Jz.

Hernández Martínez, Lucia Victoria. “El Derecho a la Intimidad Personal y su Actual Regulación Dentro del Ordenamiento Jurídico Salvadoreño”. Tesis de grado, Facultad de Jurisprudencia y Ciencias Sociales, Universidad de El Salvador, San Salvador, El Salvador, 2009. goo.gl/xu4Tga.

Ruiz Miguel, Carlos. “La Configuración Constitucional del Derecho a la Intimidad”. Tesis doctoral, Universidad Complutense de Madrid. 1992. goo.gl/qjgV95.

LEGISLACIÓN NACIONAL

Código Penal. El Salvador, Asamblea Legislativa de El Salvador, 1997.

Constitución de la Republica de El Salvador. El Salvador, Asamblea Legislativa de El Salvador, 1983.

Convención Americana Sobre Derechos Humanos Pacto de San José, OEA 1969.

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, ratificada por El Salvador el 20 de junio del año de 1978.

Ley de Acceso a La Información Pública. El Salvador, Asamblea Legislativa de El Salvador, 2010.

Ley Especial Contra Los Delitos Informáticos y Conexos. El Salvador, Asamblea Legislativa de El Salvador, 2016.

Ley Especial Para la Intervención de Las Telecomunicaciones. El Salvador, Asamblea Legislativa de El Salvador, 2010.

Pacto Internacional de Derechos Civiles y Políticos 1966. Ratificado por El Salvador, DL. Nº 27, de 23 de noviembre de 1979 publicado en DO. Nº 218, Tomo 265 del 23 de noviembre de 1979.

LEGISLACIÓN INTERNACIONAL

Código Penal de Colombia. Ley 599 de 2000.

Código Penal. Argentina, 1984.

Código Penal. Chile, 1874.

Constitución de la República de Argentina. Argentina, 1853.

Constitución de la República de Chile. Chile, 1980.

Constitución de la República de Colombia. Colombia, 1991.

Ley Relativa a Delitos Informáticos. LEY No. 19223, (Chile).

JURISPRUDENCIA

Sentencia de Amparo. Sala de lo Constitucional. Referencia 227-2000. El Salvador, Corte Suprema de Justicia, 2001.

Sentencia de Amparo. Sala de lo Constitucional. Referencia 494-2001. El Salvador, Corte Suprema de Justicia, 2002.

Recurso de Casación. Sala de lo Penal. Referencia 478-CAS-2004. El Salvador, Corte Suprema de Justicia, 2005. goo.gl/kNlzWW.

Sentencia de Hábeas Corpus. Sala de lo Constitucional. Referencia 135-2005AC. El Salvador, Corte Suprema de Justicia, 2008. goo.gl/jsHAIt.

Sentencias Definitivas de Inconstitucionalidad. Sala de lo Constitucional. Referencia 64-2006AC. El Salvador, Corte Suprema de Justicia, 2008. goo.gl/uG6xeG.

Sentencia de Hábeas Corpus. Sala de lo Constitucional. Referencia 231-2006. El Salvador, Corte Suprema de Justicia, 2009.

Sentencia de Amparo. Sala de lo Constitucional. Referencia 375-2011. El Salvador, Corte Suprema de Justicia, 2015.

REVISTAS JURÍDICAS

Ávila Hernández, Flor María, y Otros. “Los Derechos a la Intimidad y a la Privacidad en Venezuela y en el Derecho Comparado”. *Filosofía y Derecho*. Nº 11. 2007/2008.goo.gl/kiZSdd.

ColásTurégano, Asunción.“El delito de intrusismo informático tras la reforma del CP español de 2015”. *Iuris Tantum.* Nº 21. 2016. goo.gl/yszX5M.

Díaz Revorio, Javier. “El derecho fundamental al secreto de las comunicaciones”. *Universidad de Castilla-La Mancha.* 2006. goo.gl/n54Rn4.

Gonzales Rus, Juan José. “Protección Penal de Sistemas, Elementos, Datos, Documentos y Programas Informáticos”. *Ciencia Penal y Criminología*. RECPC 01-14 .1999. goo.gl/5fhRVk.

Kierszenbaum, Mariano. “El Bien Jurídico En El Derecho Penal. Algunas Nociones Básicas Desde La Óptica De La Discusión Actual”. *Universidad de Buenos Aires*. 2009. goo.gl/OcNpsE.

Maricel Lucero, Alberto Alberto. “Nuevas formas de delinquir”. *RITS.* N. 3. 2009. goo.gl/RqK2Bb.

Moscoso Escobar, Romina. “La Ley 19.223 en general y el delito de hacking en particular”. *Universidad de Chile*. Vol. 3 N.1. 2014. goo.gl/q6zOjz.

Posada Maya, Ricardo.“El delito de acceso abusivo a sistema informático: a propósito del art. 269ª del CP de 2000”. *Universidad de los Andes: Facultad de Derecho.* N. 9. 2013. goo.gl/j6OCsf.

Velásquez Velásquez, Santiago. “El Derecho a la Intimidad y la Competencia Desleal”. *Universidad Católica de Santiago de Guayaquil*. 2006. goo.gl/lSN8pi.

PÁGINAS WEB

Alcalá, Humberto Nogueira. *Tópicos constitucionales sobre la vida privada y la libertad de información ante la informática en Chile*. 2004. goo.gl/34BvjR.

Aranton, Luis. Sobre virus y virus. goo.gl/mF1ReS.

Castelli, Sebastián. “Intimidad, informática y derecho”. goo.gl/81sb09.

D'aussio, Andrés José, y otros. *Código Penal Comentado y Anotado Parte General .* Argentina: La Ley, 2005. *Artículos 1° A 78 bis.* goo.gl/IyjKRp.

Del Canto, Enrique. *Ciberdelincuencia Intrusiva: Hacking y Grooming.*goo.gl/lb88AI.

Del Pino, Santiago Acurio. *Delitos Informáticos: Generalidades*. Ecuador: Pontificia Universidad Católica del Ecuador, 2007. goo.gl/2nv7gv.

Del Pino, Santiago Acurio. *La Delincuencia Informática Transnacional y la UDIMP*. Ecuador: Ministerio Fiscal General del Ecuador, 2012. goo.gl/ucxSSk.

Derecho en Red. *Bien jurídico*. 2011. goo.gl/5R42lo.

Diccionario de la lengua española. goo.gl/3RE2vx.

Flores Mendoza, Fátima. “Delincuencia económica. Respuesta Penal Al Denominado Robo de Identidad en las Conductas de Phishing Bancario, Nuevos instrumentos jurídicos y tecnológicos”. *Estudios Penales y Criminológicos. Vol. XXXIV.* 2014. 323. goo.gl/fTqI6Y.

García Ricci, Diego. *El Derecho a la Privacidad en las Redes Sociales en Internet.*goo.gl/MJC3GX

García Rivas, Nicolás. *El Poder Punitivo en El Estado Democrático.* Cuenca: Universidad de Castilla - La Mancha, 1996. goo.gl/BfAE6N.

Glosario Web. *Breve Historia del Internet*. goo.gl/eR2lFH.

Herrera Bravo, Rodolfo. *Reflexiones sobre la delincuencia vinculada con la tecnología digital(basadas en la experiencia chilena).* goo.gl/5OOe4H.

Landeira, Renato Alberto, y otros. *Diccionario jurídico de los medios de comunicación.* Madrid: Reus, 2006. goo.gl/wpe1QA.

LEGAL CORP. *El Derecho a la Protección de Datos Personales*. goo.gl/P3BGPu.

Listasal. *Historia del Internet en El Salvador*. goo.gl/R6txw3.

Pagés López, Javier. *Informática forense*. Madrid: Universidad Politécnica de Madrid, 2013. goo.gl/snbz93.

Pérez Alvares, Fernando. *Moderno discurso penal y nuevas tecnologías.* España: universidad de Salamanca, 2013. goo.gl/76MKjo.

Pons Rafols, Xavier. *La Declaración universal de derechos humanos: comentario artículo por artículo.* Barcelona: trad. Victoria Pradilla edit. Icaria. goo.gl/6BwmZA.

Portaley.com. *El Delito de Espionaje por medios Informáticos*. goo.gl/FMEUxs.

Rivas, José. *Historia de la Computación en El Salvador.* goo.gl/lx49kj.

Rodríguez Magariños, Faustino Gudín. *Nuevos Delitos Informáticos: Phising, Pharming, Hacking y Crackin.* goo.gl/GHKKHF.

Romero Casabona, Carlos María. *De los delitos informáticos al cibercrimen.* España: Universidad de Salamanca, 2007. goo.gl/6kA7eD.

Rosende, Eduardo. *Reflexiones sobre su inclusión al código penal*. goo.gl/Go38Va.

Sánchez Bercedo, Manuel. *El delito de intrusismo informático o Hacking Artículo 197.3 CP.*goo.gl/QXktuK.

Sánchez Carazo, Carmen. *La intimidad: un derecho fundamental de todos.* goo.gl/gFDtF.

Sánchez, Pablo, y otros. *El sistema español: Los Delitos.* España: Universidad de Navarra. goo.gl/PtVlEp.

Soler de Arespacochaga, José. El delito informático. goo.gl/GNgkj8.

Trigo Calonge, Ricardo Manuel. *Internet, Intimidad y Privacy.* Madrid: 2008. goo.gl/srH5XL.

Useros Raboso, Carlos. *El Contrato de Adhesión Online en Redes Sociales.* goo.gl/wggmdu.

Vázquez Gonzales, Magaly. *Ciencias penales, temas actuales: homenaje al R.P. Fernando Pérez Llantada.* Caracas: Universidad Católica Andrés Bello, 2004. goo.gl/M87f1H.

VillazánOlivarez, Francisco José. Manual de Informática I. México: Universidad Michoacana de San Nicolás de Hidalgo, Facultad de Contaduría y Ciencias Administrativas, 2010. goo.gl/rLtoIo.