UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

DELITOS CIBERNÉTICOS INTERNACIONALES Y SU IMPACTO EN LOS DERECHOS HUMANOS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN RELACIONES INTERNACIONALES

PRESENTA:

CINTHYA MARIANA MATIAS LEON

DIRECTOR: DR. JUAN CARLOS VELÁZQUEZ ELIZARRARÁS

CD. UNIVERSITARIA, 2 DE FEBRERO DE 2023

INDICE

INTRODUCCION

Actualmente el progreso tecnológico que a diario experimenta la sociedad ha dado como consecuencia una evolución en las formas de delinquir, como las que representan los denominados delitos cibernéticos que son una realidad en el marco regulatorio del derecho internacional y un problema de especial gravedad para la comunidad de Estados, que los diferentes órdenes jurídicos nacionales y las organizaciones internacionales han tipificado como delitos informáticos, ciberdelitos o crímenes cibernéticos, definiéndolos en términos generales como cualquier acto antijurídico que atenta y que se da en contra de vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos, redes de Internet, empresas, personas físicas, entre otros sujetos.

Actualmente el uso de la tecnología se ha incorporado como un medio necesario en la vida humana a nivel internacional para poder comunicarnos, comprar, vender, tomar clases en línea, informarnos debido a la pandemia llamada covid-19 desde hace un año aproximadamente, se comenzó por una medida de seguridad sanitaria y posteriormente generó una serie de conflictos en la tecnología que ya se conocía, pero con mayor magnitud debido a su desarrollo. Este trabajo explicará de forma específica cada delito cibernético y su impacto en la sociedad internacional y también en los derechos humanos.

Los tipos de delitos cibernéticos que reconoce Naciones Unidas son los siguientes:[1] fraudes cometidos mediante manipulación de computadoras, falsificaciones informáticas, daños o modificaciones de programas o datos computarizados, acceso no autorizado servicios y sistemas informáticos, entre los principales; sin embargo, existen más como la prostitución, la pornografía, la trata de personas, secuestro virtual, Stalking, Sexting, Ciber odio, ciberbullying, piratería, propiedad intelectual, ciberterrorismo o ciberataque, entre otros que aún no son del todo reconocidos o bien no están tipificados por el derecho penal lo que obviamente impide que se prevenga y castigue o sancione su comisión tanto por personas físicas como morales e incluso agencias gubernamentales.

[1] Foro de Seguridad, Tipos de Delitos cibernéticos en línea con dirección URL: http://www.forodeseguridad.com/artic/discipl/disc_4016.htm consulta 26-09-16.

Los delitos cibernéticos se han analizado básicamente desde el plano económico, sin embargo también ha tenido repercusiones en el plano ético, jurídico y sociocultural por lo que el propósito de esta investigación es enfocarlo desde la perspectiva de los derechos humanos, que son definidos *grosso modo* como un conjunto más o menos sistematizado de principios o normas que tienen por finalidad regular, proteger y preservar los derechos del ser humano, con la ayuda de instrumentos o mecanismos nacionales e internacionales.

Los derechos humanos son derechos naturales que se reconocen en el orden jurídico interno de muchos Estados y en tratados y convenciones internacionales, y en su visión doctrinaria general se extienden más allá del derecho y conforman una base ética y moral que debe fundamentar la regulación de los derechos de la persona humana. En esta tarea, la Declaración Universal de los Derechos Humanos de 1948 se ha convertido en una referencia clave para la protección y fundamentación de los derechos del hombre, aunque también se observan algunos problemas en cuanto a su eficacia, ya que existe una gran desproporción entre lo violado y lo garantizado por el Estado soberano, que ha logrado crear su reconocimiento y atribución.

Los derechos humanos han evolucionado conforme al desarrollo de la sociedad, por lo que se han clasificado en varias generaciones: la primera generación, son los derechos políticos y civiles, con el principio de libertad; la segunda, está constituida por los derechos, sociales y culturales vinculados al principio de igualdad; la tercera generación, tiene como referentes verbigracia el derecho a la paz, a la calidad de vida, siempre vinculado a la solidaridad; y, finalmente, la cuarta generación es novedosa ya que esta nos va a permitir tener acceso a las tecnologías de la información y comunicación, con la finalidad de fomentar, por ejemplo, el derecho a la calidad de la información y del flujo e intercambio de datos de capital humano con el objetivo de que la sociedad de la información pueda prevenir y sancionar cualquier tipo de violación a estos derechos avanzados o simplemente ‘tecnológicos’.

Es importante conocer el impacto que tienen los delitos cibernéticos en los derechos humanos específicos, como, por ejemplo: el derecho de propiedad intelectual, el derecho de autor, el derecho a la libertad de expresión, el derecho a la información, derechos de la vida y el ofendido, derecho a la protección de datos personales,

derechos del niño, derecho a la reparación de violaciones a los derechos humanos, entre otros.

Los delitos internacionales cibernéticos se han desarrollado e intensificado debido a las diversas tecnologías de la información y comunicación (TIC), las cuales han influido en las relaciones internacionales, en virtud de que han originado nuevos canales de comunicación y difusión del conocimiento, y han agilizado la dilución de fronteras, revolucionando los mecanismos de relación entre Estados, y generando un nuevo sistema de interacción generalmente conocido como el “ciberespacio”, el cual se define como un área intangible que no tiene ubicación fija, que ha facilitado y ahorrado tiempo en diversas actividades tales como: transacciones bancarias, comercio electrónico, comunicación virtual, creación de redes interactivas, entre otras. Pero también ha dado pie a la diversificación del crimen organizado a través de Internet ya que existen sitios donde se desarrollan acciones delincuenciales como prostitución, pornografía, tráfico de órganos, tráfico de personas, en fin, una multitud de infracciones que es posible realizar a través de este medio; por esta y otras razones, se trata de un tema de investigación de suma importancia para la comunidad internacional.

Los delitos cibernéticos internacionales son un nuevo campo de estudio para las relaciones Internacionales, a partir de cuya metodología es posible su análisis integral, pues tradicionalmente se les ha tratado desde la perspectiva unidisciplinaria, esto es, desde la óptica exclusiva de la economía, el derecho o la política, sin considerar otras implicaciones que tiene el fenómeno en los planos de moral, la sociología, la antropología social, la ética, la psicología social, la cultura y la educación, o en suma, en la integridad física y mental de los individuos. De ello es viable desprender la necesidad de crear más y mejores leyes y tipificar con claridad las conductas criminales atípicas y los sistemas de penalización y combate más eficientes, con el objetivo terminal de brindar a la sociedad estándares más efectivos de protección de los derechos humanos de los cibernautas y de las personas en general.

Los delitos internacionales cibernéticos y los derechos humanos son un reto para el Derecho Internacional, puesto que la regulación y los mecanismos que han implementado no han sido suficientes debido al constante desarrollo del internet y la

tecnología, los cuales nos han llevado a una sociedad más compleja que cada vez requiere una normatividad más sólida.

El desarrollo del internet y la tecnología y la falta de información sobre la implementación de éstas ha dado pie a que surjan los delitos cibernéticos y en este caso dañando gravemente a los derechos humanos de los cibernautas, por lo que es necesario que los Estados participen más a fondo sobre estos temas para poder tener 'ciberseguridad', a nivel nacional e internacional.

El propósito de esta investigación es analizar la importancia de los delitos cibernéticos desde la perspectiva de los derechos humanos, puesto que es un tema novedoso y poco abordado no solo para el derecho internacional sino también para la sociedad internacional, la cual requiere de una regulación eficaz que pueda resolver dichos delitos; así como explicar el papel de los Estados y Organizaciones en el diseño y operación de mecanismos de regulación y combate de los ciberdelitos, y su interacción en los planos nacional, regional e internacional.

Esta investigación, se divide en 4 capítulos, los cuales describiré a continuación a grandes rasgos. El capítulo primero se dará la descripción jurídica y naturaleza del ciberespacio y su función en las relaciones internacionales, además del papel que juega el internet en los delitos cibernéticos y como herramienta ante el mundo, se hará una distinción sobre el ciberespacio e internet, porque suelen confundirse e implementarlos erróneamente por lo que se hablará de otros términos de suma importancia que han surgido sobre el tema, como por ejemplo los niveles que tiene internet y para qué sirve cada fase etc. por último se explicará cómo se ha ido desarrollando e incrementando avances relevantes sobre su regulación, prevención, combate y los retos e importancia del ciberespacio, internet y la Unión Internacional de Telecomunicaciones para crear un marco regulatorio frente a los delitos cibernéticos internacionales.

El segundo capítulo se explicara la evolución y la crítica de los derechos humanos en las relaciones internacionales, además de hablar sobre su evolución y sus diferentes etapas donde han ido naciendo las diferentes generaciones que han ido formando y caracterizando en cada etapa a los delitos cibernéticos que impactan o violan a los derechos humanos, siempre se ha tocado el tema de los delitos cibernéticos desde el ámbito económico en pérdidas millonarias o en el aspecto político pero es importante

resaltar la importancia que tienen en la afectación de los derechos humanos de la sociedad mundial ya que hoy en día se han incrementado un gran índice de delitos que son favorecidos por el internet y que no están tipificados, lo cual no es posible castigarse y ha dado pie a que se desarrolle y realicen de manera libre y sin castigo. También se explicará la similitud e importancia que tiene con el derecho internacional, el derecho internacional penal y el derecho internacional de los derechos humanos y de ahí la importancia en las relaciones internacionales, además de abordar todos los instrumentos jurídicos importantes y relacionados con el tema.

El tercer capítulo se abordará el análisis de los delitos cibernéticos internacionales; así como la clasificación y su contenido, ya que cada país y diversos autores dan sus diferentes puntos de vista sobre dicho tema, para así poder comprender el enfoque y jurisdicción que le otorgan cada uno de ellos. Es de suma importancia dar a conocer y explicar todos los tipos de delitos para poder comprender su regulación o nulidad que tiene cada uno en cada rincón del mundo, así como también se mostraran cifras de los delitos mayormente cometidos y muchos de ellos sigue sin estar castigados. Y en un según apartado se plasmará todo lo relacionado con los delitos cibernéticos que tienen un mayor impacto en la cuestión de derechos humanos como la prostitución infantil, trata de personas, stalking, ciber odio, ciberterrorismo, entre otros.

El cuarto y último capítulo se trata de revisar y a analizar las políticas y ordenamientos jurídicos estatales y el marco legal internacional e institucional aplicables a los delitos cibernéticos, por lo que comenzaremos con los organismos intergubernamentales generales, como la ONU, después con los organismos especializados de la ONU, como lo son UIT, y los organismos intergubernamentales fuera de la ONU; OCDE, INTERPOL, posterior con los organismos intergubernamentales regionales; Consejo de Europa, La Unión Africana, Liga Árabe y el Consejo del Golfo, la OEA, y por ultimo foros y grupos interestatales, el G7, Foro de gobernanza, APEC, FBI, Policía Cibernética en México, estos muestran su gran labor y compromiso para combatir a estos delitos. También se busca explicar cada familia jurídica y que países forman parte y hacer una comparación para poder entender porque algunos ordenamientos jurídicos y/o marcos regulatorios no son compatibles y por eso mismo no podría existir una ley homogénea para todo el

mundo sobre este tema debido a que cada familia jurídica que adopta cada país para su regulación, y así poder comprender como se mueven las leyes de cada Estado para poder prevenir, difundir y tratar de erradicar los delitos cibernéticos que día a día se han intensificado y que se denominan como un delito transnacional como se menciona en la Convención de Palermo, que es un tratado multilateral ,enfocado primordialmente a prevenir y combatir la trata de personas especialmente de mujeres y niños, también al tráfico de armas aunque no esté explícitamente plasmados o como tal, por las características que catalogan a los delitos cibernéticos, se entiende implícitamente que es un instrumento que puede ayudar a erradicar y regular la delincuencia organizada transnacional. En cambio, la Convención de Budapest, ha sido el único instrumento que aborda y reconoce a la mayoría de los delitos cibernéticos, sin embargo, hay países como México que aún no se logra regularizar del todo en esta rama.

Capítulo 1. Descripción jurídica y naturaleza del ciberespacio, y su función en las relaciones internacionales.

1. Ciberespacio.

Actualmente las llamadas nuevas tecnologías de la información (TICS) han acaparado la atención para investigar el desarrollo y futuro de estas tecnologías e interacción con la sociedad internacional, puesto que es un nuevo medio para interactuar no solo para el ámbito de negocios sino también, político, ético, jurídico y en este caso un gran impacto hacia los derechos humanos, esto ha dado lugar a la manera de pensar de las siguientes generaciones en su cultura, ideología, la información y la manera de comunicarse ahora es distinta.

No hay que olvidar que también existen espacios de dominio que se denominan los Global Commons[2] como; tierra, mares, océanos, aire y el ciberespacio que son vistos desde el punto de vista geoestratégico que es el objeto de estudio de este capítulo y que cabe resaltar que el ciberespacio se diferencia de los demás por su naturaleza artificial. Esta es un área reciente y novedosa que el hombre ha ido explorando que a comparación de los demás dominios este aún no ha sido regulado de manera uniforme y total, pero si existen estructuras para combatir el cibercrimen, más adelante se ira explicando el tema.

La historia del prefijo “ciber” proviene de una palabra más antigua pero hoy en día más utilizada la “cibernética”, que, a su vez, tiene una raíz etimológica griega; procede de kybernetike, cuyo significado es el de arte de la navegación, otros la han querido nombrar como tele polis o ciudad global.[3] El ciberespacio es considerado un lugar intangible, artificial creado por medios informáticos, los cuales lo utilizan como

---

[222] *Son aquellos espacios que normalmente sin estar sujetos a la soberanía de país alguno, son utilizados por las naciones para transportar personas o bienes y servicios o para transmitir datos. algunos son utilizados por el conjunto de las personas o bienes de servicios también se han añadido el espacio aéreo y el espacio exterior de acuerdo a las circunstancias concretas que se dieron en el momento de su diseño y desarrollo. Kut Nebrea, La importancia de dominar los Global Commons en el siglo XXI, en línea con dirección URL: https://www.ieee.es/Galerias/fichero/docs_marco/2015/DIEEEM29-2015_Global_Commons_XXI_Alexander_Kutt.pdf consultado 7-07-2018.*

[3] *ANNAN, Kofi: Informe a la Asamblea del milenio de las Naciones Unidas (2000) en línea con dirección URL: http://www.un.org/spanish/milenio/sg/report/full.htm. Consultado 10-08-2018.*

una herramienta o medio de comunicación e interacción internacional, otros definen al ciberespacio como "la geografía virtual creada por computadoras y redes"[4]

Gibson W. Neuromante nos dice que el ciberespacio surgió en el mundo de la literatura, por lo que sugiere una descripción de diversas dimensiones, debido a que es un término que trata de representar lo irrepresentable, en otras palabras, es solo una idea que se encuentra en nuestras mentes y como representación mental se apoya con las redes y ordenadores conectados, y como consecuencia de este conjunto ha surgido nuevas formas culturales, de pensar, hablar y comunicarse y esto a su vez genera una identidad propia para este mundo “paralelo”.[5]

El ciberespacio surgió por medio de unos dispositivos que al vincularse en red producen un sistema interconectado a escala planetaria. Estos recursos combinados generan el “nuevo mundo": el ciberespacio, como inteligencia colectiva. También se conoce como un espacio virtual que contiene todos los recursos de información y comunicación disponibles en la red, donde los sujetos interactúan entre sí, a través de las nuevas tecnologías. Las barreras físicas desaparecen, tiempo y espacio toman una nueva dimensión, y un individuo puede comunicarse con otros individuos en diferentes lugares del planeta al mismo tiempo.[6]

Hans Kleinsteuber, proporciona un concepto más restringido del ciberespacio denominándola como “Carta Magna de la Era de la Información” la cual se caracteriza por estar limitadas en su contenido por el poder de control del Estado y la tendencia hacia la centralización y la burocratización. El ciberespacio, por el contrario, tendría justamente las características opuestas.

El Departamento de Defensa de los Estados Unidos lo define como “un dominio global dentro del entorno de la información. Compuesto por una infraestructura de

---

[4] BRUNNER, J.J.: Cibercultura: la aldea global dividida. Mesa redonda sobre Cibercultura, Hannover, 2000, en línea con dirección URL: http://www.geocities.com/brunner_cl/cibercult.html consultado 14/09/18.

[5] TRIANA Lodoño Verónica, Representaciones del cuerpo y la mente de Neuromancer imaginado por William Gibson, en línea con dirección URL: https://repositorio.uniandes.edu.co/bitstream/handle/1992/14224/u240977.pdf?sequence=1 consultado 17-03-18

[6] S/A Concepto de ciberespacio, en línea con dirección URL: https://www.uv.es/cefd/5/lima.html consultado 30/10/18.

redes tecnológicas de la información y los controladores y procesadores integrados junto con sus usuarios y operadores".[7]

1.1. Características del ciberespacio.

Es importante señalar las características del ciberespacio, debido a que representa un nuevo campo de estudio para las relaciones internacionales, por lo que es necesario conocer como está integrado este escenario que ha demostrado en los últimos tiempos sobrepasar los límites de cómo y cuándo interactuar; entre las características del ciberespacio están las siguientes:

- Identidad, flexibilidad y anonimato: Se refiere a la falta de interacción física cara a cara causa un impacto en cómo la gente presenta su identidad. Pues se tiene la oportunidad de expresar sólo algunas partes de tu identidad o la elección de quedarte en el anonimato, también te da la opción de tener una identidad imaginaria o falsa.[8]
- En el ciberespacio todos tenemos la misma oportunidad de comunicación. Algunos llaman a esto Democracia Net.[9]
- Trasciende los límites espaciales: Las distancias geográficas no limitan quién pueda comunicarse con quién. Puedes comunicarte con cualquier persona que esté en otro país a cualquier hora.
- Tiempo extendido y condensado: puede haber una comunicación con cualquiera vía internet, puede haber varias personas sentadas en su computadora al mismo tiempo. Este tipo de comunicación crea un espacio temporal donde el estar, como tiempo interactivo se extiende. En esta modalidad se tiene tiempo para pensar cosas y dar una respuesta.

---

[7] *GOMEZ, de Agreda Ángel, El ciberespacio como escenario del conflicto. Identificación de las amenazas, 2012, en línea con dirección URL: https://dialnet.unirioja.es/servlet/articulo?codigo=4540391 consultado 30/10/18.*

[8] *S/A EcuRed, Características del Ciberespacio, en línea con dirección URL: https://www.ecured.cu/Ciberespacio consultado 30/10/18*

[9] *Se refiere a que usan las nuevas tecnologías de la información y los medios alternativos de comunicación para satisfacer sus necesidades en beneficio de todos y para mejorar procesos dentro de una sociedad virtual.*

- Existen conductas o acciones licitas e ilícitas que son adoptadas por los cibernautas.

Cabe resaltar las áreas que tiene el ciberespacio la primera y es la que compone la mayoría es el internet, también se encuentra la World Wide Web (Web), los grupos de noticias USENET y el Internet Relay Chat (IRC). A cualquiera de ellos es posible acceder con un acceso inalámbrico a Internet o con cualquier tipo de red que se tenga a la mano.[10]

Capas del ciberespacio.

De acuerdo con Martin C. Libicki se divide el ciberespacio en tres capas donde se mostrará cada vulnerabilidad:

La capa sintáctica	Se integra de todos los datos, los programas que introducimos para gestionarlos, todo el conocimiento en los servidores y en los discos.
La capa semántica	Se integra de protocolos, sistemas operativos y demás lenguajes que sirven para hacer funcionar los programas y legibles los datos constituyen. Contienen las instrucciones que los diseñadores y usuarios introducen en los sistemas y es básica para permitir que los terminales se comuniquen entre ellos. Los sistemas operativos son uno de los elementos críticos.
La capa física	Es aquello que podemos ver y tocar como; discos duros, monitores, teclados, ratones, la impresora, el router. También es de suma importancia conocer que la capa física también podría ser cables submarinos, servidores ubicados en otros países etc.

[10] S/A EcuRed, Áreas del ciberespacio, en línea con dirección URL: https://www.ecured.cu/Ciberespacio consultado 30/10/18

1.2. Internet y Ciberespacio.

El origen del internet nos puede remontar a 1962, con el nacimiento del programa "APARNET" producto de la idea que se conoció como "DARPA", la cual visionariamente proyectaba conectar computadoras en modo simultaneo a escala global. El origen del internet deriva, en gran medida, de una aplicación de comunicaciones militar, la cual se denominó, como ya habíamos mencionado "APARNET", este concepto fue financiado por el Departamento de defensa de los Estados Unidos. Es a partir de los años 80 con el surgimiento del dominio "www" de la definición del protocolo (TIC´s) y la palabra internet que se conoció a la red como actualmente se conoce. El término del "ciberespacio" actualmente forma parte del argot técnico, y comúnmente se utiliza para referirse a los contenidos y actividades que acontecen en internet. Este término se utiliza para referirse a objetos, identidades, lugares y su respectivo vínculo y asociación con sistemas de cómputo, tecnologías de información y las actividades que tienen lugar a través de internet, sin tener en cuenta la ubicación física y geográfica de los servidores, operadores y actores.[11]

Hacia el año de 1983, comenzó esta novedad tecnológica a incursionar en varias empresas y universidades, donde deciden entrelazar o unir sus redes internas de computación entre sí, con el fin de comercializar servicios y productos, comunicar los grupos de estudio y de investigación universitaria. En principio era una red poco conocida comercialmente, solo los estudiantes tenían derecho a ella y fueron convirtiendo la red en un lugar de diversión para hacer toda clase de maldades, como reservar y comprar productos a nombre de otras personas.[12]

El peligro de que se cometan delitos a través de internet es latente, pues en el ciberespacio se maneja todo tipo de información; pública, privada, comercial, de defensa nacional e inclusive de inteligencia estratégica, etc. Y así todos estos datos están almacenados en un espacio real y en la vida de las personas es total. Estadísticas de comScore "señalan que existen más de quince millones de usuarios en internet a nivel mundial con un rango de edad mayor a los 15 años y que tienen

[11] Leiner M. Barry, Breve historia del internet, en línea con dirección URL: https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/ consultado 3/05/22

[12] Op. Cit.

acceso desde su hogar o centro de trabajo, además con la creación de centros llamados “cibercafé” cualquier persona de cualquier edad que sepa usar esta tecnología puede acceder a internet con tan solo pedir que le renten una máquina.[13]

1.2.1. Principios básicos.

En cuanto al internet existe una serie de principios básicos propuestos y basados en la Carta Universal de Derechos Humanos y que todo ciberciudadano debe conocer, para poder debatir y hacer que se convierta en ley y así poder tener respaldo o defensa online;[14]

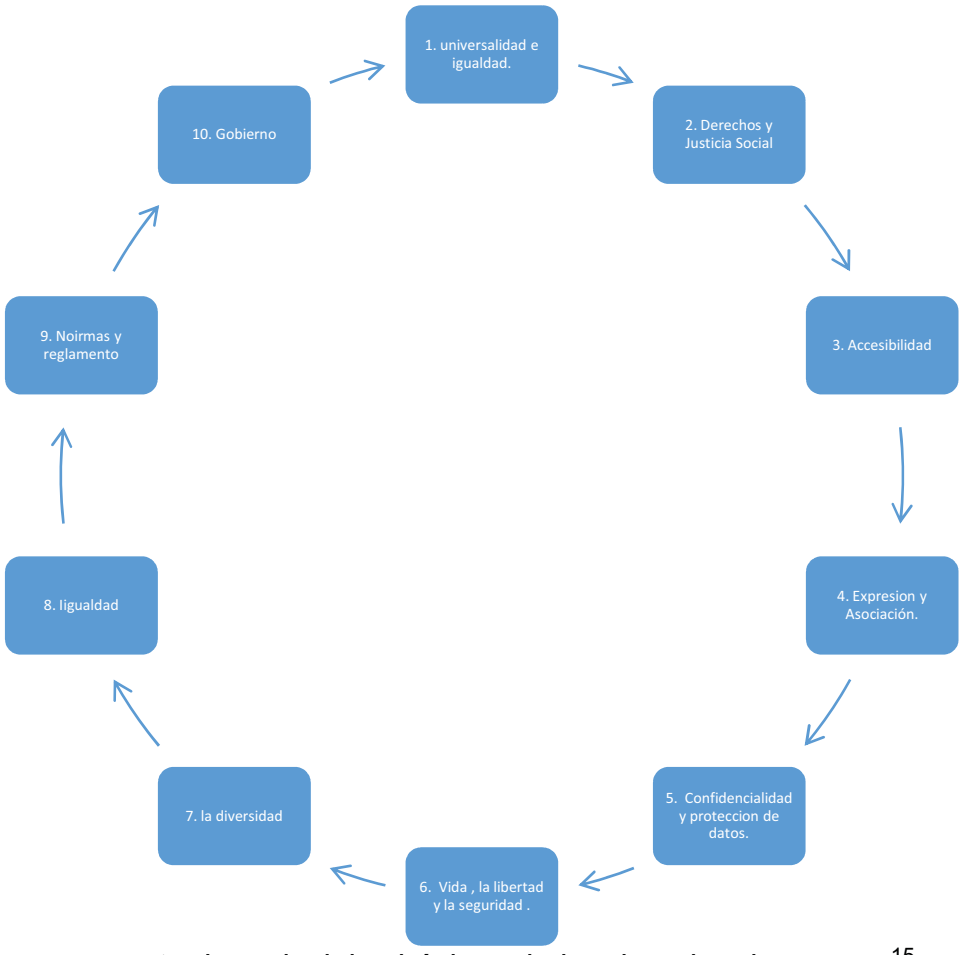


Diagrama que muestra los principios básicos de los derechos humanos.[15]

[13]Division Computer Forense, en línea con dirección URL: https://www.delitosinformaticos.info/peritaje_informatico/estadisticas consultado 3/05/22

[14] *S/A los Derechos y Principios de Internet en línea con dirección URL: http://especiales.laprensagrafica.com/2011/internet/2011/04/10-derechos-y-principios-de-internet/ consultado 02-10-2020*

[15] *Cuadro Elaborado por Cinthya Mariana Matias Leon, pero la información es basada por la Colisión de Principios básicos de Internet, en línea con dirección URL: https://internetrightsandprinciples.org/wpcharter/ consultado 02/10/2020.*

La coalición de derechos y principios de los derechos humanos de internet son una propuesta internacional con gran relevancia para poder crear ética y normas en la vida virtual, debido a las circunstancias que se están generando en la sociedad internacional se requiere de ampliar y tener nuevas medidas y protocolos para lograr un orden jurídico y la paz.

1.2.2. La importancia de Internet en las relaciones internacionales.

La sociedad del conocimiento[16] se ha convertido en una parte fundamental para el mundo en la actualidad, sin embargo, pata que se puedan llevar a cabo se requiere ayuda de las tecnologías de la información y comunicación (TIC´s) y lo que abordaremos es la internet mejor conocida como la red de redes que no solo es una simple tecnología sino también representa una poderosa palanca de transformación para el mundo, en el plano económico, político, social y cultural hoy en día.[17]

Internet incide en el desarrollo de las comunicaciones, en la organización y producción de servicios, la actividad de los diferentes gobiernos y afecta actividades tan importantes como la educación, el cuidado del medio ambiente o la salud.

Con la llegada de la sociedad pos industrial, el conocimiento se ha convertido en el principal motor de crecimiento y desarrollo tanto económico, político, social y cultural. Internet puede representar, la gran diferencia que permita alcanzar mayores niveles de educación, desarrollo, transparencia y democratización.[18]

Internet constituye actualmente la base tecnológica de la forma organizativa que caracteriza la era de la información. El acceso a internet permite el ejercicio de las libertades de forma mucho más asequible, a través de los múltiples sistemas de comunicación que coexisten en su seno tales como las redes sociales, los blogs, los foros virtuales de discusión facilita la libertad de expresión y de asociación, permite compartir el conocimiento y el aprendizaje, potencia la colaboración entre persona y universidades o empresas de todo el mundo e impulsa el desarrollo social y

---

[16] ***La Sociedad del conocimiento*** *refiere al tipo de sociedad que se necesita para competir y tener éxito frente a los cambios económicos y políticos del mundo moderno. Asimismo, se refiere a la sociedad que está bien educada, y que se basa en el conocimiento de sus ciudadanos para impulsar la innovación, el espíritu empresarial y el dinamismo de su economía. Consultado en línea con dirección URL: http://www.oas.org/es/temas/sociedad_conocimiento.asp consultado 14-10-19.*

[17] *CARBONELL, José Miguel, Capitulo II, El Acceso a Internet como derecho humano en línea con dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3647/8.pdf consultado 12-10-19.*

[18] *CARBONELL, Óp. Cit. p.19*

económico, “la nueva tecnología de la libertad” considera Manuel Castells que a través de internet aumenta de forma exponencial la capacidad de la gente para comunicarse e interactuar en la relación a temas e intereses que le son comunes.[19]

El uso de internet facilita notablemente el ejercicio de diversos derechos reconocidos en la propia Constitución Política de nuestro país; tales como la educación, la cultura, el acceso a la información, la libertad de expresión, libertad de religión.

La importancia de internet en las relaciones internacionales ha funcionado en la sustitución de la relación de los Estados por la manera más rápida de poder comunicarse y así mismo poder crear un nuevo orden internacional donde exista más participación, transparencia, autonomía y resistencia para controlar o limitar la información,[20] pero también la nuevas tecnologías de la información han sido perjudiciales en el comportamiento de las personas y de Naciones pero este tema de abordará en el capítulo tercero.

Internet es visto como un derecho humano básico y la Asamblea General de las Naciones Unidas declaró en el 2011 como; “un derecho humano por ser una herramienta que favorece el crecimiento y el progreso de la sociedad en su conjunto”. El Consejo de Derechos Humanos de las Naciones Unidas aprobó la resolución para la promoción, protección y el disfrute de los derechos humanos en internet, el documento establece, que el acceso a internet será considerado, de ahora en adelante, un derecho básico de todos los seres humanos. La resolución anima a todos los países a proveer a sus ciudadanos de acceso a la red y condena a las naciones que alteran esta libertad. El texto menciona que “los mismos derechos que tienen las personas offline deben ser protegidos online” especialmente en lo que respecta a la libertad de expresión defendida por el artículo 19 de la Declaración Universal de los Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos.[21]

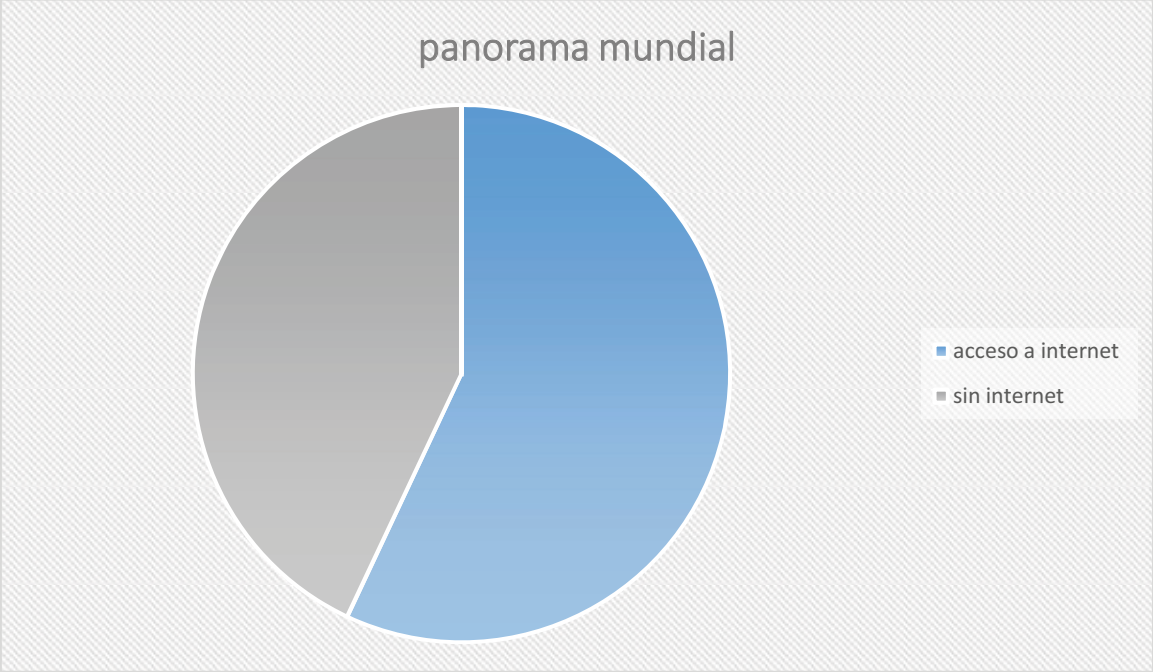
---

[19] *CARBONELL, Óp. Cit. p.20*

[20] *SLAUGHTER, Ana Marie, The chessboard, the web” en línea con dirección URL: http://www.extradigital.es/las-relaciones-internacionales-e-internet-por-mercedes-gracia/ consultado 03-10-2020.*

[21] *Secretaria de Desarrollo Económico, el acceso a Internet como derecho humano, en línea con dirección URL: https://qroo.gob.mx/iqit/el-acceso-internet-un-derecho-*

En la siguiente grafica se busca dar a conocer el panorama mundial sobre el acceso a internet por regiones y como ha ido en aumento en los últimos 5 años, la cual se basa del año 2015 a enero de 2020. Aunque aún no hay otras cifras actuales desde cuando comenzó la pandemia del COVID-19 se puede especular que ha habido un incremento mayor a nivel mundial al acceso de internet por la situación escolar. Por lo que ahora el mundo se encuentra en solo dos brechas: los de acceso a internet y los que no tienen acceso.[22]



Grafica elaborada para mostrar el panorama mundial sobre las personas que tienen acceso a internet y en 2021, a pesar de ser un derecho universal.[23]

Es paradójico pensar que casi la mitad de las personas en el mundo no tengan acceso a este Derecho humano.

El Estado no está garantiza este derecho humano universal porque como lo mencionamos no está obligado por los países a cumplir, también cabe destacar que

---

humano#:~:text=El%20Consejo%20de%20Derechos%20Humanos,de%20todos%20los%20seres%20humanos. 01-03-2021

[22] Op.Cit.

[23] *Secretaria de Desarrollo Económico, el acceso a Internet como derecho humano, en línea con dirección URL: https://qroo.gob.mx/iqit/el-acceso-internet-un-derecho-humano#:~:text=El%20Consejo%20de%20Derechos%20Humanos,de%20todos%20los%20seres%20humanos. 01-03-2021*

la situación por la cual no todos tienen el acceso es por el aspecto económico y la zona geográfica.

1.2.3. Las capas de Internet.

Existen diversas redes que conforman a internet y es importante conocer y entender sus diferencias que tiene cada una de estas redes que se utilizan para navegar ya que nos encontramos en una sociedad vulnerable y en constante evolución ya que por un lado en la sociedad se desarrolla una tendencia compulsiva y acelerada hacia la interconexión, todos somos clientes y productores de noticias en tiempo real y el concepto de verdad está siendo fácilmente inducido, mientras que por el otro lado existe un exceso de información, en otras latitudes hay un control extremo. En estos casos nos damos cuenta que existen aún sistemas de gobierno que coartan a sus ciudadanos de recibir información libremente y les niegan su derecho de pensar y opinar distinto, así como comunicarlo al resto de la humanidad.

A continuación, se abordará la diferenciación de las redes para poder entender cómo opera y que contiene cada una de ellas.

Para poder entender la Deep Web, Dark web y Darknet es necesario conocer primero la Web, o la idea que se tiene de ella, la Internet genérica y universalmente aceptada es denominada “red de redes” la cual crearon con el objetivo principal para comunicar o conectar redes distantes y compartir datos entre equipos terminales, en un principio puros militares y posteriormente con el paso del tiempo para todos los usuarios del planeta.

Surface web

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

La Surface Web es un conjunto de sitios de bases de datos, servicios, mensajería y ecosistemas sociales dispuestos para el acceso y el conocimiento del público en

general, gobiernos, proveedores de servicio, cuerpos de seguridad, sistemas de mercadeo, etc. La información de Surface Web esta soportada sobre Internet, utiliza l infraestructura, sus protocolos y estándares de comunicaciones. Es una red más dentro de la "Red de redes", pero no la única.[24]

Con este nuevo sistema de indexación y el creciente número de computadoras personales entrando en el mercado, las posibilidades de expansión de Internet aumentaban considerablemente. El paradigma del tamaño y costo de las computadoras se rompió y cada individuo podría tener uno en su casa u oficina. "internet esta lista para que todas esas pequeñas fuentes de información se unieran y compartieran sus datos, pero con esta escala de nuevos miembros y ráfagas de información desordenada, comenzó a requerirse algún sistema para poder encontrar la información exacta en el lugar correcto y de esa manera optimizar el uso de la red.

Surgieron nuevas necesidades crearon un nuevo termino, motor de búsqueda. Archie para muchos se instauro como el primer motor de búsqueda en la historia o por lo menos el primero usado masivamente, indexaba archivos descargables vía FTP y guardaba sus vínculos en una base de datos que permitía la consulta para los usuarios interesados. Los primeros motores de búsqueda seguían el principio de buscar palabras clave dentro de los sitios almacenados, guardarlas, clasificarlas de acuerdo a la cantidad de veces que se repetía esta palabra, y ofrecer una interfaz amigable para que el usuario pudiera encontrar lo que deseaba de acuerdo a esos criterios.

Conforme crecía la información en la WWW los motores de búsqueda cobraban mayor relevancia, a mediados de los noventa algunos lograron gran notoriedad como lycos, Altavista, Hispavista, AOL o Excite. Todos en su mayoría con búsquedas similares y con poca diferenciación, exceptuando la cantidad de sitios indexados que manejaban cada uno. En el año de 1996 en la Universidad de Stanford Sergey Brind y Lawrence Page tuvieron la idea de diseñar un motor que exhibiera los resultados de acuerdo a un sistema de jerarquías y rankings, nación en la academia BackRub, semilla del motor que 2 años más tarde se convertiría en Google. Con su llegada, el

[24] S/a Diferencias entre Surface web, Deep web y Dark web, en línea con dirección URL: https://www.a2secure.com/blog/diferencias-entre-surface-web-deep-web-y-dark-web/ consultado 9/03/2021

panorama de los motores de búsqueda cambio drásticamente, pasaron de ser simples indexadores a ser clasificadores y analistas de un sin número de información de todos los usuarios de la WWW y a cobrar por ello.

El desarrollo de los buscadores, las redes sociales fueron ganando espacio, en 194 naciones “Geosites” considerada la primera de su tipo en llegar a un considerable número de usuarios. Con el tiempo fueron llegando sitios como AOL y más famosos como MySpace, muy cercano al concepto de red social actual. Sin embargo, el gran auge definitivo de las redes sociales fue en febrero de 2004 con la publicación the Facebook. Esta red, de 2004 hasta la fecha ha logrado recolectar más de 2 billones de usuarios, y una cantidad inigualable de daos sobre ellos. Con el éxito de Facebook se marcó una tendencia desbordada a la recolección de información que los suscriptores voluntariamente entregan en varias redes. WhatsApp, Instagram, Twitter, LinkedIn, son solo algunos ejemplos.

Deep Web

Los inicios de la Deep web se remontan a la creación misma de ARPANET pero que por motivos de seguridad no aparecían en las listas proporcionadas a todos los nodos, lo cual no permitía su localización y las mantendrá en las “sombras”.

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

Esta red no solo almacena información sensible, secreta o cifrada. Desde el inicio de Internet bases de datos de académicas, bibliotecas de artículos especializados, grupos de lectura, grupos de hacking, activistas o simplemente individuos con interese específicos utilizaron tecnologías diferentes a las de la WWW para alojar y compartir sus contenidos con usuarios determinados, lo que la hace inalcanzable para un usuario común de la Surface Web.

Con el crecimiento exponencial de la WWW se cambió transcendentalmente la forma de concebir las relaciones sociales y el funcionamiento de la sociedad en general. La vida cotidiana se trasladó a un espacio donde los mayores protagonistas del

esquema social debían confluir y la privacidad comenzó a jugar un papel fundamental para los usuarios. Esta nueva concepción de la sociedad mitifico en cierto sentido del papel de la Deep Web, debido a su anonimato, y la rotulo como un espacio criminal de facto, sin advertir las bondades que puede ofrecer para grupos especializados que quieren tener un filtro mayor para sus visitantes.

La red contiene varios niveles que varean según cada autor, sin embargo, abordaré los niveles de López Barbera que nos dice que son 5 niveles y de Albarracín que agrega 3 niveles más y nos da en total nos da 8 diferentes niveles:[25]

Nivel 0	Este nivel representa a la web superficial, donde encontramos a la web común (buscadores tipo Google, Yahoo!…) es decir contenidos indexados.
Nivel 1	Aquí empieza la web profunda, en este nivel se encontraría contenido como bases de datos, información probada, direcciones… Es decir, información que no se encuentra indexada pero que no tiene por qué ser nada de contenido ilegal o ilícito.
Nivel 2	En este nivel ya comienzan las páginas de carácter ilegal como pornografía o resultados de búsqueda bloqueada por otros servidores.
Nivel 3	Para este nivel se requiere el uso de proxy. En este nivel se encuentran temas peligrosos que ya se encuadran dentro del cibercrimen. Desde pornografía infantil, grupos de intercambio de materiales, virus.
Nivel 4	A este nivel también se le conoce como “Chater web” o darknet. Los denominados “onion”. En este nivel hay necesidad de utilizar el navegador Tor. Aquí se encuentra pornografía de cualquier tipo, asesinatos reales, secuestros y torturas, tráfico de órganos, intercambio de divisas, hackers, documentos de Anonymous, tráfico de armas, intercambio de drogas, etc. Conforma el mercado negro más grande que se ha visto hasta la fecha.
Nivel 5	También conocido como “Marianas Web” cuyo nombre deriva de la fosa oceánica de las Marianas, la más profunda conocida. Se dice que es lo más profundo a lo que se puede llegar dentro de la red, el denominado nivel prohibido, donde no se puede confirmar el contenido, pero donde muchos dicen que agencias de inteligencia y gobiernos guardan informaciones secretas.

[25] *Termino Crimipedia: web profunda, darknet y Tor, en línea con dirección URL: https://es.scribd.com/document/429101002/df 08-08-2019.*

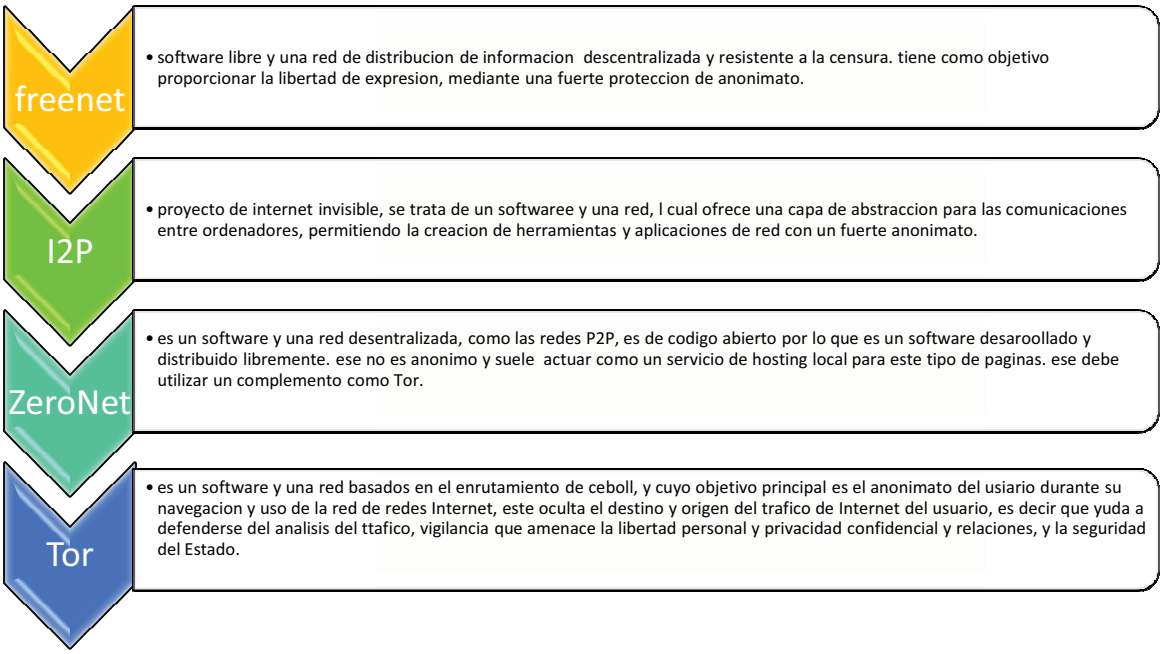
Nivel 6	Conocido como “The fog” (la niebla en castellano). Este nivel los hackers que consiguen entrar utilizan la computación cuántica para poder sobrepasar la encriptación. No existen pruebas concretas de que alguien haya conseguido acceder a él, y el contenido del mismo es cuanto menos confuso.
Nivel 7	También conocido con el sobrenombre de “virus soup” A este nivel solo acceden hackers experimentados que evitan el acceso de los que van en niveles anteriores al mismo.
Nivel 8	El nivel “The Primarch System” si el contenido de los dos niveles anteriores era confuso, en este ya se tratan de puras especulaciones donde se cree que contiene el control primario del mismo internet. Para su acceso se requieren equipos y conocimientos especiales de encriptación.

1.2.4. Diferencias entre Deep Web y Darknet.

La primera vez que se refirieron al término Darknet, fue de la mano de cuatro investigadores de Microsoft en 2002, que lo definieron como:

“Un conjunto de redes y tecnologías utilizadas para compartir contenidos digitales”. Darknet no es una red física independiente, sino una aplicación y capa que funciona en las redes ya existentes, este concepto ha evolucionado mucho. Así de forma errónea, muchos autores tienden a confundir los términos Web profunda (Deep web) y Darknet, ya que para empezar no son sinónimos e intercambiables entre sí. Pero lo cierto es que son términos totalmente diferentes y el hecho de que se traten como uno solo puede crear confusión, especialmente entre usuarios o lectores principiantes en el tema.

Para comenzar a puntualizar la web profunda, es el contenido que se encuentra oculto a la vista y que en realidad no puede ser buscado e indexado con la misma facilidad y fiabilidad que el indexado. La Darknet es tan solo una parte de la Web profunda, en concreto, se trata de aquella parte de la web profunda que recibe su nombre precisamente por el tipo de contenido que se encuentra en ella: pornografía infantil, venta de drogas, venta de armas, sicarios, etc. Por lo que la Darknet solo es un conjunto de contenidos de carácter ilegal o ilícito ubicados de la Web profunda, sin embargo, la Darknet también tiene diversas formas o herramientas de acceder a el:



Cuadro elaborado que muestra las herramientas que se pueden implementar para acceder a la Darknet.[26]

Tor en sus inicios tenía como objetivo primordial en proteger las comulaciones gubernamentales y, por tanto, sus usuarios serian la propia US Navy y el gobierno de Estados Unidos en todo caso, en la actualidad se utiliza para una amplia variedad de propósitos y por personas de diversos perfiles, como militares, profesionales de TI, ejecutivos y jefes de negocio, Activistas y denunciantes, criminales, policía, periodistas, ciudadanos en países con censura, blogueros, gente normal entre otros. Cabe destacar que todos estos medios hayan sido creados con el propósito principal del anonimato y privacidad de los usuarios, muchos de los criminales aprovechan las ventajas que les proporcionan dichos medios para delinquir, debido a la dificultad que supone rastrearos y localizarlos en este tipo de medios, por lo que se dan muchos delitos a través de este, tales como; tráfico de drogas, pedofilia y pornografía infantil, venta ilegal de armas, sicarios, venta de pasaportes falsos y falsificaciones, localización de acoso y extorsión, Terrorismo, hacktivismo, Malware, Piratería,

[26] Cuadro elaborado en base a la información de la siguiente página; https://www.xataka.com/basics/como-entrar-deep-web-guia-2020-para-entrar-tor-zeronet-freenet-e-i2p consultado 30/06/2022

revelación de documentación secreta/ y o confidencial, sin embargo algunos de estos temas serán abordados en el capítulo tres con mayor profundidad.[27]

1.3. La importancia de la Unión Internacional de Telecomunicaciones (UIT) en el ciberespacio.

La Unión Internacional de Telecomunicaciones (UIT) es la organización más importante de las Naciones Unidas en lo que concierne a las cuestiones relativas a la tecnología de información y la comunicación y a la coordinación entre los gobiernos y el sector privado para el desarrollo de redes y servicios. Su principal función es la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación, con la finalidad de crear también medidas concretas para vencer las amenazas e incertidumbres, relacionadas con el ciberespacio.

La creación fue en 1865 para promover la cooperación entre las redes telegráficas internacionales del momento, la UIT asimila a otros muchos organismos de normalización, tales como la normalización del uso del código Morse y las primeras redes de radiocomunicaciones y telecomunicaciones fijas.[28]

La importancia de la UIT en el ciberespacio y el mundo se debe porque desarrolla estándares que facilitan la interconexión eficaz de las infraestructuras de comunicación nacionales con las redes globales, permitiendo un perfecto intercambio de información, ya sean datos, faxes o simples llamadas de teléfono desde cualquier país;

Trabaja para integrar nuevas tecnologías en la red de telecomunicaciones global, para fomentar el desarrollo de nuevas aplicaciones tales como Internet, el correo y los servicios multimedia; también gestiona el reparto del espectro de frecuencias radioeléctricas y de las orbitas de los satélites recursos naturales limitados utilizados por una amplia gama de equipos incluidos los celulares, las radios y televisiones, los sistemas de comunicación por satélite, los sistemas de seguridad por navegación aérea y marítima, así como los sistemas informáticos sin cable, por lo que se

---

[27] *Diferencias entre Darknet y Deep web, en línea con dirección URL: https://www.xataka.com/basics/que-dark-web-que-se-diferencia-deep-web-como-puedes-navegar-ella . Consultado 19-10-2019*

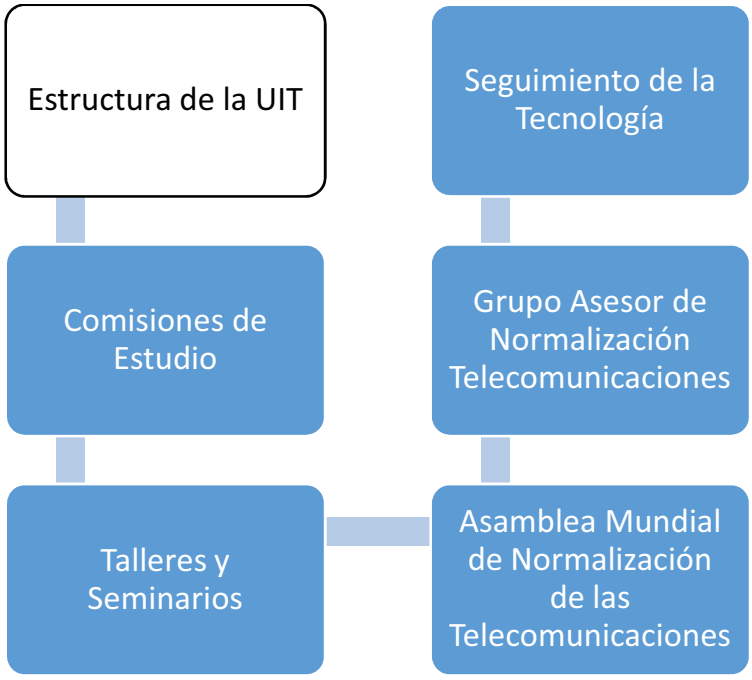
[28] *Sobre la Unión Internacional de Telecomunicaciones en línea con dirección URL: https://www.itu.int/es/about/Pages/default.aspx consultado 04/01/19*

esfuerza por mejorar la accesibilidad a las telecomunicaciones en el mundo en desarrollo a través del asesoramiento, la asistencia técnica etc.[29]

Cabe destacar que la UIT está integrada por 193 países miembros, así como de 900 empresas, universidades y organizaciones internacionales regionales.

La UIT ha logrado grandes avances y una importante de ellas es que tiene su propia constitucion integrada de nueve capitulos y 58 articulos los cuales tiene una diversa clasificacion para el tratamiento por ejemplo en su estructura establece en los articulos sus principales funciones asi como de la regulacion de otros temas como el secreto de las telecomunicaciones que se encuentra en el articulo 37.

A continuación se muestra la estructura de la UIT:



Cuadro elaborado de manera general que muestra la estructura de la UIT, información basada en la página que se muestra a pie de página.[30]

1.4. Evolución de la Gobernanza del Ciberespacio.

La gobernanza del ciberespacio es definida por Kapellman como; “un entorno virtual público a través de la cual se transmite información y se generan tejidos tecnológico-

[29] *La importancia de la Unión Internacional de Telecomunicaciones en línea con dirección URL: https://www.itu.int/es/about/Pages/default.aspx consultado 20-11-2019*

[30] [30] *Estructura de la UIT en línea con dirección URL https://www.itu.int/es/about/Pages/default.aspx consultado 10-01-2021.*

sociales, principalmente facilitados por la adopción de una red de redes popularmente denominada internet".[31]

En los primeros intentos que se realizaron para gobernar[32] al ciberespacio se remontan a las entrañas de los laboratorios y universidades que dieron luz al mismo. Como ya bien se sabe internet es una red de redes que opera en distintas capas de por medio de protocolos que determinan como se transmite la información de un punto a otro. En esta labor, organizaciones de seguridad e investigación en Estados Unidos tales como; (DARPA y NSF) en conjunto con otras especializadas (IETF, ICANN Y WWW, entre otras) fueron actores clave para determinar el rumbo descentralizado de la red; su objetivo era que ningún gobierno u organización privada pudiera monopolizar el control de la información de usuarios.[33]

Sin embargo, el papel de estas organizaciones se limitó a los aspectos técnicos de la regulación: los protocolos de envío de datos y la repartición de dominios, entre otras cosas. Con el paso de los años, la importancia de esta tecnología y su adopción en la incrementación drásticamente, incorporando a otros actores públicos y privados en la toma de decisiones. En este contexto, la enorme capacidad del internet como herramienta para estimular el crecimiento económico atrajo la atención de Naciones Unidas (ONU), incorporado por primera vez en el tema por la vía de la agenda del desarrollo.[34]

En el marco de la ONU y a raíz del planteamiento de los Objetivos del Milenio (firmados por 198 países) en el año 2000 se propuso por primera vez incorporar el acceso de las TIC, y en particular a la red, como un imperativo primordial para impulsar el desarrollo a nivel mundial. Tomando en cuenta la creciente demanda tecnológica y la brecha generada por la falta de acceso a estas tecnologías, se determinó necesario cooperar con el sector privado para generar una derrama de beneficios entre la población de modo equitativo. En el 2002 esta visión fue incorporada durante la Cumbre de Monterrey la cual se derivó de la Conferencia

[31] Solis Tourné Marco, Lo que debes saber sobre "la gobernanza del ciberespacio" en la economía digital, en línea con dirección URL: https://ibero909.fm/blog/la-gobernanza-del-ciberespacio consultado 16/01/2023

[32] Termino conocido como la acción de ejercer la dirección, el control de un Estado, ciudad, país, colectividad y en este caso al ciberespacio.

[33] *KAPELMAN, Daniel, México y el multilateralismo La gobernanza del Ciberespacio y la incipiente participación de México, la SRE, 2006.*

[34] *KAPELLMANN, OP. Cit.*

Internacional sobre Financiación para el desarrollo y el Plan de Johannesburgo sobre el Desarrollo Sostenible, incluyendo entre sus contenidos la necesidad de adoptar las TIC para optimizar labores en el sector privado si como en la provisión de servicios gubernamentales.

Todo lo anterior dio como resultado bases para convocar la primera Cumbre Mundial de la Sociedad de la Información (CMSI), la cual constituyo el primer foro multilateral especializado en el mundo digital. Dicha Cumbre fue promovida por la Unión Internacional de Telecomunicaciones (UIT), organismo especializado de la ONU se llevó a cabo en Ginebra en 2003. Su objetivo inicial fue coordinar a la comunidad internacional para disminuir la brecha digital y establecer lineamientos básicos para facilitar el desarrollo de la sociedad civil en el ámbito local, nacional, regional y global.

Aquí cabe destacar que se sentaron bases para la formulación de planes o estrategias digitales especializadas, entre las cuales destacan la Estrategia Digital para Europa 2020, eLAC 2015 en América Latina y la Estrategia Digital Nacional en México 2013-2018. Además, se creó el concepto de gobernanza de internet y se creó un Grupo de Trabajo para avanzar en esta materia.

La segunda CMSI se llevó a cabo en Túnez en 2005. Se invitó nuevamente a los participantes a profundizar en diversos aspectos como desarrollar una definición sobre la gobernanza[35] de internet en Atenas a finales de 2006, siendo este el primer espacio multilateral para dialogar sobre la gobernabilidad y la regulación del ciberespacio.

Se convocó por primera vez por el secretario general de la ONU, este foro nació con un mandato por cinco años, de 2006 a 2010. Su importancia quedo estipulada en la Resolución de la Asamblea General del 22 de diciembre de 2011, en donde se destacó su papel para reforzar la cooperación en cuestiones de políticas públicas relativas al internet, además de que se invitó a promover la participación de países en desarrollo y otros interesados. En 2010 el mandato fue prorrogado hasta 2015.[36]

[35] Este término se ha empleado desde 1990, para designar la eficacia, calidad y orientación de la intervención del Estado, es decir, es una nueva forma de gobernar, en la era de la globalización.
[36] *KAPELLMANN, OP. Cit.*

Es importante señalar que todas las iniciativas llevadas a cabo para la regulación del ciberespacio han sucedido con el apoyo de la Unión Internacional de Telecomunicaciones, organismos especializados de Naciones Unidas para las TIC. Entre los principales objetivos de esta institución se encuentran promover la conectividad global y organizar la colaboración a nivel internacional para promover una red segura y accesible. El rasgo más característico de esta institución, y la razón por la cual es única en su tipo dentro de la ONU, es que se basa en una asociación público-privada y se encuentra conformada no solo por 193 países sino también por más de 700 instituciones privadas y académicas.

El secretario general de la UIT establece 5 principios para el ciberespacio, los cuales comprenden valores esenciales y establecen acciones y obligaciones específicas que garantizaran la paz y estabilidad en el ciberespacio:[37]

1. Los gobiernos deben comprometerse a dar acceso a todos los ciudadanos a las comunicaciones.
2. Los gobiernos deben comprometerse a proteger a sus ciudadanos en el ciberespacio.
3. Los países deben comprometerse a no dar refugio a terroristas / delincuentes en su territorio.
4. Los países deben comprometerse a no lanzar el primer ataque cibernético contra otros países.
5. Los países deben comprometerse a colaborar en un marco de cooperación internacional para garantizar la paz en el ciberespacio.

También existe una Declaración de Erice sobre de principios de Estabilidad y Paz Cibernéticas[38] escritas con la finalidad de preservar y proteger la vida humana ya que el internet y las demás redes interconectadas que conforman al ciberespacio se ha vuelto indispensables para la humanidad, la independencia política y la integridad territorial de los países.

---

[37] I. *Touré Hamadoun, La Búsqueda de la Paz en el Ciberespacio, Unión Internacional de Telecomunicaciones en línea con dirección URL: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-S.pdf consultado 04/11/19.*

[38] *Fue redactada por el Panel Permanente de supervisión de la seguridad de la información de la Federación Mundial de Científicos (WFS), Ginebra y adoptada por el Pleno de la WFS con ocasión de la 42º reunión de los Seminarios Internacionales sobre Emergencias Planetarias en Erice (Sicilia) el 20 de agosto de 2009.*

El peligro radica en que el mundo está demasiado interconectado y los riesgos y amenazas son tan sofisticados y omnipresentes que han crecido exponencialmente en comparación con la capacidad de contrarrestarlos. Los países y, también los delincuentes, disponen ahora de la capacidad para perturbar considerablemente la vida y la sociedad de todos los países; la ciberdelincuencia y su vástago, el ciberconflicto, amenazan la paz de la humanidad y la utilización beneficiosa del ciberespacio.

Los sistemas e infraestructuras de la información se están volviendo indispensables para la salud, la seguridad y el bienestar de las personas y, específicamente los ancianos, discapacitados, enfermos y muy jóvenes. Las grandes perturbaciones del ciberespacio pueden causar sufrimientos y destrucciones innecesarios.

Valores y principios que propone la UIT para mantener la paz cibernética.

Por lo anterior, la UIT recomienda los siguientes principios para lograr y mantener la estabilidad y la paz cibernética:

1. Todos los gobiernos deberían reconocer que la legislación internacional garantiza la libre circulación de información e ideas; esas garantías también se aplican al ciberespacio. Solo se deberían aplicar restricciones en caso de necesidad, y estas deberían ir acompañadas de un proceso legislativo.
2. Todos los países deberían colaborar para elaborar un código común de conducta y un marco legislativo mundial armonizado que comprendiera disposiciones de procedimiento relativas a la asistencia y cooperación en las investigaciones que respeten la privacidad y los derechos humanos. Todos los gobiernos proveedores de servicios y usuarios deberían apoyar los esfuerzos de aplicación de la legislación internacional contra los ciberdelincuentes
3. Todos los usuarios, proveedores de servicios y gobiernos deberían colaborar para velar por que la utilización del ciberespacio no entrañe la explotación de los usuarios, en particular los jóvenes y las personas sin defensa, por medios violentos o degradantes.
4. Los gobiernos como las organizaciones del sector privado, incluidas las personas físicas, deben de aplicar y mantener programas de seguridad

integrales basados en prácticas idóneas y normas universalmente aceptadas que recurran a tecnologías de privacidad y seguridad.

5. Los desarrolladores sean de programación y equipos informáticos deberían tratar de desarrollar tecnologías seguras que promuevan la capacidad de recuperación y resistan a las vulnerabilidades.
6. Los gobiernos deberán participar activamente en los esfuerzos de las Naciones Unidas encaminados a promover la seguridad y la paz cibernética mundiales y evitar la utilización del ciberespacio para fines bélicos.

1.5. El ciberespacio como lugar y la llamada ciberanarquia.

Reflejada en textos simbólicos como la llamada declaración de Independencia del Ciberespacio, la concepción social que se da en llamar "ciberlibertaria" fue cronológicamente la primera en afrontar el problema de la regulación legal de internet. Conforme a sus postulados sería diferente del aquí, razón por la cual debía disfrutar de cierta autonomía frente a los poderes políticos del mundo físico. Se considera que el ciberespacio como lugar es una metáfora, ya que se ha encontrado en pleno eco en nuestro sistema cognitivo, que continuamente que recurre a vocablos e ideas relacionados con el espacio físico a efectos de parangonarlos con los propios de internet, incluso varios autores han propuesto un autogobierno siendo el único derecho que puedan dar autorregulación.

El ciberespacio: ¿anarquía libertaria o libertad garantizada?

Como la mayoría de las grandes conquistas científicas y tecnológicas que registra la historia, Internet es una realidad ambivalente. Renunciar a sus logros seria hoy una pretensión imposible, porque se trata de un avance imprescindible y un signo del progreso de nuestro tiempo. Sin embargo, ello no debe conducir a aceptar pasivamente o a claudicar ante los riesgos de abordaje criminal que avanza la navegación por el ciberespacio, ni ante la colonización de la Red por parte de los controles estatales que limitan injustificadamente la libertad.[39]

[39] *PEREZ, Luño Antonio Enrique, Internet y los Derechos Humanos, Facultad de Derecho, Universidad del Huelva, pp. 101-121.*

En sus inicios uno de los mayores alicientes de internet residía en su carácter ácrata, se trataba de un espacio absolutamente libre, sin ningún tipo de autoridad o poder que regulara o acotara. Como ejemplo de esa concepción anárquica y libertaria de Internet puede citarse la Declaración de Independencia del Ciberespacio "promulgada" por John Perry Barlow en Davos, Suiza, el 8 de febrero de 1996, las cuales articula tres ideas guía:[40]

1) La afirmación de la total autonomía de los cibernautas respecto a cualquier tipo de autoridad estatal: Gobiernos del Mundo Industrial. No son bienvenidos no tienen ninguna supremacía donde nos juntamos. El Ciberespacio esta fuera de sus fronteras.
2) Negación de los conceptos y categorías jurídicas tradicionales "nuestros conceptos legales de propiedad expresión, identidad, movimiento y contenido no se aplican a nosotros. Aquellos se basan en la materia, peri en nuestro mundo la materia no existe.
3) Confianza utópica en un ciberespacio ideal: "Crearemos una civilización de la Mente en el ciberespacio". Que sea más humana y justa que el mundo creado anteriormente por sus gobiernos. Internet ha abierto nuevas y preocupantes posibilidades operativas a los sistemas de control social y político. El utopismo ácrata se opone a cualquier regulación del Ciberespacio por entender que con ello se reprime la libertad de los cibernautas, a la vez que se refuerza el poder estatal, pero la realidad no es tan simple. Paradójicamente los grandes beneficiarios de la anarquía de Internet no solo los cibernautas particulares, sino los grandes beneficiarios de la anarquía de Internet no son los cibernautas particulares, sino las grandes multinacionales e, incluso los aparatos de control social de los gobiernos. En los últimos años, se están transmitiendo por Internet, sin ningún tipo de garantías y con evidente menoscabo del derecho a la intimidad, datos personales (incluso voz e imagen) en investigaciones policiales; a través de un medio que por su naturaleza y características es accesible a millones de usuarios de todo el mundo. Los peligros de una utilización abusiva, incontrolada o criminal de ese

[40] *PEREZ, Óp. Cit.*

> espacio plantean ahora, de forma apremiante, la necesidad de su ordenación.[41]

Se asegura que el ciberespacio es un espacio virtual, el cual puedes crear, hacer deshacer, investigar, comunicarte con otras personas desde cualquier parte del mundo, sin importar la hora, el lugar y la situación, por eso se dice que el ciberespacio es lugar libre sin reglas, sin embargo, si existen reglas pero por país, lo que dificulta que cuando para un país es calificado como delito o algo no permitido para otros países no lo es y por ende se desencadena una serie de acontecimientos tales como: choque de culturas, delitos; fraudes financieros, atentados contra empresas, personas u organizaciones, entre otros pero se abordarán a detalle en el capítulo tercero de este trabajo.

1.6. Modelo *multi-stalkeholder* de gobernanza.

La gobernanza de internet ha impulsado a grandes innovaciones en el mundo de la diplomacia multilateral: en particular, la adopción de lo que se reconoce como modelo de gobernanza multi-stakeholder[42], la cual promueve la participación de diversos actores en las discusiones internacionales acerca de la gobernanza de internet, es una invitación a involucrarse a los estados y gobiernos especialistas, miembros del sector privado y organizaciones de la sociedad civil en la gobernanza compartida a nivel local, nacional y global. Gracias a todos estos acontecimientos en la Cumbre Mundial de la Sociedad de la Información que tuvo lugar entre 2003 y 2005 dio origen a la creación del foro de gobernanza de Internet; el cual se ha convertido en un foro anual de debate en el que organismos internacionales, gobiernos, profesionales de internet, empresas y organizaciones de la sociedad civil pueden explorar, en igualdad de condiciones, el desarrollo de internet y su interacción con otros ámbitos del poder público.

Este foro fue convocado en 2006 por el secretario general de Naciones Unidas, posteriormente hubo una renovación de su mandato por parte de la Asamblea General de las Naciones Unidas en diciembre de 2015, el IGF se ha consolidado

[41] *PEREZ, Óp. Cit.*
[42] *El modelo de multi-stakeholder, se conoce como "modelo de múltiples partes interesadas".*

como una plataforma para reunir a los miembros de los diversos grupos de partes interesadas como iguales. Si bien no hay un resultado negociado, el IGF informa e inspira a aquellos con poderes de formulación de políticas tanto en el sector público como en el privado. Los delegados sostienen discusiones, intercambian información y comparten buenas prácticas entre ellos en la reunión anual.[43]

El IGF facilita una comprensión común sobre cómo se pueden maximizar las oportunidades de Internet y aborda los riesgos y desafíos que surgen. Es un foro que ofrece a los países en desarrollo la misma oportunidad que las naciones más ricas para participar en el debate sobre la gobernanza de Internet y facilita su participación en las instituciones y los arreglos existentes. En última instancia, la participación de todos los interesados, tanto de los países desarrollados como de los países en desarrollo, es necesaria para el futuro desarrollo de Internet.[44]

1.7. Retos y amenazas del ciberespacio.

No es este un lugar para una consideración detenida en pormenores sobre las múltiples implicaciones económicas, culturales, sociales y políticas que se derivan de ese ciberespacio cuya navegación y conquista ha hecho posible Internet. Las consecuencias que pueden derivarse de esa forma de comunicación en soporte informático son imprescindibles y a veces paradójicas. Puede darse la circunstancia de que el máximo desarrollo de la comunicación tecnológica implique simultáneamente un empobrecimiento de las formas de comunicación tecnológica a las formas de comunicación tradicionales. Suele aducirse, para corroborar esos riesgos, la anécdota de un foro de cibernautas que concentraron un encuentro personal para reforzar sus contactos iniciados a través de Internet el cual fue un fracaso.

En cuanto a una renovación de los valores cívicos que se puede promover en Internet, tenemos el caso del área francófona se ha utilizado la expresión “Netiquette”, es decir “ética de la Net, para aludir a las reglas deontológicas que

---

[43] *Internet Society, Foro de Gobernanza de Internet, en línea con dirección URL: https://www.internetsociety.org/es/events/igf/2017/ (consultado 20 de enero de 2019)*

[44] *Internet Society, Foro de Gobernanza de Internet, en línea con dirección URL: https://www.internetsociety.org/es/events/igf/2017/ consultado 20 de enero de 2019*

deben presidir la utilización de Internet. Se trata de normas o programas éticos dirigidos a evitar las conductas perturbadoras realizadas por los cibernautas y para prevenir cualquier actividad que perjudique el normal funcionamiento de la red.

Se presentan dificultades para la regulación del ciberespacio es la cantidad inimaginable de datos que son transferidos de modo veloz y continuo a través de la red por millones de usuarios y organizaciones. De acuerdo con la consultora IDC, entre 2013 y 2020 la cantidad de información que generamos se duplicara cada dos años alcanzando un total de 44 zettabytes (es decir un trillón de gigabytes). Esto incluye todo tipo de contenidos que van desde fotografías personales y mensajes entre amigos, hasta videos famosos, programas empresariales, aplicaciones gubernamentales, juegos, software malicioso, películas con o sin derechos de autor, música legal e ilegal, etc. Sin embargo, esta representa por un lado una ventaja en términos de libertad de expresión en la red, pero esto a su vez provoca problemas en la red, las cuales resultan difícil discernir entre aquella información que es lícita e ilícita, privada y pública. Este tema es complicado debido a que la red es un espacio abierto a cualquier individuo, empresa u organización o país se puede programar nuevas funciones, generar contenidos, innovar y compartir lo que guste sin restricción alguna, por lo que resulta el monitoreo o control de todos los datos que pasan por la red no solo es complejo, sino que desencadena severos daños para las libertades y derechos de los usuarios.[45]

Es urgente la creación de estructuras públicas y privadas, puesto que los operadores de servicios suelen no solo brindar cobertura, sino también ser dueños de la infraestructura que permite la conexión de internet. Es por ello que se ha vuelto necesaria la regulación multi-stakeholder como un posible mecanismo para promover la cooperación entre los encargados de manejar cada una de las capas que forman internet, dando origen a la libertad de la red, como ya mencionamos anteriormente las ventajas y objetivos de la creación de IFG.[46]

Otro factor que impide la regulación de internet es la geografía del ciberespacio, debido a que dificulta la identificación de un individuo u organización que realiza un ataque, accede a información privada, descarga o comparte contenidos ilícitos. En

[45] *KAPELLMAN, OP. Cit.*
[46] *KAPELLMAN, OP. Cit.*

línea, criminales, terroristas, activistas, usuarios, empresas, hackers, civiles y demás operan en un esquema de horizontalidad bajo el anonimato que les provee de nuevas herramientas digitales. Cabe resaltar que el tipo de armas y herramientas que se utilizan en el ciberespacio son radicalmente diferentes de aquellas utilizadas en el ámbito físico, las cuales permiten el anonimato del usuario o atacante, generan resultados impredecibles y pueden realizarse ya sea de modo inmediato o gradual (un virus para robo de información o daño a sistemas puede mantenerse escondido durante un largo periodo de tiempo u operar gradualmente). Por ellos rastrear a la persona detrás de una pantalla suele ser complicado e impreciso, requiriendo mucho tiempo y recursos, e incrementando los costos de implementar estrategias defensivas en comparación con los gastos necesarios para cometer actos ilícitos.[47]

Hacia una ética jurídica ciberespacial.

No es este lugar para una consideración detenida en pormenores sobre las múltiples implicaciones económicas, culturales, sociales y políticas que se derivan de ese ciberespacio cuya navegación y conquista ha hecho posible internet. Las consecuencias que pueden derivarse de esa forma de comunicación humana en soporte informático son imprevisibles y, a veces paradójicas. Puede darse la circunstancia de que el máximo desarrollo de la comunicación tradicionales. Suele aludirse, para corroborar esos riesgos, la anécdota de un foro de “cibernautas” que concentraron un encuentro personal para reforzar sus contactos iniciados de internet. La reunión fue un completo fracaso por las dificultades para establecer un dialogo interpersonal; la comunicación sol se hizo de nuevo fluida cuando cada uno de los cibernautas que concentraron un encuentro personal para reforzar sus contactos iniciados a través de internet. La comunicación solo se hizo de nuevo fluida cuando cada uno de los cibernautas la reemprendió desde su pantalla de ordenador.

Cabe resaltar que hay que reconocer la variedad de valores cívicos que se pueden promover a través de internet y a su vez una renovación de dichos valores cívicos, por ejemplo, en el área francófona se ha utilizado la expresión “Netiquette”, es decir, “ética” de la Net (red) para aludir a las reglas deontológicas que deben presidir la

[47] *KAPELLMAN, OP. Cit.*

utilización de internet. Se trata de normas o programas éticos dirigidos a evitar las conductas perturbadoras realizadas por los cibernautas y para prevenir cualquier actividad que perjudique el normal funcionamiento de la Red.[48]

Sin embargo, los principios que resultan necesarios para abordar los problemas éticos planteados por internet se basan en gran medida en principios individuales y sociales. Se describen los principios individuales, sociales y globales necesarios. En virtud de dichos principios, se discuten los problemas individuales de índoles ética relacionadas con el sexo en internet y la "piratería". Los problemas sociales de carácter ético contemplados son la brecha digital y los impuestos sobre las ventas realizadas a través de internet. También hay cuestiones de carácter mundial relacionadas con el uso de internet analizadas son la libertad de expresión en internet, la regulación de los sitios web con presencia global y la contribución de internet a la globalización, pero se explicará a fondo en el capítulo tercero.[49]

Se busca que la sociedad se organice de tal manera que todos los miembros disfruten de la mayor igualdad de libertades posibles, incluida la justa igualdad de oportunidades, junto a las libertades básicas como la libertad de expresión, de reunión, de religión, etc. Se incluye la libertad de oportunidades. Así las normas de la sociedad no están predispuestas contra nadie y permiten que todos los miembros de una sociedad puedan perseguir sus intereses y desarrollar sus capacidades.[50]

El ciberespacio es un espacio enorme intangible, el cual está conformado por diferentes campos, y una de ellas es Internet, el cual ha ido creciendo de tal manera que se han creado puntos positivos y negativos, sin embargo en este trabajo de investigación abordaremos los puntos negativos que son de suma importancia para las relaciones internacionales ya que un internacionalista se encarga de estudiar los procesos históricos el cual busca crear paz, regular y dar una respuesta sobre dichos procesos o acontecimientos.

Otro punto crucial para las relaciones internacionales y para el mundo en general es la importancia del Derecho Internacional de los Derechos Humanos, las aportaciones

---

[48] *PÉREZ Luño Antonio Enrique, Internet y los Derechos Humanos, Derecho y conocimiento, vol. 2, págs. 101-121, Facultad de Derecho, Universidad de Huelva*.

[49] *S/A, Ética y Ciberespacio en línea con dirección URL: https://www.bbvaopenmind.com/articulos/etica-e-internet/ consultado 07/11/19.*

[50] *S/a, Ética y Ciberespacio en línea con dirección URL: https://www.bbvaopenmind.com/articulos/etica-e-internet/ consultado 07/11/19*

que ha dado para el tema del cibercrimen internacional además del tratamiento internacional que se ha dado para todo ser humano, a través de sus diversas etapas, pero este tema se abordara en el siguiente capítulo.

El panorama presentado sobre el ciberespacio hace un llamamiento a toda la comunidad internacional interesada en erradicar la problemática en el ciberespacio que cada día se convierte en un problema severo debido a que cada vez en más difícil poder encontrar a la persona que se encuentra delinquiendo desde cualquier parte del mundo gracias a la ayuda de internet que se ha vuelto el lugar perfecto para cometer el crimen y es difícil de encontrar al culpable y pocas veces se la captura y se juzga.

Capítulo 2. Evolución y critica de los derechos humanos en las relaciones internacionales.

"hablar de Derechos Humanos es referirse a un mensaje de alegría, de optimismo y esperanza. Es creer en la posibilidad de un mundo en donde las sonrisas infantiles sean el sol de cada día."

Sagastume Gremmell Marco Antonio

2.1. Definición de los Derechos Humanos.

Los derechos humanos son derechos que tiene toda persona en virtud de su dignidad humana, son aquellos derechos universales, colectivos y múltiples, ya que comprende a los derechos civiles, políticos y económicos, sociales y culturales por ello son indispensables e inalienables, que resultan atribuidos directamente por las normas jurídicas a todos en cuanto personas, ciudadanos o capaces de obrar.[51]

De acuerdo con Naciones Unidas define a los Derechos humanos como; "derechos inherentes a todos los seres humanos, sin distinción alguna de nacionalidad, lugar de residencia, sexo, origen nacional o étnico, color, religión, lengua, o cualquier otra condición. Todos tenemos los mismos derechos humanos, sin discriminación alguna. Estos derechos son interrelacionados, interdependientes e indivisibles.[52]

En ingles existen dos palabras para referirse al derecho: right y law. En español se conocen como derecho objetivo y como derecho subjetivo. El primero se refiere a las normas jurídicas que tienen el respaldo coactivo del Estado: los códigos, las leyes, las constituciones, los reglamentos, etc.[53]. El segundo son las expectativas de acción y omisión de los Estados, las empresas, los poderes facticos, y del resto de las personas respecto a ciertos bienes primarios constitutivos de lo que se considera la dignidad humana.[54]

---

[51] *Oficina del Alto Comisionado de Naciones Unida, Manual para Parlamentarios N 26 en línea con dirección URL: https://www.refworld.org.es/pdfid/5b72fb824.pdf 07-09-2020*

[52] *Naciones Unidas, Derechos Humanos, Oficina del Alto Comisionado, en línea con direcciónURL:https://www.hchr.org.mx/index.php?option=com_content&view=article&id=448&Itemid=249 consultado 07-10-2020.*

[53] *Para mayor información y profundidad del tema se encuentra en Wesley N. Hohfield, Robert Alex y, o Liborio Hierro, 133-173.*

[54] *Curso IV Fundamentos teóricos de los derechos humanos. Características y principio, en línea con dirección URL: https://cdhcm.org.mx/serv_prof/pdf/fundamentosteoricosdelosderechos.pdf consultado 20-11-19*

Luigi Ferrajoli considera al derecho subjetivo como “toda expectativa jurídica positiva (prestación) o negativa (de no lesión)”. Es una expectativa que se forma una persona con respeto a la acción u omisión de otra esta concepción inicial nos lleva a dos conceptos de nivel básico del derecho: derecho y deber. Los derechos humanos son derechos subjetivos. Son expectativas en todas las personas en relación con la acción u omisión de los Estados, las empresas, los poderes facticos y del resto de las personas respecto a ciertos bienes primarios constitutivos de lo que se considera la dignidad humana.

Existen muchos derechos subjetivos, pero no todos ellos califican como derechos humanos o derechos fundamentales, los cuales son aquellos derechos universales y, por ello, indispensables e inalienables que resultan atribuidos directamente por las normas jurídicas a todos en cuanto a personas ciudadanos o capaces de obrar. A partir de todo lo antes mencionado como punto de partida que los derechos humanos son exigencias éticas justificadas, especialmente importantes, que deben ser protegidas eficazmente a través del aparato jurídico. [55]

Los derechos humanos son inherentes a la naturaleza humana, sin ellos no se puede vivir como ser humano. Pueden ser definidos como el conjunto de derechos por los cuales se afirma la de la persona frente al Estado; en otras palabras, son derechos públicos subjetivos que tienen como correlativa obligación las limitaciones, obligaciones o prestaciones que ha de observar el Estado en favor del individuo.[56]

En su aspecto positivo, son aquellos derechos reconocidos por el sistema jurídico de que se trate. Como es el caso de México, en el que serían los que se establecen en la Constitución Política de los Estados Unidos Mexicanos, además de los que se recogen en los pactos, convenciones y tratados internacionales suscritos y ratificados por el gobierno mexicano.[57]

Al respecto, Enrique Pérez Luño expresa que los derechos humanos son:

“Un conjunto de facultades e instituciones que, en cada momento histórico, concretan las exigencias de la dignidad, la libertad y la igualdad humanas, las cuales

---

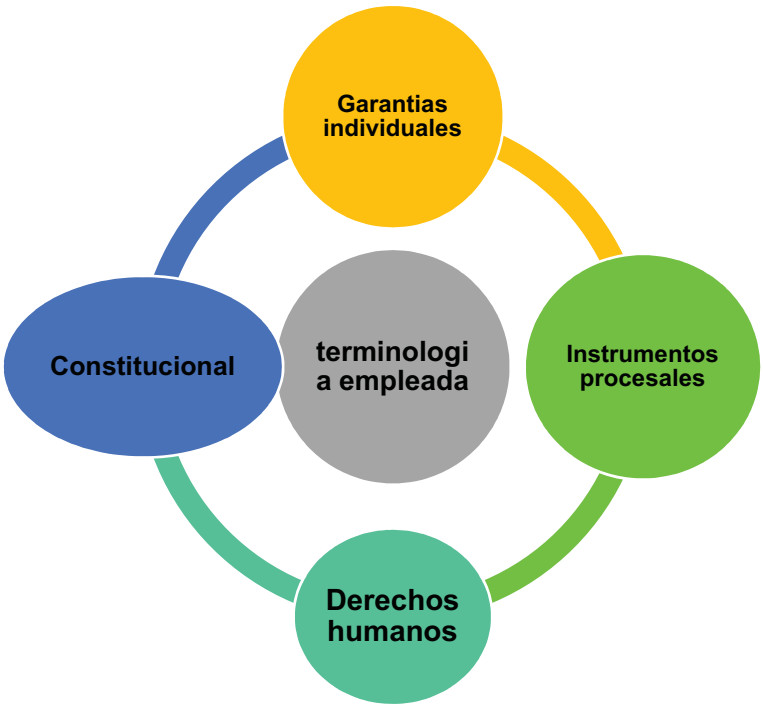
[55] *Curso IV Fundamentos Teóricos de los derechos humanos. Características y principios, Op. Cit.*

[56] *Op. cit https://cdhcm.org.mx/serv_prof/pdf/fundamentosteoricosdelosderechos.pdf consultado 20-11-19*

[57] *Op. Cit.*

deben ser reconocidas positivamente por los ordenamientos jurídicos a nivel nacional e internacional; y los derechos fundamentales son aquellos derechos humanos garantizados por el ordenamiento jurídico positivo, en la mayor parte de los caos en su normatividad constitucional y que suele gozar de una tutela reforzada".[58]

En cuanto a Margarita Herrera Ortiz nos define a los Derechos Humanos: "el conjunto de filosofías sociales, políticas, económicas, culturales, religiosas, aspiraciones éticas, de justicia, de seguridad, de equidad, juicios de valor, etc. que se encuentran consagrados en la Constitución Federal, y en los tratados, convenios, convenciones, etc., internacionales que México ha incorporado a su derecho interno. Conforme al artículo 133 constitucional, con que cuentan los gobernados, para vivir y convivir con la dignidad que les corresponde como seres humanos, por lo que su disfrute se encuentra debidamente garantizado contra las violaciones de autoridades estatales por el juicio de amparo, así como por diversos instrumentos procesales constitucionales".[59]



[58] *PÉREZ Luño Antonio Enrique, Derechos Humanos, Estado de Derecho y Constitución 7ª ed., Madrid, Tecnos, 2001, p. 48.*
[59] *HERRERA Ortiz, Margarita, Manual de Derechos Humanos 4ª ed., México, Porrúa, 2003, p.23.*

Cuadro de elaboración propia para mostrar de manera dinámica la terminología empleada sobre sus derechos humanos y sus jerarquías.[60]

La Comisión Nacional de los Derechos Humanos de México define a los Derechos Humanos como el conjunto de prerrogativas sustentadas en la dignidad humana, cuya realización efectiva resulta indispensable para el desarrollo integral de la persona. Este conjunto de prerrogativas se encuentra establecido dentro del orden jurídico nacional, en nuestra Constitución Política, tratados internacionales y las leyes.

El respeto hacia los derechos humanos de cada persona es un deber de todos. Todas las autoridades en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos consignados en favor del individuo.

2.2. Naturaleza de los derechos humanos.

La historia de los derechos humanos está muy relacionada con la del liberalismo, aunque no son la misma historia. Desde la teoría política liberal, el viejo régimen, la monarquía absoluta llego a su fin a partir de un concepto básico: la libertad a partir de la propiedad de uno mismo, soy dueño de mi cuerpo y de los productos obtenidos por mi cuerpo, el rey no es más mi soberano.[61]

En el liberalismo existen cuatro conceptos básicos para entender este proceso de reconstrucción de la legitimidad política : la libertad como autodeterminación, la celebración de un contrato social política; la existencia de derechos naturales inherentes a todas las personas y previas a la celebración de ese contrato y finalmente, el derecho a la resistencia cuando el contrato era roto por el gobernante cuando había violaciones sistemáticas a los derechos naturales reconocidos y protegidos en el contrato , lo que nos lleva de nuevo a un estado de naturaleza. A partir de esta lógica es que los derechos humanos se concebían como derechos naturales, aunque su enumeración variaba dependiendo de quién hiciera la tipología. Por ejemplo para Hobbes, el principal y único derecho natural es la vida por eso la

[60] *MATIAS Leon Cinthya Mariana, Elaboración del cuadro propio, para ejemplificar la principal terminología sobre los Derechos Humanos y las ideas de diversos autores, 11-06-19.*

[61] *Esta concatenación es la idea básica que recupera Robert Nozick para pensar la teoría de la justicia que sostiene la lógica del mercado a partir de lo que David Gauthier denomina moral por acuerdo.*

forma de gobierno que el diseña es una monarquía cuasi-absoluta, para Locke es la vida la libertad y la propiedad de ahí que el tipo de gobierno más pertinente sea la monarquía cuasi absoluta; para Lock es la vida la libertad y la propiedad de ahí que el tipo de gobierno más pertinente sea la monarquía constitucional; en cambio, para Roseau los derechos naturales son la libertad civil proveniente de las leyes y la igualdad política y económica por lo que para él la forma de gobierno indicada es la democracia radical.

La naturaleza de los derechos humanos se puede ver desde la perspectiva de 4 dimensiones:

Derechos naturales	Esta concepción se apoya en el pensamiento liberal a partir del cual se consideró la existencia de derechos naturales inherentes a todas las personas y previos a la celebración de un contrato social, así pues, se tenía el derecho a la resistencia cuando el contrato era voto por el gobernante, cuando había violaciones sistémicas a los derechos naturales reconocidos y protegidos en el contrato.
Derechos morales	Aquí se piensa en el individuo aislado, sino en la construcción de principios y de valores compartidos.
Derechos positivos	Tanto Norberto Bobbio desde la filosofía jurídica como Luigi Ferrajoli desde el positivismo critico dieron por hecho que la emisión de la Declaración Universal de Derechos Humanos podía solventarse el problema del sustento de los derechos humanos: están ahí y están positivados. En la medida en que ya entraron al sistema jurídico positivo, la problemática es otra (por ejemplo, cómo hacerlos eficientes o efectivos), pero la

	fundamentación ya no es una problemática.
Derechos históricos	En esta concepción permite observar el proceso de nacimiento de los derechos, los grupos que los apoyaron, los objetivos, los procesos de cambio y exclusión en su institucionalización, entre otros aspectos, lo que enriquece los contextos de creación del derecho para una mayor interpretación del derecho a partir de cambios de contexto, así como la aparición de nuevos derechos.

Cuadro simplificado que muestra las perspectivas de los derechos humanos de manera general.[62]

2.3. Principios de los derechos humanos.

Existen 4 principios básicos de los derechos humanos que son reconocidos por la Constitución en su artículo 1, los cuales se explicaran a continuación por medio de un cuadro[63]:

Principio de Universalidad para todas las personas.	Los derechos humanos corresponden a todas las personas, por igual, sin discriminación alguna, de ello se desprende el principio de universalidad
Principio de interdependencia e indivisibilidad: Todos los derechos humanos	Los derechos humanos son interdependientes, es decir que no pueden separarse o fragmentarse unos con otros. Todos los derechos humanos, civiles, políticos, económicos, sociales y culturales deben comprenderse como un conjunto. Lo anterior implica que el goce y ejercicio

[62] *HERRERA Ortiz, Margarita, Manual de Derechos Humanos 4ª ed., México, Porrúa, 2003.*

	de un derecho está vinculado a que se garantice el resto de los derechos; así como la violación de un derecho pone también en riesgo los demás derechos. Los principios de interdependencia e indivisibilidad generan la obligación de otorgar igual importancia a todos los derechos humanos.
Principio de Progresividad	Se refiere al gradual proceso para lograr su pleno cumplimiento de ciertos derechos se requiera tomar medidas a corto, mediano y largo plazo, pero procediendo lo más expedita y eficazmente posible. También se relaciona de forma estrecha con la prohibición de retrocesos o marchas injustificadas a los niveles de cumplimiento alcanzados, la no regresividad, en la protección y la garantía de derechos humanos, la "no regresividad" en la protección y garantía de derechos humanos.

Cuadro elaborado de manera metódica para mostrar de manera puntualizada y su importancia de los 4 principios básicos.[64]

Los derechos humanos, en su vertiente técnica implican principalmente el control de los actos estatales respecto a "ciertos atributos inviolables de la persona humana que no pueden ser legítimamente menoscabados por el ejercicio del poder público". Se trata de esferas individuales que el Estado no puede vulnerar, o en los que solo puede penetrar limitadamente.

[64] *En la Biblioteca Digital de la Comisión Nacional de los Derechos Humanos, los principios de universalidad, interdependencia indivisibilidad de los derechos humanos en línea con dirección URL: https://www.cndh.org.mx/sites/all/doc/cartillas/2015-2016/34-Principios-universalidad.pdf 24-01-2020*

La importancia de los principios es considerada como una base o insumos que ya son fijos e inmutables, los cuales obligan a que se cumplan los derechos y obligaciones de las personas.

2.4. Características de los derechos humanos.

Los derechos humanos tienen características que los hacen distinguirse de los demás derechos que componen el ordenamiento jurídico. Se caracterizan por lo siguiente:

a. Son inherentes al ser humano. Una característica básica de los derechos humanos es su inherencia a todo hombre, porque para que se reconozco a toda persona, se prescinde de cualquier dato accidental o externo al ser humano, como sería su nacionalidad, cultura, condición social, económica o política, y basta con su existencia como tal para que se considere que le está adscrito a la persona toda una serie de derechos. Para su existencia no se precisa de su reconocimiento por el Estado, ya que le son oponibles a este aun ante su ignorancia o desconocimiento, o bien su franca vulneración.
b. Universalidad. Le corresponden a todo ser humano, con independencia del sitio del orbe en que se sitúe. Le están adscritos en forma igual y sin que para ello se relevante su raza, color, sexo, idioma, origen nacional o condición política, económica o social, así como su ideología o creencias. Tan es así que estén reconocidos en los principales instrumentos internacionales de derechos humanos por el concierto unánime de naciones.
c. Son supremos. Los derechos humanos, por el hecho de estar consagrados en el texto constitucional gozan de la supremacía que establecen los artículos 133 t 1. Como consecuencia, los derechos humanos son ley Suprema de la Unión.
d. Restricciones u obligaciones. En primer lugar, para el Estado nacional, y enseguida para la comunidad internacional, el concierto de naciones, así como para los particulares. Su contenido permite advertir que son limitaciones al poder público que abundan en beneficio de las libertades de igualdad, libertad y seguridad jurídica, los derechos sociales o los que corresponden a los pueblos o naciones, ya que impiden al poder público interferir en ámbitos

que están reservados a los particulares o titulares del derecho de que se trate, salvo con ciertas limitaciones que sean estrictamente necesarias, racionales y no arbitrarias;

e. Transaccionalidad o internacionalidad. En la medida que no están suscritos a su reconocimiento por un Estado en concreto, porque no se establecen a favor de un individuo en razón de su nacionalidad o residencia, o bien el lugar en que se encuentre, les son atribuidos al hombre por su condición de persona. El Estado no puede impedir su protección internacional bajo la manifestación de soberanía ni mucho menos para afectarlos.
f. Irrenunciabilidad. La vigencia o validez de los derechos humanos no está sujeta a la voluntad de un particular o del Estado, por lo que no puede la persona convenir su limitación o restricción, ni disponer por un acto de voluntad unilateral o bilateral, entre la persona y cualquier otro sujeto de derecho, que puedan modificarse los alcances de sus derechos.
g. Irreversibilidad. Una vez que se incorpora formalmente como parte del estatuto jurídico de un individuo, o bien que ha sido reconocido como inherente al ser humano, deviene en definitivo e irrevocable dentro de la categoría de derecho humano. De esa manera no cabe la denuncia de los que estén establecidos en un tratado internacional, porque aún seguirán pensando como norma imperativa de ius cogens.
h. Progresividad. Son el mínimo mínimum. Es decir, tienen un carácter de básicos o elementales e irreductibles porque desconocerse ya no podría señalarse que se tiene la condición de ser humano. Su imposible desconocimiento, desde el punto de vista jurídico, daría lugar a la negación de la persona humana. Esta característica ha llevado al reconocimiento de las generaciones de derechos humanos y a la instauración de diversos instrumentos de derechos humanos para su defensa y protección.

i. Son rígidos. Esta característica obedece a la característica de rigidez de cada Constitución, de la cual participan los derechos humanos por ser parte integrante.[65]

2.5. Clasificación de los derechos humanos.

Existen muchas clasificaciones sobre los Derechos Humanos son la finalidad de establecer cuales derechos surgieron primero. Maurice Duvenger habla de las libertades-limites (aquella que definen un coto cerrado a la actividad gubernamental), y las libertades- oposición (son libertades que procuran medios de oposición al gobierno para evitar que su imperio sea demasiado fuerte). En las primeras ubica a las libertades de la persona o libertades civiles, libertades económicas y las libertades de pensar, especialmente en las libertades religiosas y las libertades artísticas, estas últimas conforman también a las libertades –oposición, las diferencias se encuentran en que son a su vez limite y oposición para el gobierno.[66]

Para Sánchez Agesta son 4 grupos, atendiendo a la naturaleza del bien protegido por los derechos humanos y a la diversa naturaleza de su realización y garantía jurídica[67]:

a) Derechos civiles que protegen la vida personal e individual. Comprenden este grupo:

1. Los derechos de la intimidad personal (protección negativa de la autonomía de la vida privada frente a su violación de los particulares o por agente de estado);
2. Los derechos de la seguridad personal (protección de la libertad mediante la garantía de la ley aplicada por el juez);
3. Derecho de la seguridad económica (garantía de la propiedad y de la legalidad de los impuestos) y derechos de la libertad económica.

---

[65] *S/A, Capítulo I, Conceptos y Características de los Derechos Humanos, en línea con dirección URL: www.derechos.org.mx consultado 10-01-2021.*

[66] *DUVENGER, Maurice, Instituciones Políticas y Derecho Constitucional. Ed. Tecnos, Madrid, 1970.*

[67] *NUÑEZ, Palacios Susana, Derechos Humanos en línea con dirección URL: file:///C:/Users/maby /Downloads/5118-4517-1-PB.pdf consulta 09-03-2021.*

b) Derechos públicos: que son derechos de intervención en la formación de la opinión pública (libertades de reunión, de expresión del pensamiento, de información y de constituir asociaciones políticas y culturales).
c) Derechos políticos que son los derechos de participación en la vida pública (derecho de petición, de sufragio, de ejercer cargos públicos).
d) Derechos sociales, de los que se pueden hacer 2 grupos:

1. Derecho de desenvolvimiento personal (derecho a la instrucción y a la educación, a constituir una familia, a la práctica del culto religioso) y
2. Derechos sociales estrictos, que implican en una prestación positiva del Estado, inspirándose en los principios de justicia social y seguridad social (derecho a la propiedad personal y familiar, el trabajo, a un salario justo, a los seguros sociales a la asociación laboral).

Loewestein los clasifica de la siguiente manera[68]:

1. Libertad Civiles en el sentido propio, a la que pertenece la protección contra la arbitraria privación de la libertad (habeas corpus), la inviolabilidad del domicilio, la protección contra registros y confiscaciones legales, la libertad y el secreto de correspondencia y de otros medios de comunicación, la libertad de residencia dentro del territorio nacional y, así mismo, las posibilidades de libre decisión que se deduce de la individualización de las relaciones familiares.
2. Derechos de autodeterminación económica, que comprende la libertad de la actividad económica general, la libertad de elección de profesión económica, la libertad de competencia, la libertad disposición sobre la propiedad y la libertad de contrato.
3. Las libertades políticas fundamentales, hacen referencia a la participación del individuo en el proceso político. Las más importantes entre ellas son las relacionadas con la formación de la opinión pública: la libertad de asociación, la libertad de reunión y el derecho a organizarse en grupo, el derecho de votar y de tener igual acceso a los cargos públicos.

[68] *NUÑEZ, Palacios Susana, Óp. Cit. p.2*

Fernando Volio cataloga con muchos aciertos, como original la clasificación que hace Jean Marquiset, quien partiendo del derecho natural nos habla de los derechos del hombre sobre su cuerpo, es decir, los que se reconocen a la persona humana en el ejercicio de su actividad fisiológica. En cada una de las categorías el autor deriva diversas situaciones que engendran derechos:[69]

1) El derecho a la existencia: la intangibilidad del cuerpo humano, la protección de la vida intrauterina, la protección del recién nacido, la protección de los menores de quince años, el derecho de corrección, la legitima defensa, el suicidio, la eutanasia, el duelo.
2) El derecho a la integridad personal: la reparación de las lesiones corporales, la libertad de movimientos, el derecho a la mutación, la vocación del peligro, el gusto del riesgo, el aspecto físico y la cirugía estética, el tatuaje, la defensa de la propia imagen, la donación de la leche y de la sangre.
3) El derecho a la salud: el derecho de comer, de descansar y de cuidarse, la protección de la salud pública, la vigilancia de la salud individual, el alcoholismo, la toxicomanía.
4) El derecho a la vida sexual: la unión libre, el casamiento
5) Los derechos de la justicia sobre el cuerpo humano: la mano de la justicia, los derechos de la policía, la identificación de un malhechor, la búsqueda de alcohol en la sangre, los derechos del juez de instrucción; el informe pericial médico legal, el informe pericial psiquiátrico y el pentotal, las penas corporales y la justicia civil.
6) Los derechos del médico sobre el cuerpo humano: la intervención del médico, el contrato médico, la responsabilidad del médico.
7) Los derechos del hombre sobre su cadáver: la libertad de los funerales, el respeto al cadáver, el embalsamiento, la integridad del cadáver y los trasplantes anatómicos.

Clasificación de los derechos humanos en México

En México se clasifica a los derechos humanos en dos ramas:

[69] *VOLIO Fernando, Algunas Tipologías de Derechos Humanos. Universidad de Costa Rica, Costa Rica, 1978, p.64*

a. Los derechos humanos consignados dentro del texto constitucional y que nuestro máximo ordenamiento legal designa con el nombre “De los derechos humanos y sus garantías” y que se localizan en los primeros 29 artículos de nuestra Carta Magna, aunque además de ellos también encontramos derechos humanos, en la parte orgánica por ejemplo en los artículos 30, 34,123 entre otros.
b. B. Los tratados, pactos, convenios internacionales y otros que han pasado a ser parte de nuestro orden jurídico positivo, por el procedimiento que señala el artículo 133 y actualmente el artículo 1 de nuestra Constitución Federal, como son, por ejemplo: la Declaración Universal de los Derechos Humanos, documento expedido por la Organización de las Naciones Unidas el 10 de diciembre de 1948 y que México hizo suya.

Los derechos contemplados en nuestra Constitución Política de los Estados Unidos Mexicanos, son los siguientes: Igualdad ante la ley, Igualdad de todas las personas, Libertad persona, Libertad de trabajo profesión, industria o comercio. Libertad de expresión, Libertad de imprenta, Libertad de asociación y reunión, Libertad de tránsito y residencia, Libertad religiosa, Derechos a poseer armas, Derecho a la Información, Irretroactividad de las leyes, Garantía de audiencia, Garantía de legalidad, Seguridad jurídica en materia penal internacional, Inviolabilidad de las comunicaciones privadas, Inviolabilidad del domicilio, Seguridad jurídica en materia de ordenes de aprehensión o detención, Seguridad jurídica para los procesados en materia penal, Derecho a la jurisdicción, Seguridad jurídica en las detenciones ante autoridad judicial. Garantías del procesado en materia penal, Derechos de la víctima o del ofendido, Seguridad jurídica respecto a la imposición de penas y multas. Seguridad jurídica en los juicios penales, Protección de la integridad física y moral de las personas a las que se imponga una pena. Derecho a la nacionalidad, Derecho de petición, Protección jurídica al derecho a la vida, Derechos de los pueblos indígenas, Derecho a la educación. Derecho a un medio ambiente adecuado, derecho a la vivienda, Derechos sociales a favor de los trabajadores, Derechos de los niños, Derechos a la propiedad, Derecho a la propiedad comunal y ejidal de tierras, Derecho a la ciudadanía, Derechos del ciudadano.

Podemos mencionar asimismo la Convención Americana de los Derechos Humanos (que amplio el contenido y alcance de la Declaración Americana de Derechos y Deberes del Hombre de 1948), auspiciada por la Organización de Estados Americanos y suscrita en la Conferencia de San José de Costa Rica el 22 de noviembre de 1969, entró en vigor 18 de julio de 1978. Fue ratificada por nuestro país e incorporada a nuestro derecho interno al ser aprobada por el Senado de la Republica en junio de 1981.

2.6. La evolución histórica de los derechos humanos y las generaciones.

Los Derechos Humanos nacen con la humanidad misma, siempre se han encontrado presentes en la historia del ser humano, estos derechos han evolucionado de acuerdo a cada época; por ejemplo en la sociedad griega de hace 2,500 años vamos a encontrar que existían los ciudadanos griegos que gozaban de determinados derechos y que estos estaban protegidos por las leyes Griegas; sin embargo, existían personas que no gozaban de estos derechos y estaban privados de su libertad, a estos se les denominaba esclavos por gozar de esos derechos en una historia tan larga como la esclavitud mismo, los ejemplos más claros son de Espartaco y de Antonio. Todo este proceso de lucha forma parte de la actual dignidad humana. Este ejemplo nos muestra que cada uno de los Derechos Humanos que actualmente están protegidos por el Derecho Internacional han sido como producto de luchas de miles de pueblos y naciones enteras; gracias a ellos, ahora podemos abrir una Constitución y encontrar una efectiva protección a tales derechos a nivel nacional como una protección mediante convenciones internacionales.

Es de suma importancia conocer cómo han evolucionado los Derechos Humanos, eso nos dará oportunidad de saber toda la importante labor de nuestros antepasados y valorar esa herencia maravillosa y al mismo tiempo sabremos que este proceso no ha acabado y que nos corresponde un papel responsable como miembros de la comunidad en la promoción, respeto y reconocimiento de los Derechos Humanos a nivel mundial.

Para conocer a profundidad esa evolución, tendríamos que estudiar la historia de cada pueblo, sus costumbres y sus sistemas jurídicos; sin embargo, en razón a la

necesidad de síntesis, nos remitiremos a los principales instrumentos o documentos que históricamente se han referido a lo que hoy conocemos como Derechos Humanos.

Como bien lo mencionamos las diversas etapas de los derechos humanos son el acontecimiento histórico y resultado de la evolución de la sociedad que a través del tiempo se creen nuevos derechos.

German J. Bidart Campos lo describe como" un fenómeno cronológico y temporal que se ubica en el tiempo histórico en el ámbito de la cultura, en la evolución de las ideas políticas, el cual da un contorno de fenómeno cultural, humano, propio de la vida de los hombres, de lo que piensan, representan, son, aspiran, proyectan, ambicionan, hacen, valoran, esperan, necesitan, etc".[70]

La sistematización de los derechos humanos en generaciones ha sido ampliamente usada por la doctrina internacional, influenciada por razones ideológicas y políticas características del periodo de la guerra fría. Sin embargo, desde finales de los años 80 dicha doctrina ha sido rechazada energéticamente esa sistematización con argumentos históricos, éticos, políticos, jurídicos.

2.6.1. Los derechos humanos de primera generación.

Esta generación se ubica en la época en que cae el absolutismo político junto con las monarquías que le daban sustento, cuando ya hacia finales del siglo XVIII surge el constitucionalismo clásico. En esta etapa comienza a tomar conciencia de que, para poder acceder a la convivencia política, conforme a las ideas liberales, debía tener ciertos derechos que le permitieran ejercitar libremente las ideas de la época. Las colonias inglesas se independizan de Inglaterra y surge la Declaración Francesa de los derechos del hombre y del ciudadano.

La Constitución de Estados Unidos de América del Norte y en la Declaración Francesa es en donde surge la primera generación de los derechos humanos, los llamados derechos individuales que contienen a la par derechos civiles y derechos políticos.

---

[70] *S/A, Capitulo I, Los Derechos Humanos, en línea, con dirección URL: https://funceji.files.wordpress.com/2017/09/lectura-3.pdf, consultado 14/03/2021*

Las ideas que dieron forma a esta primera generación son proporcionadas por Aristóteles, Cicerón, Santo Tomas de Aquino, etc. Posteriormente por Roseau, Voltaire, Diderot, DÁlembert y otros personajes. Como resultado de grandes luchas esas exigieron fueron consagradas como auténticos derechos y difundidas internacionalmente[71]. Entre ellos resaltan:

- Toda persona tiene derechos y libertades fundamentales sin distinción de raza y color, idioma, posición social o económica.
- Todo individuo tiene derecho a la vida a la libertad y a la seguridad jurídica
- Los hombres y mujeres poseen iguales derechos.
- Nadie estará sometido a esclavitud o servidumbre.
- Nadie ser sometido a torturas ni a penas o tratos crueles, inhumanos o degradantes, ni se le podrá ocasionar daño físico psíquico o moral.
- Nadie puede ser molestado arbitrariamente en su vida privada, familiar, domicilio o correspondencia, ni sufrir ataques a su honra y reputación.
- Toda persona tiene derecho a circular libremente y a elegir su residencia.
- Toda persona tiene derecho a una nacionalidad.
- En caso de persecución política, toda persona tiene derecho a buscar asilo y a disfrutar de él, en cualquier país. Los hombres y las mujeres tienen derecho a casarse y a decidir el número de hijos que desean.
- Todo individuo tiene derecho a la libertad de pensamiento y de religión.
- Todo individuo tiene derecho a la libertad de opinión y expresión de sus ideas.
- Toda persona tiene derecho a la libertad de reunión y de asociación pacífica.

2.6.2. Los derechos humanos segunda generación.

En los llamados derechos humanos de la segunda generación, los derechos civiles y políticos ya consagrados reciben, por parte de la sociedad, una ampliación acorde

[71] *FLORES, Salgado Lucerito Ludmila, Temas actuales de los derechos humanos de última generación, Benemérita Universidad Autónoma de Puebla, Puebla México, 1era edición 2015, en línea con dirección URL: http://cmas.siu.buap.mx/portal_pprd/work/sites/fdcs/resources/PDFContent/1378/Libro%20DIG%20-%20Temas%20actuales%20de%20los%20derechos%20humanos.pdf consultado 09-03-2021.*

con las necesidades de la época. Esto sucede por primera vez en México en 1917; en Rusia en 1918; en Weimar, Alemania en 1919.

Los derechos de la segunda generación son básicamente de tres tipos: derechos sociales y derechos económicos, sumándoles casi inmediatamente los derechos culturales. Estas anexiones emergieron debido a las necesidades de los hombres por mejorar sus condiciones de vida social, en el campo, en la religión cultural, etc.

Los filósofos, ideológicos y pensadores que dan vida a los derechos humanos de la segunda generación son: entre otros, Karl Marx, Federico Engels, Lenin, Hegel y algunos más.[72]

Los derechos humanos de la segunda generación deben cumplir con una función social, desde luego sin dejar de ser personales, o mejor dicho individuales. De esta manera, el individuo, que es su titular, deberá ejercerlos provisto de una conciencia social.

El constitucionalismo clásico se convierte en constitucionalismo social en la Constitución de 1917, ya que enfrenta las exigencias de que los derechos sociales y económicos descritos en las normas constitucionales, sean realmente accesibles y disfrutables. Se demanda un Estado de Bienestar que implemente acciones, programas y estrategias a fin de lograr que las personas los gocen de manera efectiva, y son los siguientes;[73]

- Toda persona tiene derecho a la seguridad social y a obtener la satisfacción de los derechos económicos, sociales y culturales.
- Toda persona tiene derecho al trabajo en condiciones equitativas y satisfactorias.
- Toda persona tiene derecho a formar sindicatos para la defensa de sus intereses laborales.
- Toda persona tiene derecho a un nivel de vida adecuado, que le asegure a ella y a su familia la salud, la alimentación, vestido, vivienda, asistencia médica y los servicios sociales necesarios.
- Toda persona tiene derecho a la salud física y mental.

[72] *S/A, Capítulo I, Los Derechos Humanos, en línea, con dirección URL: https://funceji.files.wordpress.com/2017/09/lectura-3.pdf, consultado 14/03/2021*

[73] *S/A, Capítulo I, Los Derechos Humanos, en línea, con dirección URL: https://funceji.files.wordpress.com/2017/09/lectura-3.pdf, consultado 14/03/2021*

- Durante la maternidad y la infancia, toda persona tiene derecho a ciudadanos y asistencia especiales.
- Toda persona tiene derecho a la educación en sus diversas modalidades.
- La educación primaria y la secundaria son obligatorias y gratuitas.

2.6.3. Los derechos humanos de la tercera generación.

También se denominan los derechos de solidaridad, en términos generales se refieren al derecho de los pueblos para reclamar ciertas prestaciones de la sociedad internacional. Como derecho a la paz, derecho a un medio ambiente sano y ecológicamente equilibrado, derecho a beneficiarse con el patrimonio común de la humanidad, derecho a la comunicación, derecho al desarrollo, etc. También el doctor Luis Díaz Müller agrega el derecho a un nuevo orden internacional. Asimismo, existen también el derecho a los recursos materiales, patrimonio cultural y artístico, etc.[74]

Entre los pensadores, filósofos e ideólogos que hicieron surgir los derechos de la tercera generación podemos mencionar a Harold J. Laski, Benedetto Croce, Marcery Fry, Mahatma Gandhi, Jacques Maritain Kurt Riezler, George Friedman, Hung-Shulo, Luc Somerhausen, Humayeun Kahir y Richard McKeon, entre muchos otros. Al hablar de esta generación nace un tiempo de “exigencia” en cuanto a su respecto o cumplimiento. Nos referimos a los llamados intereses difusos, colectivos, transpersonales o supraindividuales.

Esta terminología se emplea para designar a los sujetos a los que el derecho de la tercera generación está destinado a proteger, aquí nos damos cuenta de que no se trata de un individuo.

Este grupo de derechos fue promovido a partir de la década de los setenta para incentivar el progreso social y elevar el nivel de vida de todos los pueblos, en un marco de respeto y colaboración mutua entre las distintas naciones de la comunidad internacional. Entre otros, destacan la relación con:

- La autodeterminación
- La independencia económica y política.

[74] *S/A, Capítulo I, Los Derechos Humanos, en línea, con dirección URL: https://funceji.files.wordpress.com/2017/09/lectura-3.pdf, consultado 14/03/2021*

- La identidad nacional y cultural.
- La paz.
- La coexistencia pacífica.
- El entendimiento y la confianza.
- La cooperación internacional y regional.
- La justicia internacional.
- El uso de los avances de las ciencias y la tecnología.
- La solución de los problemas alimenticios, demográficos, educativos y ecológicos.
- El medio ambiente.
- El patrimonio común de la humanidad.
- El desarrollo que permita una vida digna.

2.6.4. Los derechos humanos de cuarta generación.

Los derechos humanos en sus tres primeras generaciones son obra de la cultura humana que exige tiempo y esfuerzo para dar vigencia sociológica a esos derechos y llevar a su realización valores positivos.[75]

En los últimos años, el estudio generacional de los derechos humanos ha ido concentrando nuevos planteamientos y opiniones de no poca importancia como son, entre otros, los de David Vallespín Pérez, Franz Matcher, Antonio Pérez Luño, Augusto Mario Morello, Robert B. Gelman y Javier Bustamante Donas. Todos estos autores apuntan al establecimiento de una generación de los derechos humanos.[76]

Esta generación de derechos emergentes viene a responder a nuevas necesidades de la sociedad que no habían aparecido antes, en el contexto de la contaminación de las libertades ante los usos de algunas nuevas tecnologías y avances en las ciencias biomédicas.

Son resultado de nuevas reivindicaciones de los ciudadanos, por una parte, y por la otra, de las transformaciones tecnológicas derivadas de los nuevos conocimientos

[75] Bailón Corres Moisés Jaime, *Derechos Humanos, generaciones de derechos, derechos de minorías y derechos de los pueblos indígenas*; algunas consideraciones generales, en línea con dirección URL: https://www.corteidh.or.cr/tablas/r28614.pdf consultado 10-01-2021

[76] Bailón Corres Moisés Jaime, *Derechos Humanos, generaciones de derechos, derechos de minorías y derechos de los pueblos indígenas*; algunas consideraciones generales, en línea con dirección URL: https://www.corteidh.or.cr/tablas/r28614.pdf consultado 10-01-2021

científicos y de su aplicación a diversos campos de la vida del hombre. Corresponden al actual estado social de derecho o estado democrático de derecho. Esta generación abarca diversos derechos que se siguen discutiendo ya que abraca, el peso de la tecnología y de la globalización que son los más importantes. En la mayoría de los casos esta nueva generación se trata de nuevos derechos y también referentes a los derechos ya establecidos en las anteriores generaciones. Todavía no existe claridad.[77]

Una de las clasificaciones más cercanas de esta generación los divide en tres subgrupos:

a) los derechos del hombre relativos a la protección del ecosistema, para garantizar la pervivencia futura de la vida humana en el planeta, y al patrimonio de la humanidad. Dentro de estos últimos destacan los derechos culturales y de autonomía de los pueblos indígenas. Se trata en algunos casos de derechos encaminados a las generaciones futuras. Se incluyen sin embargo algunos derechos ya definidos en la anterior generación, como el derecho al medio ambiente.[78]

b) un segundo grupo subgrupo de esta nueva generación de derechos corresponde a aquellos relativos a un nuevo estatuto jurídico para la vida humana, a consecuencia de las nuevas condiciones de las tecnologías biomédicas. Dentro de ellos podemos ubicar el derecho a la vida, pero al igual que en el caso anterior, se trata de un derecho que por los avances recientes de la ciencia es necesario redefinir.[79]

c) el tercer subgrupo corresponde a los derechos derivados de las nuevas tecnologías de la comunicación y la información.

Uno de estos derechos es el acceso a internet, derecho a la libertad de expresión.

2.6.5. Los derechos humanos de la última generación.

Los derechos humanos de última generación surgen como resultado de las necesidades humanas. Estas exigencias obligan a desarrollar nuevos derechos que 3garanticen el acceso universal a formas más avanzadas de ciudadanía y civilidad,

[77] Bailón Corres Moisés Jaime, *Derechos Humanos, generaciones de derechos, derechos de minorías y derechos de los pueblos indígenas*; algunas consideraciones generales, Op. Cit.
[78] Bailón Corres Moisés Jaime, *Derechos Humanos, generaciones de derechos, derechos de minorías y derechos de los pueblos indígenas*; algunas consideraciones generales, Op. Cit.
[79] Bailón Corres Moisés Jaime, *Derechos Humanos, generaciones de derechos, derechos de minorías y derechos de los pueblos indígenas*; algunas consideraciones generales, op. Cit.

de libertad y de calidad de vida e incluyen, entre otros derechos: a la paz y a una justicia internacionales: la limitación del derecho a la inmunidad diplomacia para determinados delitos; el derecho a crear un tribunal internacional que actúe de oficio en los casos de genocidio y crímenes contra la humanidad; al desarrollo sostenible que permita preservar el medio ambiente natural; el derecho a un entorno multicultural que supere el concepto de tolerancia sexual; las nuevas formas de industrialización y métodos de trabajo, que entraría bajo la llamada flexibilización laboral ; y la protección de los derechos de las personas incapacitadas.[80]

Cabe destacar que se debe añadir el uso y establecimiento de nuevas tecnologías, tales como la inteligencia artificial, los nuevos medios de comunicación masivos (en la red), así como la reivindicación de los derechos ya definidos y desarrollados en la 1ª, 2ª y 3ª generaciones, solo que en el entorno del ciberespacio. A continuación, se desglosará una lista de los derechos de la última generación y abordare los derechos humanos del acceso a la información y el ciberespacio.[81]

- La flexibilización laboral.
- Transexualidad
- Derechos homosexuales.
- Los derechos reproductivos de la mujer.
- El derecho a la información, de acuerdo al artículo 19 de la Declaración Universal de los Derechos Humanos, es que toda persona posee garantías fundamentales, mismas que son:

a. El derecho a obtener información: influye facultades como el acceso a archivos, registros y documentos públicos.

b. El derecho a informar: recibir información objetiva y oportuna, la cual debe ser completa y con carácter universal.

c. El derecho a ser informado: emplea los más diversos espacios, instrumentos y tecnologías para la transmisión de ideas y hechos.

[80] *S/A, Capítulo I, Los Derechos Humanos, en línea, con dirección URL: https://funceji.files.wordpress.com/2017/09/lectura-3.pdf, consultado 14/03/2021*

[81] *S/A, Capítulo I, Los Derechos Humanos, en línea, con dirección URL: https://funceji.files.wordpress.com/2017/09/lectura-3.pdf, consultado 14/03/2021*

En los últimos años se han podido ver como el interés regulador de la libertad de expresión por parte de los gobiernos se ha centrado también en el internet. En regímenes dictatoriales o en los que los derechos civiles no están plenamente reconocidos, se intenta frecuentemente censurar a la red con la excusa de la defensa de los valores culturales autóctonos frente a modelos de vida extranjeros.

En muchos casos, él envió de correo electrónico al extranjero o la consulta de páginas web no autorizada trae consigo fuerte penas o cárcel. En el caso de China, la represión y de acceso a la información. Una de estas medidas es la implantación de “cortafuegos” (firewalls). Antes de entrar por primera vez en internet todo ciudadano chino está obligado a rellenar un exhaustivo formulario, de tal manera que se garantiza la plena identificación del usuario en la red y el control gubernamental de cualquier tipo de acceso o intercambio de información.

Diferentes países han adoptado también medidas legislativas que limitan el ejercicio de los derechos civiles a través de las autopistas de la información. Los estados miembros de la Asociación de Países del Sudeste Asiático (ASEAN) formad por Brunéi, Indonesia, Vietnam, Singapur, Filipinas, Tailandia y Malasia, firmaron en 1996 un protocolo por el que establecían un marco de cooperación para limitar el acceso a internet a sus ciudadanos.

Su argumento estribaba en defender las tradiciones culturales y morales de dichos países frente a la decadencia moral de Occidente, evitando así la exposición de sus ciudadanos a contenidos informativos que podían generar dudas con respecto a la legitimidad de sus regímenes y gobernantes.

2.7. Los derechos humanos en el ciberespacio.

El internet es la estructura social más importante de las nuevas tecnologías de comunicación que haya tenido el mundo, ya que en el siglo XXI el mundo de las guerras del futuro, y se diriman las disputas de poder en todas las esferas, sí no ahora hay una guerra cibernética.

No será necesario invadir un país, ni tampoco poner grilletes en muñecas y tobillos o atar las manos a sus ciudadanos, si podemos reeducar el deseo, convertirlos en consumidores, colonizar las conciencias a través de los valores implícitos en los productos audiovisuales. Los nuevos colonialismos no obligan a sus provincias al

pago de onerosos impuestos, sino que se invaden sus mercados de productos y servicios de todo tipo.

Los derechos humanos en el ciberespacio siguen siendo un tema complejo interesante y carente de información para poder crear políticas, organismos o instituciones que logren hacer una ley o protección que sea aplicable a nivel internacional debido a que choca con el derecho interno, sin embargo, existe la Declaración de los Derechos del Ciberespacio los cuales se podrían resaltan los referentes a los Derechos humanos.

El sistema internacional de Derechos Humanos debe hacer frente a los vertiginosos cambios de la escena mundial y analizar, aplicar las modificaciones o adaptaciones necesarias a fin de responder a una realidad compleja. Ante tales circunstancias son indudables las transformaciones que las TIC y específicamente Internet han generado en la esfera social y política contemporánea, la protección de los Derechos Humanos en el ciberespacio no debe ser una tarea ignorada, pues se trata de un lugar si bien intangible de interacción social, y además de ser un punto donde se encuentran todo tipo de participantes de cualquier parte del globo.

La Word Wide Web se ha convertido en un nuevo medio para ejercer derechos como a la privacidad, a la libre expresión y a la información y como tales deben ser protegidos. A pesar de los desafíos que la naturaleza de la red de redes plantea para los aparatos jurídicos nacionales e internacionales es necesario reunir esfuerzos para que las libertades de las personas no sean violentadas, pues internet no solo se relaciona con el intercambio de datos y opiniones, sino que, de forma general, y de acuerdo con Eleonora Rabino Vich, amplia las oportunidades para el ejercicio de los Derechos Humanos. El ciberespacio representa una vía denuncia global en contra crímenes de lesa humanidad, de agresión a la dignidad e interactividad de las personas y de toda actividad que atente contra los Derechos Humanos, también no necesariamente son directamente las violaciones a una persona sino también existe el caso de sus bienes como robo a la propiedad, adulteración de documentos, venta de armas, delitos sexuales (pornografía infantil), desfalco, fraude, juegos de Azar (no entrega del premio) ilegales, propiedad robada o tráfico, intento de agresión (ciberacoso, ciberbullyng, sexting etc.), violación de leyes sobre venta de drogas, delitos de propiedad intelectual o piratería y los delitos más recientes o destacados

son el crimen organizado virtual, crimen de finanzas crimen motivado por prejuicios, robo de identidad y ciberterrorismo, estos ciberdelitos serán explicados de manera detalla en el capítulo tercero.

Hacia una declaración de los Derechos Humanos en el Ciberespacio

"La Web se ha convertido en algo más que una vía de comunicación su impacto en la economía política, sociedad, cultura y seguridad de una nación demanda la estructuración de un marco normativo eficiente que, por un lado proteja la integridad y los intereses nacionales, y por el otro asegure el respeto a los derechos y libertades de las personas , el objetivo no es nada sencillo pues diversas propuestas para la regulación de Internet a menudo encierran disposiciones que atentan contra determinados derechos, por ello especialistas como Javier Bustamante han llamado a considerar a internet como un espacio donde se manifiestan, profundizan y desarrollan los Derechos Humanos. La importancia de los flujos de comunicación transfronterizos vía internet fue analizado a finales del siglo pasado, como resultado Robert B Gelman desarrolló una propuesta de Declaración de Derechos Humanos en el ciberespacio presentada en 1997, en ella se refiere a nuevas versiones o modalidades de derechos tradicionalmente aceptados que experimentan un re significación en el entorno virtual".

El escrito de Gelman está inspirado en la Declaración Universal de los Derechos Humanos y, entre otros puntos, reconoce:

- Que las ideas y opiniones de todos los seres humanos merecen oportunidad igual para poder expresarse, considerarse y compartirse con otras. Según la voluntad del emisor y del receptor directa o indirectamente.
- Toda persona tiene derecho a la privacidad, anonimato y seguridad de las transacciones en línea
- Nadie puede ser sometido a vigilancia arbitraria de sus opiniones o actividades en línea. [82]

[82] *BUSTAMANTE, Donas Javier, Hacia la Cuarta Generación de los Derechos Humanos: repensando la condición humana en la Sociedad Tecnológica, Revista Iberoamericana de Innovación en línea con dirección URL: http://www.oei.es/revistacts/numero1/Bustamante.htm&gt*

A partir de la Declaración de Gelman otros especialistas se han concentrado en desarrollar propuestas similares con el fin de estructurar la que mejor se adapte a la compleja naturaleza de la red de redes.

Norberto Bobbio plantea un punto importante sobre la delimitación de los derechos en línea; su protección: En este sentido, existe conflicto respecto a quiénes serán los encargados de velar por la seguridad y la protección de los derechos en línea, por un lado aparecen los Proveedores de Servicios de Internet (ISP) quienes hacen posible la conexión entre dispositivos electrónicos y la red lo que significa que reciben, resguardan y transfieren cientos de datos y por el otro lado, están los organismos estatales encargados de las telecomunicaciones y quienes exigirían cuentas a los ISP. No obstante, la posibilidad de otorgar el monitoreo de las comunicaciones digitales a los ISP coloca a los derechos en línea en una situación vulnerable, pues debido a que los ISP pertenecen al sector privado carecen de mecanismos de rendición de cuentas (por lo menos de aquellos que se aplican a los órganos estatales) y de transparencia, abriendo la oportunidad a posibles violaciones a los derechos y libertades en línea. Mientras que, del lado de las dependencias estatales, quienes idealmente deberían ostentar dicha función, se requiere también de mecanismos eficientes de rendición de cuentas y transparencia. Al respecto es preciso recalcar la unidireccionalidad en cuanto a la protección de los DD. HH entre el Estado y los ciudadanos, a fin de que la regulación de las comunicaciones digitales no caiga en manos de terceros.[83]

2.8. Derecho Internacional de los Derechos Humanos (DHIH).

La internacionalización de los derechos humanos ha modificado la mayor parte de los sistemas jurídicos del mundo, así como la visión, alcance y contenidos de los organismos internacionales que han surgido después de la Segunda Guerra Mundial y hasta la fecha, por los excesos del Nacismo, se transitó de una protección nacional de los derechos fundamentales a una etapa de protección internacional y regional de los derechos humanos

[83] *REVISTA, CYBERINTERNATIONALAFFAIRS, en línea con dirección URL: https://berenicefn.wordpress.com/2017/12/15/internet-y-su-efecto-sobre-los-derechos-humanos/ consulta 10-03-2021.*

Ahora bien, ya desde 1946 contamos con una serie de documentos e instituciones que tratan los derechos humanos que, como ya hemos mencionado, hoy se encuentran en crisis. Tenemos principalmente:

La legislación internacional moderna de los derechos humanos es un fenómeno posterior a la Segunda Guerra Mundial; su evolución se produjo a partir de las enormes violaciones a estos perpetradas bajo la férula de Hitler. Carta de la Organización de las Naciones Unidas (ONU) fue un documento que estableció las bases legales y conceptuales, que permitió elaborar la legislación de los derechos humanos contemporánea.

El Derecho Internacional de los Derechos Humanos, es una rama del Derecho Internacional público la cual se fortaleció con la Declaración Universal de los Derechos Humanos en 1948. El cual establece obligaciones que los Estados a actuar de una manera determinada, para promover y proteger los derechos humanos y las libertades fundamentales de los individuos o grupos.

El Derecho Internacional de los Derechos Humanos es un conjunto de normas internacionales que reafirman los derechos y la dignidad de todos los seres humanos, mujeres, hombres y niños sin discriminación.

Fernández Casadevante define el Derecho Internacional de los Derechos Humanos como “aquel sector de ordenamiento internacional, compuesto por normas de naturaleza convencional, consuetudinaria e institucional que tiene por objeto la protección de los derechos y libertades fundamentales del ser humano inherentes a su dignidad”

El derecho internacional de los Derechos Humanos tiene por objeto de estudio las normas y los principios internacionales relativos a los derechos humanos:

- Incorpora a la persona como sujeto de derecho internacional
- Cuenta con sus propios órganos de protección, entre otros los “órganos creados en virtud de tratados, “las Comisiones y Cortes regionales de derechos humanos.
- Tiene sus principios de interpretación propios, entre ellos el principio pro persona, consagrado en el párrafo segundo del artículo 1º de la constitución mexicana. Algunos autores identifican como principios de derechos humanos: el principio de posición de fuerza expansiva de los derechos humanos o

prefered freedom, el principio de fuerza expansiva de los derechos humanos y el principio de progresividad.

- También es importante destacar el papel de la recepción nacional del Derecho Internacional de los Derechos Humanos a través de los órganos internos de los Estados, en sus funciones ejecutivas, legislativas y jurisdiccionales, lo que nos pone en contacto directo con sus fuentes.

La Declaración francesa de Derechos del Hombre y del Ciudadano de 1789 y posteriormente en diversas constituciones.

El concepto del derecho internacional de los derechos humanos es una rama de derecho internacional público, cuyo objeto es la promoción y protección de los derechos humanos.

Es importante hacer referencia de los demás derechos que conlleva el derecho internacional de los derechos humanos, para evitar confusiones y así comprender la disciplina. El derecho internacional público es "el conjunto de principios, normas, y reglas adoptadas de cumplimiento obligatorio, que fijan los derechos y deberes de los Estados y otros sujetos del derecho internacional y rigen sus relaciones reciprocas"[84] por lo que se dirigió principalmente a los Estados, después a las organizaciones internacionales y a ciertos individuos. Por si parte el Derecho Internacional de los Derechos Humanos, comienza con la protección de los seres humanos, de manera individual o con miembros de una colectividad frente al Estado que se encuentre.

2.8.1. Fuentes del Derecho Internacional de los Derechos Humanos.

Los tratados internacionales.

Son una fuente prioritaria de derecho internacional. La Convención de Viena sobre Derecho de los Tratados de 1969, define en su artículo 2º. Que un tratado es un acuerdo internacional celebrado por escritos entre Estados y regido por el derecho internacional celebrado por escrito entre Estados y Regido por el derecho

[84] *CASTAÑEDA, Mireya, El Derecho Internacional de los Derechos Humanos y su recepción nacional, Comisión Nacional de los Derechos Humanos, México, 2018, en línea con dirección URL: http://appweb.cndh.org.mx/biblioteca/archivos/pdfs/Observaciones-Comite-ONU-vol-II.pdf consulta 10-03-2021.*

internacional, ya consté en un instrumento único o en dos o más instrumentos conexos y cualquiera que sea su denominación particular".[85]

Existe una gran diferenciación sobre los tratados sobre derechos humanos y los tratados internacionales en general, el primero se refiere por el tipo de obligaciones en ellos plasmadas, y los últimos establecen un cambio reciproco de derechos y obligaciones entre los Estados partes. Los tratados de derechos humanos se pueden clasificar en:

1) Universales o regionales

Un tratado es universal si ha sido aprobado por la Asamblea General de Naciones Unidas, o regional si ha sido aprobado por un organismo regional, como lo es la Organización de Estados Americanos.

2) Generales o específicos

Los tratados generales de derechos humanos están dirigidos a toda persona, los específicos a ciertos grupos que se han identificado en situación de vulnerabilidad, como son, mujeres, niñas y niños, migrantes, personas con discapacidad.

Costumbre internacional

Es la fuente más antigua de derecho internacional, y junto con los tratados ha sido interpretada como una fuente prioritaria en el marco del Estatuto de la Corte Internacional de Justicia. Esta es referida por el artículo 38 del estatuto como "prueba de una práctica generalmente aceptada como derecho".[86]

Los principios generales del derecho

La función principal de esta fuente es la subsidiariedad para la solución de controversias cuando existan lagunas o para ayudar a la interpretación de normas convencionales o consuetudinarias.

La doctrina

El artículo 38 del Estatuto de la Corte Internacional de Justicia señala como medio auxiliar para la determinación de reglas del derecho internacional. La doctrina ha sido usada tanto en sentencias, como en opiniones separadas o disidentes de jueces por

[85] *CASTAÑEDA, Mireya, El Derecho Internacional de los Derechos Humanos y su recepción nacional, CNDH, México, 2018. P.34.*

[86] *CASTAÑEDA, Mireya, El Derecho Internacional de los Derechos Humanos y su recepción nacional, óp. Cit. P. 36*

la Corte Internacional de Justicia. Se considera como fuente análoga a las publicaciones de la Comisión de Derecho Internacional de Naciones Unidas.

En México, la Comisión Nacional de los Derechos Humanos ha abierto un espacio para la difusión y reflexión del Derecho Internacional de los Derechos Humanos, a través de algunas de sus colecciones de escritos.

Las decisiones judiciales

El Estatuto de la Corte Internacional se refiere a las decisiones judiciales como medios auxiliares para la determinación de las reglas de derecho internacional. La Corte Internacional de Justicia se tuvo que ajustar los distintos sistemas jurídicos como Common Law en los países anglosajones.[87]

La interpretación de tratados de derechos humanos

Está hecha por un órgano supranacional hecha particularmente para la aplicación por parte de los jueces y tribunales nacionales. También se debe tomar el principio pro persona, para la aplicación, pero sin petrificarla a cierta sentencia, porque como señalo la Corte un tratado debe ser: "interpretado y aplicado en el cuadro del conjunto del sistema jurídico en vigor en el momento en que la interpretación tiene lugar. [88]

Las resoluciones de organismos internacionales

Para Becerra Ramírez, las resoluciones de organismos internacionales progresivamente han ocupado un lugar como fuentes en la práctica internacional. Pueden designar cualquier acto que se pueda denominar de distintas maneras, verbigracia decisión, acuerdo, declaración. En el caso especial de las resoluciones emitidas por la Asamblea General de las Naciones Unidas, se ha señalado que no son obligatorias en virtud de su origen, es decir, por no reconocerlo así por la Carta de las Naciones Unidas; sin embargo, muchas de ellas han tenido una repercusión indudable.[89]

[87] *CASTAÑEDA, Óp. Cit. P. 37*
[88] *CASTAÑEDA, Óp. Cit. P. 38*
[89] *SORENSEN*, Max, *Manual de Derecho Internacional Público*, p. 184

2.8.2. Principios Internacionales de los Derechos Humanos.

Soberanía interna	Tanto la Organización de las Naciones Unidas (ONU) como la Organización de Estados Americanos (OEA) se constituyen a partir del reconocimiento y respeto mutuo de la soberanía. A su vez, cuando los Estados aceptan y ratifican un tratado internacional, asumen la obligación de adecuar sus prácticas a los compromisos adquiridos por éste. La práctica internacional entiende que los derechos humanos, principalmente las violaciones graves, sistemáticas, crímenes de lesa humanidad y genocidios son de interés común, y la apelación a la soberanía esta fuera de sitio. Sin embargo, no todos los temas relacionados con los derechos humanos tienen que ver con crímenes de guerra, genocidio o crímenes de lesa humanidad. Al firmar un tratado internacional, el país se compromete a adoptar estándares de comportamiento acordes a dicho documento. Ha de notarse que la intervención en un país por parte de un organismo internacional no es solo una intervención en asuntos internos, sino también una verificación del cumplimiento de las obligaciones adquiridas. El derecho de los Estados a que se respete su soberanía implica su obligación de respeto a los derechos humanos. El organismo internacional, ha de tomar en

	cuenta las condiciones culturales, económicas y sociales de dicho país, pues la determinación del cumplimiento de las obligaciones del Estado organizará sus recursos para conseguir ese respeto. Además, en el derecho interno se reconocen unos compromisos del Estado mexicano hacia los derechos humanos. Esto se puede entender en el sentido de que la "soberanía" de México está limitada o, si se prefiere, íntimamente formado por los derechos humanos.
Principio de la buena fe: *Pacta sunt servanda:*	El artículo 26 de la Convención de Viena establece que todo tratado vigente obliga a las partes y debe ser cumplido por ellas de buena fe. En derechos humanos, esto implica que el Estado cumplirá con las obligaciones adquiridas en el pacto de buena fe, y realiza sus mejores prácticas en aras de su cumplimiento. "una parte no podrá invocar las disposiciones de su derecho interno como justificación del incumplimiento de un tratado. En consecuencia, aunque algunos de los procesos de derechos humanos terminen en recomendaciones, o los informes sobre un país sean una descripción genérica, dichas resoluciones no solo son buen propósito, sugerencia o consejo. Con la firma del tratado, el país está obligado a implementar las acciones razonables para garantizar y respetar los derechos, lo que se traduce en por lo

	menos tomar en cuenta las recomendaciones o el contenido de los informes.
	Las normas y prácticas de los derechos humanos han de interpretarse “ratione personae;” es decir; en función de que la persona es tal y de manera que se le proteja lo mejor posible. Las obligaciones de los Estados en cuanto a los derechos humanos se determinan en función de la persona en sus particulares necesidades de protección, ya sea por su condición personal o por la situación específica en que se encuentre. Otro principio de interpretación de los procesos en derechos humanos. Es decir, las obligaciones de los Estados y la acción de los organismos de protección han de buscar la efectiva protección de los derechos humanos. Por ejemplo, el recurso judicial por violación a los derechos humanos debe ser razonablemente eficaz.
	Los organismos de derechos humanos y los documentos que los originaran están orientados, más que a establecer un equilibrio de intereses entre los Estados, a garantizar el goce de los derechos y libertades del ser humano. Por eso, la distinción entre sistemas va dirigida más a la determinación de competencias y tipos de asuntos entre los sistemas, que a una “separación” entre ellos. En consecuencia, aun si los organismos

	internacionales solo pueden conocer de asuntos relacionados con países que hayan ratificado tanto el tratado como aceptado la competencia de dicho organismo, en razón de la materia, también pueden auxiliarse de los tratados, la jurisprudencia y el ius cogens del resto de los sistemas de protección. A este principio se le conoce como "de incorporación ".

Cuadro simplificado para mostrar los principios de los derechos humano con base a la información que aparece a pie de página.[90]

2.8.3. Principales diferencias del Derecho Internacional de los Derechos Humanos (DIDH) con otras ramas del Derecho.

El derecho internacional de los Derechos Humanos tiene cierta cercanía, pero importantes diferencias, con otras dos ramas del Derecho Internacional Público: el Derecho Internacional Humanitario y el Derecho Penal Internacional. Estos últimos no serán objeto de estudio en esta ocasión, solo se indicarán en este apartado algunos aspectos generales.[91]

Derecho internacional Humanitario

Es una de las ramas más antiguas del Derecho Internacional Público, fue conocido como Derecho de Guerra. El Comité de la Cruz Roja Internacional lo define como: "Un conjunto de normas que, por razones humanitarias, trata de limitar los efectos de efectos de los conflictos armados. [92]

[90] *CASTAÑEDA, Mireya, El Derecho Internacional de los Derechos Humanos y su recepción nacional, Comisión Nacional de los Derechos Humanos, México, 2018, en línea con dirección URL: http://appweb.cndh.org.mx/biblioteca/archivos/pdfs/Observaciones-Comite-ONU-vol-II.pdf consulta 10-03-2021.*

[91] *CASTAÑEDA Mireya, El Derecho Internacional de los Derechos Humanos y su recepción nacional, CNDH, 2018 formato electrónico.*

[92] *CASTAÑEDA, IBID.*

Luis Ángel Benavides distingue del Derecho Internacional Humanitario del Derecho internacional de los Derechos Humanos además de agregar al Derecho Internacional Penal, entre otros elementos, los siguientes;

Derecho Internacional Humanitario (DIH)	**Derecho Internacional de los Derechos Humanos (DIDH)**	**Derecho Internacional Penal (DIP)**
Se aplica en caso de conflicto armado. No admite restricciones ni suspensiones, y El órgano que principalmente lo promueve es el Comité de la Cruz Roja Internacional.	Se aplica en todo momento. En ciertos casos acepta restricciones y suspensiones. Existen diversos organismos nacionales regionales y universales para su protección.	Se concentra en determinar responsabilidades penales de personas por los crímenes más graves, como son el genocidio, los crímenes de guerra y lo crímenes de lesa humanidad.[93] El artículo 21 del Estatuto de la Corte Penal señala que la Corte aplicara e interpretara el derecho de manera compatible con los derechos humanos internacionalmente reconocidos, sin distinción alguna basada en motivos como el género; la edad, la raza, el color, la religión o el credo, la opinión pública de otra índole, el origen nacional, étnico o social: la posición económica, el nacimiento u otra condición.

El Derecho Penal Internacional en su artículo 21 del Estatuto de la Corte Penal señala que la Corte aplicara e interpretara el derecho de manera compatible con los derechos humanos internacionalmente reconocidos, sin distinción alguna basada en

[93] *CASTAÑEDA, IBID*.

motivos como el género; la edad, la raza, el color, la religión o el credo, la opinión pública de otra índole, el origen nacional, étnico o social: la posición económica, el nacimiento u otra condición.

Se apoya actualmente de instrumentos universales y regionales como el Pacto Internacional de Derechos Económicos, Sociales y Culturales y el Pacto Internacional de Derechos Civiles y Políticos. Existen diversos tratados especializados. A partir de las Declaraciones Universal y Americana de Derechos Humanos se desarrolló una serie de instrumentos internacionales en la materia, de carácter universal, como; (anexo)

2.9. Cuadro elaborado de los tratados relacionados o aplicables a los derechos humanos en los delitos cibernéticos.

De todos los documentos que existen solo se abordará los relacionados a los derechos humanos en los delitos cibernéticos, los derechos que se buscan preservar y proteger son la libertad de expresión, la privacidad y datos personales, derechos de autor y acceso al conocimiento, derecho a la intimidad y a la propia imagen, derecho al olvido en redes sociales, derecho a la información y a la educación digital, también un tema de suma importancia son los derechos de menores entre muchos otros, sin embargo solo en algunos países como es el caso de España, Estados Unidos y Chile se encuentran avanzados en el tema.

Convención internacional sobre la eliminación de todas las formas de discriminación racial.	Tiene 25 artículos y se divide en 3 partes.	El artículo que se encontró en común con los antes mencionados es; Art. 5 Referente al Derecho de opinión y la libertad de expresión.	4 de enero de 1969 entro en vigor.
Pacto Internacional de los Derechos Civiles y Políticos	Contiene 53 artículos.	Artículos: 17 nadie será atacado ilegalmente a su	23 de marzo de 1976 Status: 74

		honra y reputación. 18 Libertad de manifestar sus creencias, religión etc. 19. libertad de expresión 24 derechos del niño a no ser discriminado.	signatarios y 173 partes
Pacto Internacional sobre Derechos Económicos, Sociales y Culturales	Contiene 31 artículos	Articulo 13 Derecho a la educación	16 de diciembre de 1966 entro en vigor. Signatarios 45 partes 24
Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes	Contiene 45 artículos y se divide en 3 partes	Articulo 13 y 14 El Estado velara de cualquier tortura.	10 de diciembre de 1984 Signatarios 83 partes 169
Convención sobre los Derechos del Niño	Contiene 54 artículos Se divide en 3 partes.	Artículos: 12, Los Estados partes deben garantizar el derecho a expresar la libertad de expresión 13, Derecho del niño a la libertad de expresión 14, 15, 17, 19 y 37 libertad de	20 de noviembre de 1989 Signatarios 140 Partes 196

		pensamiento, conciencia y religión.	
Convención Internacional para la protección de todas las personas contra las desapariciones forzadas	Contiene 45 artículos y se divide en 3 partes	Artículo: 2, y 17 referente a la privación de la libertad y 24 reparación de la desaparición forzada.	23 de diciembre de 2010 Status: 98 signatarios, Partes: 62.
Protocolo facultativo de la Convención sobre Los Derechos del Niño relativo a la	Entró en vigor el 18 de enero de 2002. En esta convención si abarca el tema de la ciberdelincuencia que hay en internet. Contiene 17 artículos.	Artículos Art.1: Los Estados Partes prohibirán la venta de niños, la prostitución infantil y la pornografía infantil. Art.2: referido a la venta de niños,	176[94] países son parte de la Convención, pero 9 países no lo han ratificado. Cameron Islas Salomón Kenia Nauru

[94] *Lista de países ratificantes del tratado, Afganistán, Albania, Algeria, Andorra, Angola, Antigua, y Barbuda Arabia Saudita, Argentina, Armenia, Australia, Austria, Azerbaiyán, Alemania, Bahamas, Bahréin, Bangladesh, Bélgica, Belice, Benín, Bután, Bolivia, Bosnia y Herzegovina, Bostwana, Brasil, Brunei, Bulgaria, Burkina Faso, Burundi, Cabo Verde, Cambodia, Cameron, Canadá, Republica Africana Central, Chad, Chile, China, Colombia, Comoros, Congo, Costa Rica, Costa de Marfil, Croacia, Cuba, Chipre, República Checa, República de Corea, República del Congo, Dinamarca, Yibuti, Dominica, Republica, Ecuador, Egipto, El Salvador, Guinea Ecuatorial, Eritrea, España, Estonia, Esuatini, Etiopia, Finlandia, Francia, Gabón, Gambia, Georgia, Grecia, Granada, Guatemala, Guinea, Guinea Bissau, Guyana, Haití, Santa Sede, Honduras, Hungría, Islandia, India, Indonesia, Irán, Iraq, Irlanda, Israel, Italia, Jamaica, Japón, Jordana, Kazajistán, Kiribati, Kuwait, Kirguistán, Laos, Letonia, Libia, Líbano, Lesoto, Liechtenstein, Lituania, Luxemburgo, Macedonia del Norte, Madagascar, Malawi, Malasia, Maldivas, Mali, Malta, Islas Marshall, Mauritania, Mauricio, México, Micronesia, Mónaco, Mongolia, Montenegro, Moroco, Mozambique, Myanmar, Namibia, Nepal, Nueva Zelanda, Nicaragua, Nigeria, Noruega, Omán, Pakistán, Panamá, Paraguay, Perú, Filipinas, Polonia, Portugal, Qatar, Corea, Republica de Moldavia, Rumania, Rusia, Ruanda, Samoa, San Marino, Senegal, Serbia, Seychelles, Sierra Leona, Eslovaquia, Eslovenia, Islas Salomón, Suth África, Sudan, Sri Lanka, Sta. Lucia, San Vicente y las Granaditas, Palestina, Sudan, Suranime, Suecia, Suiza, Tayikistán, Tailandia, Timor este, Togo, Tunisia, Turkey, Turkmenistán, Uganda, Ucrania, Emiratos Árabes Unidos, Irlanda del Norte, Tanzania, Estados Unidos de América, Uruguay, Uzbequistan, Vanuatu, Venezuela, Vietnam, Yemen, Zimbabue.*

venta de niños, la prostitución infantil y la utilización de niños en la pornografía.		prostitución infantil y pornografía infantil. Art.3: referido a la explotación sexual, transferencia de órganos con fines de lucro, trabajo forzado Art.5: donde deben acatar los Estados parte esta Convención.	Fiji Ghana Irlanda Liberia Zambia

Cuadro que muestra todos los documentos relacionados a los derechos humanos en los delitos cibernéticos de manera puntual, la información basada en diversos artículos y libros que están citados en este trabajo.

2.9.1. Sistemas Regionales de Protección de los Derechos Humanos.

Existen 2 tipos de protección de los derechos humanos, nacional e internacional que a continuación se explicará:

1.- Sistema Universal de Protección de Derechos Humanos:

Este surge con la Declaración Universal en 1948 en el seno de la Organización de Naciones Unidas, se conforma de instrumentos, órganos de protección y mecanismos de tutela; Consejo de Derechos Humanos, Oficina del alto Comisionado de Naciones Unidas de Derechos Humanos y el Sistema de nueve tratados de Derechos Humanos, además de sus respectivos órganos o comités creados para su observancia.

2.- Sistema Regionales de Derechos Humanos

Surgen después de la Segunda Guerra Mundial y solo se han consolidado tres:

1. Europeo
2. Interamericano
3. Africano

Es el más antiguo y el que inspiró la creación de los otros sistemas regionales de protección. Surgió después de la Segunda Guerra Mundial, en el Consejo de Europa; su órgano no jurisdiccional es el Tribunal Europeo de Derechos Humanos (TEDH), ubicado en Estrasburgo.

El Consejo de Europa es el mecanismo de protección que están empleando, fue creado en 1949, el cual está integrado por 47 países miembros. Tiene como objetivo salvaguardar los derechos humanos y de las libertades fundamentales y buscar su mayor efectividad Tiene los siguientes órganos;

1. El Comité de ministros, órgano de decisión de la Organización
2. La Asamblea Parlamentaria, órgano impulsor de la cooperación europea.
3. El Congreso de los Poderes locales y Regionales, portavoz de las regiones y municipios de Europa.
4. La secretaria general

En cuanto a los instrumentos del Sistema Europeo se abordará en el siguiente apartado a mayor detalle.

El Sistema Africano de Derechos Humanos y de los Pueblos

Es un sistema regional no basta comparar los instrumentos e instituciones de cada uno, sino que hay que tomar en cuenta las características históricas, políticas, sociales y culturales de cada región. Hay una cuestión que incrementa la complejidad de este sistema es el insuficiente acercamiento a la cultura y las tradiciones africanas, por lo que solo se esquematizará el sistema.

Se integra por una Comisión y una Corte, la cual la comisión está integrada por 111 miembros, elige a su presidente y vicepresidente, los cuales duran dos años en el cargo y después podrán ser reelectos, además de un secretario y el personal necesario. La comisión africana puede presentar comunicados realizados por cualquier persona física o moral, los que podrían ser considerados por la Comisión siempre y cuando así lo decida la mayoría de miembros.

La Corte Africana fue creada por el Protocolo de la Carta Africana de Derechos Humanos y de los Pueblos en 2004, está integrada por 11 jueces de los Estados miembros de la Unión Africana, elegidos como su capacidad como juristas, su

reconocida practica judicial o académica y su experiencia en los derechos humanos y de los pueblos. Su mandato dura 6 años y puede ser reelectos una sola ocasión. La sede de la Corte se encuentra en Arusha, Tanzania.

El Sistema Interamericano de Derechos Humanos en México

Este sistema pertenece a México, la Organización de Estados Americanos tiene gran influencia en este sistema, sin embrago esta se abordará de manera profunda en el siguiente apartado de instrumentos de protección de los derechos humanos. Tiene sus fundamentos generales en el siglo XIX en los Congresos de Panamá.

Se integra por la Comisión Interamericana sobre Derechos humanos y la Corte Interamericana de los derechos Humanos, la Corte se encarga de supervisar el cumplimiento de sus fallos; para ello, los Estados deberán presentar un informe en el que las víctimas o sus representantes podrán realizar observaciones. La Corte no puede acudir al uso de la fuerza pública para el cumplimiento de sus funciones, solo puede acudir a la instancia política representada por la Asamblea General de la OEA. La Comisión Interamericana de Derechos Humanos; es un órgano de la OEA, fue creada para promover la observancia y la defensa de los derechos humanos y servir como órgano consultivo de la OEA en la materia, tiene su sede en Washington, D:C. se compone de 7 miembros que son elegidos por la Asamblea General de la Organización, también cuenta con una Secretaria Ejecutiva, compuesta por un secretario ejecutivo, un secretario ejecutivo adjunto y el personal profesional, técnico y administrativo necesario. Cabe destacar que tiene las siguientes funciones:

a) Estimular la conciencia de los derechos humanos en los pueblos de América.
b) Solicitar a los gobiernos de los Estados miembros para que adopten medidas progresivas en favor de los derechos humanos.
c) Formular recomendaciones a los Estados miembros para que adopten medidas progresivas a favor de los derechos humanos, y dentro de sus posibilidades, les prestara el asesoramiento que estos le soliciten.
d) Practicar visitas in loco[95], con anuencia o invitación del Estado.

[95] *Es una de las funciones más importantes de la Comisión, estas consisten en acudir a un Estado parte, con anuencia o invitación de su gobierno, para verificar la situación de los derechos humanos en ese territorio. La visita puede tener como propósito recabar información de organizaciones no*

2.9.2. Organismos e Instrumentos Internacionales de protección de los derechos humanos.

La oficina del Alto Comisionado para los Derechos Humanos (OACDH) se esfuerza por ofrecer el mejor asesoramiento experto y apoyo a los diversos mecanismos de supervisión de derechos humanos en el sistema de las Naciones Unidas: los órganos basados en la Carta de la ONU, incluido el Consejo de Derechos Humanos, el cual la mayoría recibe apoyo de la secretaria de la Subdivisión de tratados y del consejo de la OACDH.

Los órganos basados en la Carta de las Naciones Unidas	Los Órganos de tratados
• El Consejo de Derechos Humanos • Examen Periódico Universal • La Comisión de Derechos Humanos (sustituido por el Consejo de Derechos Humanos) • Los Procedimientos especiales de la Comisión de Derechos Humanos • Procedimiento de reclamación del Consejo de Derechos Humanos	Existen nueve órganos en virtud de tratados de derechos humanos que supervisan la aplicación de los principales tratados internacionales de los derechos humanos: • Comité de Derechos Humanos (CCPR) • Comité de Derechos Económicos, Sociales y Culturales (CESCR) • Comité para la Eliminación de la discriminación racial (CERD) • Comité para la eliminación de la Discriminación contra la Mujer (CEDAW) • Comité contra la Tortura (CAT) • Subcomité para la Prevención de la Tortura (SPT) • Comité de los Derechos del niño (CRC) • Comité para la Protección de los

gubernamentales, victimas, funcionarios, oficiales u otros actores para tener un cuadro más completo de la situación de ese país.

	Derechos de todos los Trabajadores Migratorios y de sus familiares. (CMW) • Comité sobre los derechos de las personas con discapacidad (CRPD) • Comité contra la desaparición forzada

Cuadro basado en los órganos de las Naciones Unidas y los órganos de los tratados, mostrando una comparación para su mayor entendimiento.[96]

En general, dentro del artículo 1º de dicha Carta se proclama la siguiente meta como uno de los "propósitos" de la ONU: lograr la cooperación internacional para la solución de problemas, internacionales de carácter económico, social, cultural, o humanitario: y fomentar y alentar el respeto por los derechos humanos y las libertades fundamentales de todos, sin distinción de raza, sexo, idioma o religión.
En tanto, las obligaciones básicas de la ONU y los Estados miembros para alcanzar estos propósitos se encuentran en los artículos 55 y 56 de la Carta, en los que se busca fomentar principalmente el respeto universal, la observancia de los derechos humanos y las libertades fundamentales, a través de diversos organismos que la misma ONU asigna como la Asamblea General y el Consejo Económico y Social.

La Carta Internacional de Los Derechos Humanos

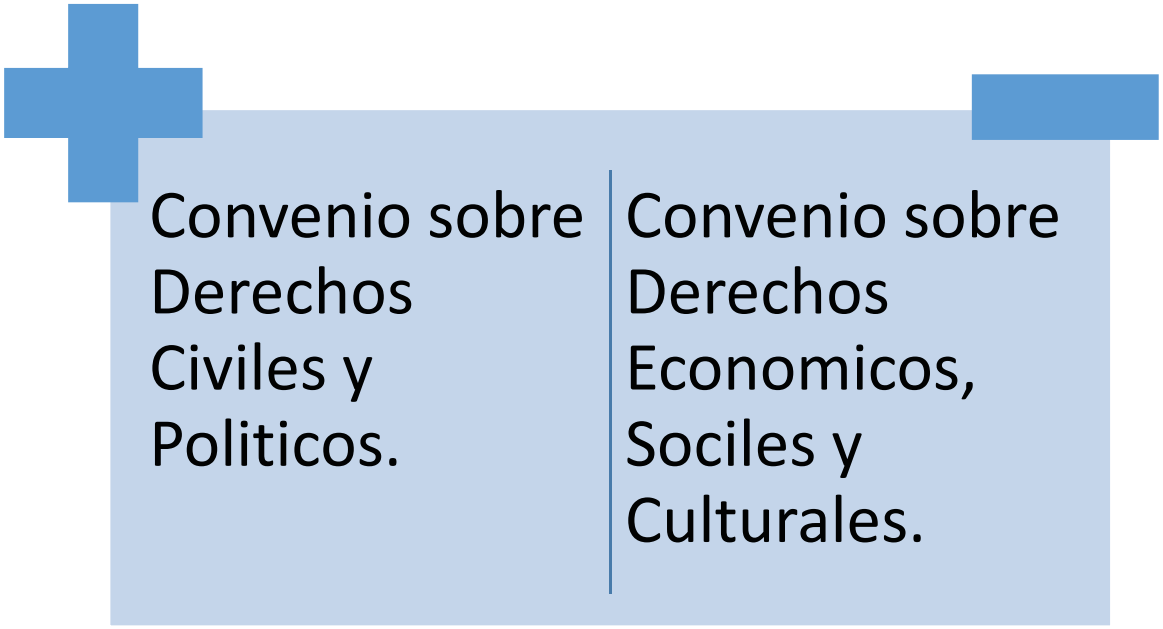
Esta carta, además de las disposiciones sobre derechos humanos de la Carta de la ONU, contiene:

1. La declaración como una interpretación autorizada de la Carta de la ONU, la cual enuncia muy detalladamente el significado de los términos "derechos Humanos" y "libertades fundamentales", a cuya promoción y observancia se han comprometido los Estados miembros, de acuerdo con la Carta. La declaración Universal se ha incorporado a la Carta como parte

[96] La Oficina del Alto Comisionado para los Derechos Humanos, en línea con dirección URL: https://acnudh.org/la-oficina/ consultado 15/04/21.

de la estructura constitucional de la comunidad mundial. La Declaración se ha convertido en un componente básico del derecho consuetudinario internacional, y de comprometer a todos los Estados, no solo a los miembros de las Naciones Unidas.

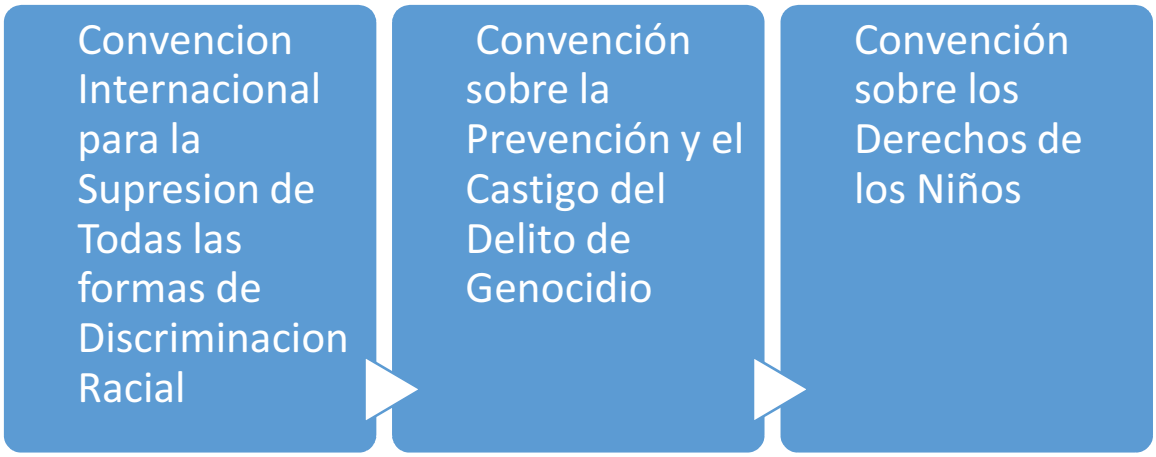
2. Los convenios internacionales sobre derechos humanos. Estos se refieren a los que podría describirse como “derechos de los pueblos” o colectivos, teniendo como disposiciones en común el derecho a la autodeterminación (artículo 1); el derecho a disponer libremente de sus recursos naturales; y que “en ningún caso se debe derivar a un pueblo de sus propios medios de subsistencia”.
3. También impide la discriminación basada en raza, color sexo, idioma, religión opinión política o de otro tipo, origen nacional o social, propiedad o nacimiento.
4. A pesar de sus similitudes, estos convenios se dividen en dos:



Existen otros tratados de la ONU sobre los derechos humanos

A lo largo de los años, la ONU ha formulado y promulgado diversos tratados para hacer frente a las nuevas problemáticas que día a día enfrenta el mundo con referencias a los nuevos tipos de violaciones de los derechos humanos, entre ellos la

discriminación racial, el apartheid en su momento, la discriminación de la mujer, la tortura, el genocidio, etc.



Oficina del Alto Comisionado para los Derechos Humanos (ACNUDH)

Es la principal entidad de las Naciones Unidas en el ámbito de los derechos humanos. La Asamblea General encomendó al Alto Comisionado y a su Oficina la misión de promover y proteger todos los derechos humanos de todas las personas. El programa de derechos humanos de las Naciones Unidas está orientado a velar por que la protección y el disfrute de los derechos humanos sean una realidad en la vida de todas las personas. El ACNUDH desempeña una función fundamental en la salvaguarda de los tres pilares interrelacionados de las Naciones Unidas: la paz y la seguridad, los derechos humanos y el desarrollo.[97]

La Oficina del ACNUDH forma parte de la Secretaría de las Naciones Unidas, cuenta con una plantilla de alrededor de 1.300 personas, su sede está en Ginebra y dispone además de una oficina en Nueva York. Su presencia sobre el terreno comprende oficinas regionales y nacionales/independientes. Además, el ACNUDH apoya a los componentes de derechos humanos de las misiones de paz de las Naciones Unidas

[97] *Alto Comisionado de las Naciones Unidas en línea con dirección URL: https://www.ohchr.org/sp/aboutus/Pages/WhoWeAre.aspx consultado 20-05-20*

o las oficinas políticas y emplea asesores en materia de derechos humanos para colaborar con los equipos de país de las Naciones Unidas.

Corte Interamericana de Derechos Humanos

En noviembre de 1969 se celebró en San José de Costa Rica la Conferencia Especializada Interamericana sobre Derechos Humanos. En ella, los delegados de los Estados Miembros de la Organización de los Estados Americanos redactaron la Convención Americana sobre Derechos Humanos, que entró en vigor el 18 de julio de 1978, al haber sido depositado el undécimo instrumento de ratificación por un Estado Miembro de la OEA. [98]

Es una institución jurídica autónoma de la OEA, cuyo objetivo principal es la aplicación y la interpretación de la Convención Americana sobre Derechos Humanos y de los otros tratados del Sistema Interamericanos.[99]

Con el fin de salvaguardar los derechos esenciales del hombre en el continente americano, la Convención instrumentó dos órganos competentes para conocer de las violaciones a los derechos humanos: La Comisión Interamericana de Derechos Humanos y la Corte Interamericana de Derechos Humanos. La primera había sido creada en 1959 e inició sus funciones en 1960, cuando el Consejo de la OEA aprobó su Estatuto y eligió sus primeros miembros.

Este tratado regional es obligatorio para aquellos Estados que lo ratifiquen o se adhieran a él y representa la culminación de un proceso que se inició a finales de la Segunda Guerra Mundial, cuando las naciones de América se reunieron en México y decidieron que una declaración sobre derechos humanos debería ser redactada,

---

[98] *Corte Interamericana de los Derechos Humanos en línea con dirección URL: http://www.corteidh.or.cr/historia.cfm consultado 23/05/2020*

[99] *Actualmente, veinticinco naciones americanas han ratificado o se han adherido a la Convención: Argentina, Barbados, Bolivia, Brasil, Colombia, Costa Rica, Chile, Dominica, Ecuador, El Salvador, Granada, Guatemala, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Suriname, Trinidad y Tobago, Uruguay y Venezuela. Trinidad y Tobago denunciaron la Convención Americana sobre Derechos Humanos, por comunicación dirigida al secretario general de la OEA, el 26 de mayo de 1998. Venezuela denunció la Convención Americana sobre Derechos Humanos, por comunicación dirigida al secretario general de la OEA, el 10 de septiembre de 2012.*[99]

para que pudiese ser eventualmente adoptada como convención. Tal declaración, la Declaración Americana de los Derechos y Deberes de la persona, fue aprobada por los Estados Miembros de la OEA en Bogotá, Colombia, en mayo de 1948.

El 30 de julio de 1980 la Corte Interamericana y el Gobierno de la República de Costa Rica firmaron un convenio, aprobado por la Asamblea Legislativa mediante Ley No. 6528 del 28 de octubre de 1980, por la cual se creó el Instituto Interamericano de Derechos Humanos. Bajo este Convenio se establece el Instituto como una entidad internacional autónoma, de naturaleza académica, dedicado a la enseñanza, investigación y promoción de los derechos humanos, con un enfoque multidisciplinario y con énfasis en los problemas de América. El Instituto, con sede también en San José, Costa Rica, trabaja en apoyo del sistema interamericano de protección internacional de los derechos humanos.

Organización de Estados Americanos (OEA)

Es una organización internacional panamericanista de ámbito regional y continental fue creada el 30 de abril de 1948, con la finalidad de ser un foro político para la toma de decisiones, el diálogo multilateral y la integración de América. La declaración de la organización dice que trabaja para fortalecer la paz, seguridad y consolidar la democracia, promover los derechos humanos, apoyar el desarrollo social y económico favoreciendo el crecimiento sostenible en América. En su accionar busca construir relaciones más fuertes entre las naciones y los pueblos del continente. Los idiomas oficiales de la organización son el español, el portugués, el inglés y el francés. Sus siglas en español son OEA y en inglés OAS (Organization of American States).[100]

También dentro del Sistema Interamericano se encuentra La Declaración Americana sobre Derechos y Deberes del Hombre, la Convención Americana sobre Derechos Humanos, otros Protocolos adicionales en Materia de Derechos Económicos, Sociales y Culturales, Protocolo a la Convención Americana sobre Derechos Humanos Relativo a la Abolición de la Pena de Muerte, Convención Interamericana para Prevenir, Sancionar y Erradicar la violencia contra la Mujer, también conocida

[100] *Historia de la OEA en línea con dirección URL: http://www.oas.org/es/acerca/nuestra_historia.asp consultado 28/07/2020.*

como “Convención de Belem Do Para”, Convención Interamericana sobre Desaparición Forzada de Personas, Convención Interamericana para la Eliminación de Todas las Formas de Discriminación contra las personas con Discapacidad, pero estos se ven reflejados en el otro subtema el cual mostrará su ratificación y adhesión y en el anexo (=) se proporciona información más amplia para su mayor entendimiento .

La Corte Europea de Derechos Humanos

La Corte Europea de Derechos Humanos, COEDH tiene sus orígenes en la implementación de la Convención Europea de Derechos del Hombre, CEDH, firmada el 4 de noviembre de 1950, CEDH. Se compone de 43 jueces, electos por seis años renovables por Asamblea. Cada juez es escogido de una terna presentados por cada Estado miembro.

La composición de la COEDH funciona en pleno, comités, cámaras y grandes cámaras. Si funciona en pleno le compete no realizar funciones contenciosas, elige al presidente de la COEDH, vicepresidentes y los “greffiers”. El comité es de tres jueces los cuales realizan el filtro de las demandas. Las cámaras se componen de siete jueces, el cual se integra también por el Estado que forma una de las partes del litigio. Y las grandes cámaras se componen de diecisiete jueces, el cual es presidido por el presidente de la COEDH, los presidentes de las cámaras y los jueces de los estados partes del litigio.

Contiene su propia Convención la cual se basa en la protección de los derechos humanos por lo que es un modelo desde el año de 1950 el cual lo convierte en un documento ejemplar a comparación de otros documentos clásicos del derecho internacional en relación con los límites de los derechos definidos especialmente con los derechos civiles y políticos. Su principal objetivo es que propone un control supranacional de actos y órganos que actúan generalmente a iniciativa de los individuos convirtiéndose en verdaderos sujetos de derecho internacional. Contiene 6 protocolos normativos, los cuales cada uno tiene temas diversos sobre la regulación de los derechos humanos.

Corte Penal Internacional

La Corte Penal Internacional (CPI) es el primer tribunal internacional de carácter permanente encargado de juzgar a los responsables de crímenes contra la humanidad, de genocidio, de crímenes de guerra y, tras la Conferencia de Revisión del Estatuto de Roma celebrada en Kampala en 2010, del crimen de agresión en el caso de aquellos países que hayan ratificado, como el caso de España, dicha revisión.[101]

La Corte Penal Internacional se compone de una presidencia con tres magistrados; la División judicial con tres secciones (Casos Preliminares, Primera Instancia y Apelaciones) a cargo de 18 jueces; la Oficina del Fiscal y el Registro. Actualmente ostenta el cargo de presidente el juez Chile Eboe-Osuji, de Nigeria, y el de fiscal, Fatuo Bensouda, de Gambia. Aproximadamente 700 personas de 90 países trabajan para la Corte, que cuenta con 6 oficinas sobre el terreno.[102]

Cabe mencionar que los crímenes de competencia de la Corte no prescriben. La Corte solo puede aplicar penas máximas de 30 años y de forma excepcional la cadena perpetua si es de extrema gravedad y si el caso lo amerita, pero jamás podrá condenar a muerte.[103] Esta instancia se considera una de las más importantes para la protección de los derechos humanos, la cual contiene diversos mecanismos para resolver conflictos.

2.9.3. El impacto de los tratados internacionales de derechos humanos.

La huella que ha dejado la aplicación de los derechos humanos en el mundo es de gran relevancia, pues se ha creado un movimiento que algunos autores como Huber Gayo señala que se da en un doble sentido: en primer término, ha producido una ampliación en cuanto al número y contenido de estos derechos, y además hay una evolución que punta hacia una mayor extensión y alcance, en la que se enriquece al

---

[101] *SANTOS Villareal, Mario, La Corte Penal Internacional, servicios de investigación y análisis, en línea con dirección URL: http://www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-10-10.pdf consultado 07-10.2020*

[102] *NACIONES UNIDAS, La Corte Penal Internacional, en línea con dirección URL: http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/NacionesUnidas/Paginas/CortePenalInternacional.aspx consultado 08-10-2020.*

[103] *Óp. Cit.*

mismo tiempo la protección del individuo, así como las esferas cívicas, sociales y culturales.[104]

Una segunda vertiente se presenta en los ámbitos territorial y personal de la protección jurídica de estos derechos, ya que puede iniciarse en una región circunscrita por ciertos sectores de la población, después se hace nacional y llega a tener carácter internacional público se filtró al ámbito Estatal interno. Ello ha implicado que el alcance de los derechos ya no sea exclusivo de cada Estado dentro de su jurisdicción interna, sino que abarca al derecho internacional público, y este a su vez se preocupa por los derechos internos, ya que ambos derechos parte de lo que se llama el bien común internacional.

Actualmente, la comunidad internacional considera que uno de los requisitos esenciales para la paz mundial radica en el respeto interno de los derechos humanos por parte de cada Estado.

Esta situación se ha propiciado bajo el influjo de una serie de documentos internacionales provenientes de la ONU o de los organismos regionales, que, a través de convenciones, pactos, tratados, etc. De alcance internacional comprometen a los Estados, y en muchas ocasiones a los organismos supranacionales, para su cumplimiento.

Pero hay algo todavía más importante, consistente en que en dichos documentos se han creado tribunales u organismos especiales para controlar a los sujetos obligados internacionalmente, sobre todo cuando se producen las violaciones a los derechos que en ellos se reconocen, lo que se ha logrado con bastante éxito.

Otro aspecto de extraordinaria importancia es que, por mediación de estos instrumentos, el hombre ha adquirido la calidad de sujeto del derecho internacional, no solo por el reconocimiento de sus derechos personales en la esfera internacional, sino sobre todo porque esta posibilitado para llevar denuncias o quejas ante organizaciones internacionales, para que estas juzguen si el Estado al que pertenecen si han lesionado sus derechos humanos.

Algunos documentos internacionales que en derechos humanos México ha suscrito, y que como consecuencia son parte del derecho interno mexicano.

---

[104] *S/A, Capítulo I, Los Derechos Humanos, en línea, con dirección URL: https://funceji.files.wordpress.com/2017/09/lectura-3.pdf, consultado 21/03/2021*

- Pacto internacional de Derechos Económicos, Sociales y Culturales. Nueva York, 16 de diciembre de 1996, publicado en el DOF el 12 de mayo de 1981.
- Convención Americana de los Derechos Humanos. San José de Costa Rica, 22 de noviembre de 1969, publicada en el DOF el 7 de mayo de 1981.
- Protocolo Adicional a la Convención Americana sobre Derechos Humanos en Materia de Derechos Económicos, Sociales y Culturales. San Salvador, 17 de noviembre de 1988, publicada en el DOF 1 de septiembre de 1998.
- Convenio (núm. 169) de la OIT sobre Pueblos Indígenas y Tribales en Países Independientes. Ginebra, 17 de junio de 1989, publicada en el DOF el 24 de enero de 1991.
- Convención sobre Derechos del Niño. Nueva York, 20 de noviembre de 1989, publicada en el DOF el 25 de enero de 1991
- Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belem Do Para, Brasil, 9 de junio de 1994, publicada 19 de enero de 1999.

Es importante señalar que el impacto de los tratados en los derechos humanos ha sido de manera positiva porque ha logrado que algunos países lleven a cabo la regulación, protección y prevención de los tratados que han firmado y que además les permite tener una mayor participación y desarrollo en el área cultural, jurídica, económica y política con otros países.

2.9.4. Tratados Internacionales en materia de Derechos Humanos ratificados por México.

México ha tenido una significativa participación como suscriptor de diferentes tratados, manteniéndose en ese sentido actualizado en materia de derechos humano en el campo internacional. En ellos imprime sus propios sellos bajo los principios fundamentales que históricamente ha enarbolado en su política exterior, como el de soberanía, libertad y justicia.

Instrumento	Sigla	Fecha de firma	Fecha de la ratificación, Fecha de adhesión (a), de sucesión (b)
Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes	CAT	18 mar 1985	23 ene 1986
Protocolo facultativo de la Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes	CAT-OP	23 sep 2003	11 abr 2005
Pacto Internacional de Derechos Civiles y Políticos	CCPR		23 mar 1981 (a)
Segundo Protocolo Facultativo del Pacto Internacional de Derechos Civiles y Políticos, destinado a abolir la pena de muerte	CCPR-OP2-DP		26 sep. 2007 (a)
Convención Internacional para la protección de todas las personas contra las desapariciones forzadas	CED	06 feb 2007	18 mar 2008
Convención sobre la eliminación de todas las formas de discriminación contra la mujer	CEDAW	17 jul 1980	23 mar 1981
Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial	CERD	01 nov 1966	20 feb 1975
Pacto Internacional de Derechos Económicos, Sociales y Culturales	CESCR		23 mar 1981 (a)
Convención internacional sobre la protección de los derechos de todos los	CMW	22 may 1991	08 mar 1999

Instrumento	Sigla	Fecha de firma	Fecha de la ratificación, Fecha de adhesión (a), de sucesión (b)
trabajadores migratorios y de sus familiares			
Convención sobre los Derechos del Niño	CRC	26 ene 1990	21 sep 1990
Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la participación de niños en los conflictos armados	CRC-OP-AC	07 sep 2000	15 mar 2002
Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía	CRC-OP-SC	07 sep. 2000	15 mar 2002
Convención sobre los derechos de las personas con discapacidad	CRPD	30 mar 2007	17 dic 2007

Cuadro elaborado para puntualizar los instrumentos internacionales firmados, ratificados por el Estado mexicano ejemplificados en una tabla con su respectiva fecha de firma, ratificación y/o adhesión.[105]

Este capítulo muestra la amplitud de lo general a lo particular sobre el tema de los derechos humanos, como ha sido su historia, su desarrollo a través del tiempo, sus diferencias internas, semejanzas de cada una y para cada estado; además de la relación con otras ramas que son importantes y que juegan en conjunto, también es importante conocer su naturaleza jurídica y principios, los cuales nos llevan a entender que instrumento utilizar o de qué manera solucionar cualquier situación que muestra la violación a algún derecho humano, que ahora ya se encuentra

[105] [105] *Oficina del Alto Comisionado, Naciones Unidas México, en línea con dirección URL:https://www.hchr.org.mx/index.php?option=com_content&view=article&id=452&Itemid=250 consultado 01-05-2020.*

clasificados en diversas áreas para poder identificarlos. Cabe resaltar que los tratados son una garantía de que sean respetados los derechos humanos y castigarlos a quienes no lo cumplan.

Los derechos humanos han tomado una estructura con el paso del tiempo y gracias a sus características y principios los convierten universales, irrevocables, interdependientes y progresivos.

También decidí plasmar las ideas o perspectiva filosófica de los derechos humanos para mostrar una mejor conciencia y dar a conocer que los derechos humanos no solo se trata de documentos o cuestiones jurídicas sino también son cuestiones del ser y que desde nuestro interior podemos crear grandes cambios como sociedad.

Las generaciones muestran el gran desafío y desarrollo que presentan los derechos humanos a través de las épocas o procesos históricos de las sociedades, como el ultimo acontecimiento que estamos viviendo en pleno 2020, con la pandemia del COVID-19 el cual ha dado un giro de 360 grados y el desafío y exigencia sobre tener un enfoque más amplio sobre los derechos humanos, debido a que hoy en día la sociedad se encuentra comunicado por medio de la tecnología y el internet, lo cual da pie a que se desencadenen más situaciones que aún no tengan regulación .

Los sistemas regionales son un tema primordial para poder comprender la funcionalidad que tiene cada región en cuanto los derechos humanos,

Los Organismos Internacionales fungen una parte muy importante como instituciones guardianas de preservar, proteger y combatir a los derechos humanos, además de tener una enorme tarea de educar a la sociedad internacional sobre los derechos humanos, por medio de políticas públicas, campañas que podrían ser transmitidas por todos los medios de comunicación existentes.

En el apartado de los derechos humanos y el ciberespacio, aún queda mucho por crear, porque aunque haya material e instrumentos para su regulación, combate y prevención sigue siendo insuficientes para sancionar y/o perseguir el delito a quienes los cometen, sin embargo en el siguiente capítulo abordaremos todo lo relacionado con los delitos cibernéticos su funcionamiento, sus características, su naturaleza y su alto desarrollo y operatividad a nivel mundial, también se mencionará algunos casos.

La situación en México en este tema actualmente se tiene un panorama desfavorable de acuerdo a las recomendaciones emitidas por la Comisión Nacional de Derechos Humanos, el cual recalca que el sistema de justicia penal pese a la adopción de leyes que garanticen y reparen el daño no han sido empleadas siguen siendo insuficientes para poder combatir todas las situaciones de violencia desde las desapariciones forzadas, hasta los temas principales de este trabajo como; la libertad de expresión, donde decenas de periodistas han desaparecido, en cuanto a los derechos de las mujeres y niños. También existen otros temas como el problema de los migrantes, de los abusos que cometen la Guardia Nacional. Se requiere que se aplique con mayor vigor castigos o soluciones.

Hablar sobre el tema de derechos humanos suele ser complicado para muchas naciones debido a que no todos tienen el mismo enfoque; histórico, cultural, político y económico. Es claro que a diario los organismos e instituciones encargadas por velar a los derechos humanos no han tenido éxito debido al cambio constante de la sociedad que cada vez exige nuevos mecanismos de protección. Otra cuestión que es muy clara es que a pesar de que los derechos son considerados universales aun no son posibles en su totalidad, debido al desarrollo de cada país y los tratados a los que se han adherido.

Capítulo 3. Análisis de los Delitos Cibernéticos Internacionales: clasificación y contenido

3. 1. Definición de los delitos cibernéticos internacionales.

Definir el delito desde cualquier perspectiva suele ser complicado, debido que al tratar de aplicar el crimen transnacional y la delincuencia organizada de manera uniforme a nivel internacional es imposible debido a que cada Estado tiene su derecho constitucional y disposiciones legales internas que a su vez podría llegar a discrepar entre sí. No obstante, el desarrollo que ha tenido es significativo tomando en cuenta la globalización lo cual ha sido favorable para la masificación y la clasificación de los delitos y en especial a los delitos cibernéticos internacionales.[106]

Existen diversas definiciones de los delitos cibernéticos internacionales por lo que plasmaremos algunas definiciones de autores que a mi criterio son de suma importancia para poder comprender el tema.

Los delitos cibernéticos internacionales se conocen también como delitos informáticos, delitos de internet, ciberdelitos, delitos electrónicos, delitos relacionados con las computadoras, entre otros son aquellas acciones negativas e ilícitas que pueden perjudicar a cualquier persona por medio de una computadora o dispositivo que tenga acceso a internet.

En los países anglosajones se maneja el término del cibercrimen el cual hace alusión a la cibernética y el crimen, es un término que se encuentra en debate en cuanto a la legislación de muchos países del mundo se refiere incluyendo a México.[107]

Parker define a los delitos cibernéticos como todo acto intencional asociado de una manera u otra a los computadores; en los cuales la victima ha o habría podido sufrir una perdida y cuyo autor ha o habría podido obtener un beneficio.[108]

Marcelo Huerta y Claudio Líbano nos ofrecen una definición más precisa, como "todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, tratándose de

---

[106] *AUCURIO del Pino Santiago, Delitos cibernéticos, en línea con dirección url: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf consulta 10-07-17*

[107] *MONTOYA, Piña Javier Omar, Delitos Federales cometidos a través de medios informáticos, editorial flores, México, 2015.*

[108] *AUCURIO del Pino Santiago, Óp. Cit. p. 11*

hechos aislados o de una serie de ellos, cometidas contra personas naturales o jurídicas realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio a la víctima a través de atentados a la sana técnica informática, lo cual, generalmente producirá de manera colateral lesiones a distintos.[109]

Para Julio Téllez Valdez define a los delitos informáticos como aquellas actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin o a las conductas típicas, antijurídicas y culpables".[110]

Para Jorge Esteban Cassou Ruiz considera a los delitos informáticos como toda aquella conducta ilícita susceptible de ser sancionadas por el derecho penal, consistente en el uso indebido de cualquier medio informático.[111]

La Organización para la Cooperación Económica y el Desarrollo los define como: "cualquier conducta ilegal, no ética, no autorizada, que involucra el procesamiento no automatizado de datos y/o transmisión de datos"[112]

El delito cibernético es una forma emergente del crimen transnacional y con mayor desarrollo con la ayuda de internet y la forzosa aceleración de la digitalización debido a la pandemia del covid-19 por lo que ahora ha tomado una reconfiguración

El delito cibernético ha asumido actividades criminales que en primera instancia los países han tratado de encuadrar figuras públicas de carácter tradicional, tales como robos o hurtos, fraudes o falsificaciones, perjuicios o estafas, sabotaje, pornografía infantil, ciberacoso, etcétera que a su vez generan malestares a los cibernautas y en este caso violaciones a sus derechos humanos. Por lo que es de suma importancia conocer las técnicas informáticas que ha creado nuevas posibilidades sobre el uso indebido de las computadoras lo que ha propiciado una exhaustiva regulación por parte del derecho.[113]

---

[109] *MONTOYA, Piña Javier Omar, Delitos Federales cometidos a través de medios informáticos, editorial flores, México, 2015*

[110] *AUCURIO del Pino Santiago, Óp. Cit. p. 11*

[111] *RUIZ, Cassou Jorge Esteban, Delitos informáticos en México, 2009 Ciudad de México en línea con dirección URL: ,https://revistascolaboracion.juridicas.unam.mx/index.php/judicatura/article/view/32260/29257 consultado 14-03-2021.*

[112] *GRANADOS Delgado María Lourdes, Articulo, Delitos informáticos delitos electrónicos en línea con dirección URL: http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf consultado 13-03-2020*

[113] *BERNAL*, Écija Álvaro, *Ciberespacio un mundo sin le*y, en línea con dirección URL: http://ciberderecho.com/El_ciberespacio_un_mundo_sin_ley.pdf consultado 14-03-2019

3.2. Características de los Delitos Cibernéticos.

De acuerdo con Julio Téllez Valdez nos proporciona amplias características sobre los delitos cibernéticos: [114]

- Son conductas criminales de cuello blanco, en tanto que solo un determinado número de personas con ciertos conocimientos hablando en términos técnicos pueden llegar a cometerlas.
- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se encuentra trabajando.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones de sistemas tecnológicos y económicos.
- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos que se presentan a nivel mundial y local y pocas denuncias, y de todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto es por su mismo carácter técnico.
- En su mayoría son imprudenciales y no necesariamente se cometen con intención.
- Ofrecen facilidad para su comisión a los menores de edad.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

[114] *TELLEZ* Valdés Julio, *Derecho Informático*, 1991, UNAM, México Porrúa en línea con dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/1/313/1.pdf consultado 10-07-2017

3.3. Clasificación de los delitos cibernéticos.

Se clasifican en base a dos criterios:

Como instrumento (medio):

En esta clasificación se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de los delitos convencionales (hurto, homicidio, fraude, etc.)
- Lectura, sustracción o copiada de información confidencial.
- Modificación de datos tanto a la entrada como a la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan “interrupciones” en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a varias informaciones en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso[115].

Como fin u objetivo

En esta clasificación, se enmarcan las conductas criminales que van dirigidas contra los computadores, accesorios o programas como entidad física, ejemplo:

- Programación de instrucciones que producen un bloqueo total al sistema.

[115] *Se refiere al procesamiento de datos provenientes de terminales o de la unidad central*.

- Destrucción de programas por cualquier método.
- Daño a la memoria.
- Atentado físico contra la maquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pagos de rescate etc.)

Otra clasificación de los delitos cibernéticos, en este caso más precisa, es la que encontramos en el “Convenio de Ciberdelincuencia del Consejo de Europa” ratificado en el año 2001 por el conjunto de países de la Unión Europea. En este convenio se habla de cuatro grupos de delitos informáticos o delitos cibernéticos:
Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.

Delitos informáticos:

- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

Delitos relacionados con el contenido:

- Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines, como la copia y distribución de programas informáticos, o la piratería informática.

3.4. Tipos de delitos cibernéticos internacionales.

Los delitos que se ven favorecidos por el uso de internet, aun cuando no son "ciberdelitos" podemos decir que el control en los contenidos informáticos es de vital importancia para garantizar el derecho a que los usuarios utilicen el internet con toda seguridad.

La Organización de las Naciones Unidas (ONU), define tres tipos de delitos cibernéticos:

Fraudes cometidos mediante manipulación de computadoras.

Manipulación de datos de entrada.

Daños o modificaciones de programas o datos computarizados.

Los Fraudes cometidos mediante manipulación de computadoras pueden clasificarse en:

- Manipulación de los datos de entrada o sustracción de datos.
- La manipulación de los datos de salida.
- Fraude efectuado por manipulación informática: también nombrado "Técnica del salchichón", aprovecha las interacciones automáticas de los procesos de cómputo.
- Los fraudes cometidos mediante la manipulación de los datos de entrada:

Como objeto: alteración de los documentos digitales.

Como instrumento: uso de las computadoras para falsificar documentos de uso comercial.

- Los daños o modificaciones de programas o datos computarizados:

Sabotaje informático: acción de eliminar o modificar funciones o datos en una computadora sin autorización, para obstaculizar su correcto funcionamiento.

- Acceso no autorizado a servicios y sistemas informáticos.
- Reproducción no autorizada de programas informáticos de protección legal.

Este tipo de delitos se caracterizan por la dificultad que entraña su descubrimiento, persecución y prueba, debido a la propia vulnerabilidad de los sistemas y al elevado

nivel de especialización que tienen los sujetos que los perpetran a tal grado de catalogarlos como delitos de cuello blanco.[116]

Existen otros delitos que no son propiamente delitos informáticos sino que son favorecidos por el uso de internet y de los diferentes sistemas de cómputo que afectan a las personas: tal es el caso de la pornografía infantil, el cual es un delito que vulnera los derechos de los menores de edad o la extorsión o chantaje que mediante el uso de internet pueden cometerse en cierta medida con mayor facilidad, es decir que hay delitos claramente tipificados en los que se ha hecho uso de internet para ser realizados, pero podríamos hablar del caso contrario, de delitos cometidos a través de internet que no tienen relación directa con los delitos normalmente tipificados en los códigos penales.

"De acuerdo con el departamento de justicia de los Estados Unidos, los delitos relacionados con sistemas de cómputo pueden ser clasificadas de acuerdo con la actividad o el rol de los mismos en un determinado delito. Como ya mencionamos anteriormente; una computadora puede ser el objeto de un delito […] un sistema de cómputo puede ser el sujeto de un delito. Dentro de esta categoría se encuentran todos aquellos delitos en los cuales no existe una analogía de un delito tradicional y para los cuales se requiere la aplicación de una legislación especial.[117]

Una de las compañías especializadas en seguridad informática más prestigiosas del mundo, Symantec clasifica en dos a los delitos cibernéticos:

Delitos cibernéticos de tipo I. Son todos aquellos que tienen lugar una única vez respecto a la misma víctima. Con relativa frecuencia, aunque no siempre, algún tipo de programa malicioso para registrar la actividad de la víctima aprovechando los fallos de seguridad del navegador, del propio sistema operativo… Forman parte de este tipo de delitos el phishing (envío de un correo electrónico falso que trata de engañar al usuario para que éste revele sus datos personales, bancarios, credenciales de acceso, etcétera), la instalación de un malware en un ordenador

[116] *MENENDEZ, Mato Juan Carlos, Derecho e Informática, ética y legislación, editorial Bosch Editor, 2014. p. 319.*

[117] *LÓPEZ Calvo Pedro, Derechos Humanos, Victimología, Terrorismo y sus Diversas Modalidades Delictivas, capítulo V, pág. 440.*

para espiar a la víctima, la usurpación de identidad, el fraude, la piratería, etcétera. Es decir, para cometer el delito sólo se interactúa con la víctima en una ocasión.[118]

Delitos cibernéticos de tipo II. En este caso, la interacción con la víctima se produce en repetidas ocasiones, por ejemplo, en casos de chantaje, extorsión, acoso, espionaje industrial, planificación de actividades terroristas, etcétera.[119]

A pesar de estas clasificaciones que se mencionan, se abordará el tema describiendo uno por uno para poder tener mayor conocimiento e importancia sobre el tema.

3.4.1. Delito cibernético del Spam.

Hace referencia a los mensajes no solicitados que son enviados en cantidades masivas y recibidas en las direcciones de correo electrónico, sin existir relación previa alguna entre el iniciador del mensaje y el destinatario del mismo y normalmente sin el consentimiento expreso del mismo.[120]

Actualmente, se define como SPAM o correo basura al conjunto de mensajes publicitarios que son enviados de forma masiva a un número elevado de usuarios al mismo tiempo, sin ser solicitados y que perjudican o interfieren con el resto de mensajes recibidos. Generalmente son recibidos por correo electrónico, pero también a través de otros medios, como el teléfono, la mensajería electrónica o actualmente las redes sociales.[121]

Los mensajes considerados como SPAM tienen una serie de elementos característicos:

Generalmente tienen un contenido publicitario. Suelen tener asuntos llamativos, para captar la atención del destinatario. La dirección del remitente suele ser desconocida e incluso en muchos casos falsificada. Los mensajes generalmente no permiten ser contestados. Y en el caso de que provengan de direcciones válidas, no sirve de nada

---

[118] *ALFOCEA J. El delito cibernético, concepto y clasificaciones, en línea con dirección URL: http://legadoo.com/legal/index.php/abogados-discapacidad/delito-cibernetico-concepto-clasificaciones/ consultado 21-05-2021.*

[119] *ALFOCEA J. Óp. Cit.*

[120] *LOPEZ, Óp. Cit. p. 441.*

[121] *SERVICIO DE INFORMATICA, Universidad de Jaén, en línea con dirección URL: https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%201.%20SPAM.pdf consultado 21-10-2020*

contestar a estos mensajes de SPAM. Generalmente las respuestas serán dirigidas a usuarios que no tienen nada que ver con ellos.[122]

Las medidas y soluciones anti-SPAM han evolucionado considerablemente para intentar detener esta plaga, pero, aun así, los spammers no dejan de adaptarse e inventan nuevos sistemas para intentar que el SPAM sea efectivo, evitando así las distintas soluciones anti-spam.[123]

Las técnicas empleadas generalmente de los spammers con el principal objetivo es el de conseguir el mayor número de direcciones de correo válidas y operativas. Para ello, utilizan numerosas y variadas técnicas, algunas de ellas muy sofisticadas: Usan listas de correo: los spammers consigue darse de alta en numerosas listas de correo y mediante diferentes técnicas consiguen las direcciones de correo electrónico de todos los usuarios pertenecientes a cada una de esas listas. [124]

Hacen uso de programas específicos de rastreo automático que recorren Internet en busca de direcciones de correo a partir de numerosas fuentes (páginas web, foros de discusión, blogs, etc.).

A partir de la compra de extensas bases de datos de direcciones de correo comercializadas por particulares o empresas. En el caso de España, esta práctica incumple la actual Ley Orgánica de Protección de Datos de carácter personal (LOPD de 15/1999 del 13 de diciembre).

Una técnica muy habitual es la generación de direcciones de correo artificiales a partir de un dominio de Internet, cambiando el nombre de usuario y enviando mensajes a las mismas. Estos ataques se suelen hacer mediante diccionarios de palabras o directamente mediante fuerza bruta, probando numerosas combinaciones de letras y números de forma automática. El servidor de correo electrónico perteneciente a ese dominio devolverá mensajes de error por cada una de las direcciones no válidas. Así, los spammers averiguan cuáles de las direcciones generadas son reales.[125]

A partir de correos electrónicos con chistes, cadenas y adjuntos que se suelen reenviar sin ocultar las direcciones (sin usar el campo Bcc), y que pueden llegar a

[122] Op. Cit.
[123] Op. Cit.
[124] Op. Cit.
[125] *Op. Cit.*

acumular docenas de direcciones en el cuerpo del mensaje, pudiendo ser capturadas por un troyano o por un usuario malicioso.

Spam a través de ventanas emergentes (pop-ups). Se produce cuando estamos navegando por Internet y el navegador nos empieza a lanzar ventanas secundarias con mensajes, publicitarios o no, que poco o nada tienen que ver con la página que estamos visitando.[126]

Hoaxes. Son mensajes de correo electrónico, generalmente distribuidos en cadena, con contenido falso o engañoso. Algunos de estos mensajes están relacionados con virus falsos, fórmulas para ganar rápidamente una enorme cantidad de dinero, falsos mensajes de solidaridad y timos de lo más variado.[127]

A partir de la entrada ilegal en servidores lo que permite a los atacantes descargar cuentas de correo electrónico, una vez comprometidos los servidores.

Mediante troyanos y ordenadores zombis pertenecientes a botnets. Desde hace un tiempo se ha extendido el uso de una técnica consistente en la creación de virus y troyanos que se expanden masivamente por ordenadores que no están protegidos adecuadamente. Estos ordenadores infectados son utilizados por los spammers como "ordenadores zombis", que envían correo basura a sus órdenes, pudiendo incluso rastrear los discos duros o clientes de correo en busca de más direcciones. Esto puede causar perjuicios al usuario que ignora que está infectado (no tiene por qué notar nada extraño), al ser identificado como spammer por los servidores a los que envía spam sin saberlo, lo que puede conducir a que se le deniegue el acceso a determinadas páginas o servicios. Actualmente, se calcula que el 40% de los mensajes no deseados se envían de esta forma.[128]

Servidores de correo mal configurados. En concreto los servidores configurados como open relays (reencaminadores abiertos) no necesitan un usuario y contraseña para que sean utilizados para el envío de correos electrónicos, por lo que cualquier puede hacer uso de ellos para el envío. Existen diferentes bases de datos públicas

[126] *Op. Cit.*
[127] *Op. Cit.*
[128] Op. Cit.

que almacenan listas de servidores configurados como open relays que permiten que los spammers hagan uso de ellos.[129]

Existen medidas y recomendaciones para combatir el spam a pesar de que no existen técnicas infalibles para protegerse del correo basura, hay diferentes técnicas que podemos poner en práctica para restringir la disponibilidad de nuestras direcciones de correo electrónico, así como la prevención y la reducción de los mensajes de tipo SPAM recibidos en la bandeja de entrada de nuestro cliente de correo electrónico:[130]

- ✓ Desconfiar de los correos de remitentes desconocidos.
- ✓ No abrir ficheros adjuntos en curso.
- ✓ Utilizar el filtro anti-spam
- ✓ Ocultación de direcciones
- ✓ No responder nunca al spam
- ✓ Ser cautos al rellenar formularios en páginas web.
- ✓ Desactivar HTML en el correo electrónico
- ✓ Disponer de direcciones de correo electrónico alternativas
- ✓ Se debe tener demasiada precaución en cuanto a los mecanismos que ofrecen para el cambio de contraseñas en muchos sitios webs.
- ✓ No facilitar la cuenta de correo a desconocidos.
- ✓ Cuando reenvíes mensajes a múltiples destinatarios utiliza siempre la copia oculta (CCO ó BCC) para introducir las direcciones de los destinatarios.

3.4.2. Delito cibernético del Phishing.

El significado varía dependiendo al país inclusive es utilizado como sinónimo de robo de identidad. El Anti-Phishing Group, lo define como un mecanismo que emplea tantas técnicas de ingeniería social y técnicas evasivas para robar la identidad, los datos personales y la información financiera de los consumidores.

Este tipo de fraude se lleva a cabo por medio de correos electrónicos o de ventanas emergentes, el robo de identidad es uno de los ciberdelitos que más ha aumentado habitualmente, la mayoría de las victimas ha sido atacadas con secuestros de sus

[129] *Op. Cit.*
[130] *Op.cit.*

tarjetas de tarjetas de crédito, pero para muchas otras la situación es peor, porque han solicitado hipotecas a nombres de las víctimas, por lo que se ha desencadenado una red fraudulenta que cada vez se vuelve más fuerte y es difícil de poder frenarla.[131]

Las características más comunes que tiene el phishing son las siguientes:[132]

- Problemas de carácter técnico.

• Recientes detecciones de fraude y urgente incremento del nivel de seguridad.
• Nuevas recomendaciones de seguridad para prevención del fraude.
• Cambios en la política de seguridad de la entidad.
• Promoción de nuevos productos.
• Premios, regalos o ingresos económicos inesperados.
• Accesos o usos anómalos a tu cuenta.
• Inminente desactivación del servicio.
• Falsas ofertas de empleo.

Existe una gran cantidad de hacer phishing y en este cuadro se mostrarán de manera resumida;

Spear phishing o phishing segmentado	Funciona atacando a grupos determinados, es decir que busca a grupos vulnerables a diferencia de la modalidad anterior.
Pasarelas de pago online (PayPal, MasterCard, Visa, etc.)	Excusas utilizadas para engañar al usuario: cambio en la normativa del servicio, cierre incorrecto de la sesión del usuario, mejoras en las medidas de seguridad, detectada intrusión en sus sistemas de seguridad, etc. Con el objetivo al igual que en el caso del phishing anterior, principalmente robar datos bancarios
Redes sociales (Facebook, Twitter,	Excusas utilizadas para engañar al usuario: alguien te ha enviado un mensaje privado, se han detectado conexiones

[131] *AUCURIO Del Pino Santiago, Delitos informáticos, en línea con dirección URL: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf consulta 19-10-2020*

[132] *OFICINA DE SEGURIDAD INTERNAUTA, en línea con dirección URL: https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen consultado 19-10-2020.*

Tuenti, Instagram, LinkedIn, etc.)	extrañas en la cuenta, por motivos de seguridad es necesario que se cambien las claves, etc. Con el objetivo de robar cuentas de usuarios, obtener sus datos privados y suplantar su identidad.
Páginas de compra/venta y subastas (Amazon, eBay, etc.)	Excusas utilizadas para engañar al usuario: problemas en la cuenta del usuario, detectados movimientos sospechosos, actualización de las condiciones del uso del servicio, etc. Con el objetivo robar cuentas de usuarios y estafar económicamente al usuario.
Juegos online	Excusas utilizadas para engañar al usuario: fallos de seguridad en la plataforma del juego, problemas en la cuenta del usuario. El objetivo de robar cuentas, datos privados, bancarios y suplantar la identidad de los usuarios.
Soporte técnico y de ayuda (helpdesk) de empresas y servicios (¡Outlook, Yahoo!!, Apple, Gmail, etc.)	Excusas utilizadas para engañar al usuario: confirmación de la cuenta de usuario, eliminación de cuentas inactivas, detectada actividad sospechosa en la cuenta, se ha superado el límite de capacidad de la cuenta, etc.
Servicios de almacenamiento en la nube (Google Drive, Dropbox, etc.)	Existe una serie de tipos de phishing, los cuales se mencionarán de manera breve y general; Objetivo: Conseguir cuentas de distintos servicios de usuarios, obtener información privada.
Phishing a servicios o empresas públicas	Excusas utilizadas para engañar al usuario: información sobre una notificación, una multa, con el objetivo: infectar el ordenador, robar datos privados, bancarios y estafar económicamente al usuario.
	Excusas utilizadas para engañar al usuario: el paquete enviado no ha podido ser entregado, tienes un paquete esperando, información sobre el seguimiento de un pedido, etc. Con el objetivo; infectar ordenadores, robar datos privados y bancarios de los usuarios.

Phishing a servicios de mensajería	Excusas utilizadas para engañar al usuario: el paquete enviado no ha podido ser entregado, tienes un paquete esperando, información sobre el seguimiento de un pedido, etc. Con el objetivo; infectar ordenadores, robar datos privados y bancarios de los usuarios.
Falsas ofertas de empleo.	Excusas utilizadas para engañar al usuario: puestos de trabajo, con el objetivo de robar datos privados que pueden ser utilizados posteriormente con distintos fines fraudulentos. Existen ocho falsas ofertas de empleo más utilizadas por ciberdelincuentes en Internet; trabaja desde casa, haciendo tareas manuales, oferta de trabaja donde tienes que llamar para pedir informes, rellenar encuestas, trabajo fácil, solo hay que realizar transferencias bancarias, trabajar en el extranjero, trabajar invirtiendo algo, empieza a trabajar con tan solo facilitar tus datos. Las empresas y servicios están invirtiendo muchos esfuerzos en mejorar sus sistemas de seguridad. La práctica del phishing no se debe asociar a problemas de seguridad por su parte, se trata de una técnica que utilizan los ciberdelincuentes, empleando la imagen de empresas y servicios conocidos como gancho para propagarse. Debido a la cantidad de problemas que genera este fraude entre los usuarios, la mayoría de empresas y servicios luchan contra el phishing y alertan sobre él en su página web.[133]

Cuadro elaborado donde muestra las ocho maneras de hacer phishing, información basada de la siguiente página.[134]

Hay una serie de recomendaciones para protegerte del phishing, usar los filtros antispam que facilitan los clientes de correo electrónico. También puedes ayudarte

[133] *Lista de 8 maneras de hacer phishing en línea con dirección URL: https://www.osi.es/es/actualidad/blog/2014/03/04/las-8-falsas-ofertas-de-empleo-mas-utilizadas-por-ciberdelincuentes-en-in consultado 19-10-2020.*

[134] *Lista de 8 maneras de hacer phishing en línea con dirección URL: https://www.osi.es/es/actualidad/blog/2014/03/04/las-8-falsas-ofertas-de-empleo-mas-utilizadas-por-ciberdelincuentes-en-in consultado 19-10-2020.*

de herramientas específicas que bloquean el correo no deseado. Configura la opción anti phishing que incorporan los navegadores:

1 - El Filtro Smart creen de Internet Explorer ayuda a identificar sitios web notificados como de suplantación de identidad (phishing) o de malware

2 - Protección contra el Malware y el Phishing en Firefox

3 - Protección contra phishing y software malicioso en Google Chrome

4 - Evitar la suplantación de identidad (phishing) en Safari

Verifica la legitimidad del sitio web. Fíjate siempre en la URL para asegurarte que estás en la página web oficial en la que querías estar y no se trata de una web que la está suplantando.

3.4.3. Delito cibernético de Robo de identidad.

El robo de identidad surgió por el interés de la individualización del ser humano en la sociedad de las masas. De acuerdo a la visión del Derecho, "la identidad hace referencia a un conjunto de características, datos o informaciones que permiten individualizar una persona". Este conjunto de tributos de cada una de las singulares personas permite el desarrollo de las relaciones sociales y de los efectos jurídicos que las mismas puedan producir.[135]

La definición sobre el robo de identidad depende ampliamente del marco jurídico respectivo de cada país. El término se refiere a la descripción de la información personal de un individuo, tal y como la información identificable, financiera o médica, ha sido obtenida y utilizada sin su consentimiento y con el propósito de cometer una actividad ilícita fraudulenta.

Actualmente internet ha dado pie a que surja la identidad electrónica o identidad digital, que fundamentalmente se encuentra constituida por datos personales sensibles que pueden incluir claves de acceso a cuentas bancarias o redes, mediante los cuales las personas se comunican u operan en redes informáticas o telemáticas y cuya circulación transfronteriza es potencialmente peligrosa ante su posible apropiamiento no autorizado. De igual forma existes varias vertientes de

[135] *ROMERO Flores Rodolfo, El robo de usurpación de identidad por medios informáticos o telemáticos: su tratamiento jurídico penal. en línea con dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/6/2958/20.pdf consultado 19-10-2020.*

identidad tales como; la identidad genética o biológica, la identidad sexual, la identidad cultural, entre otras, pero solo nos enfocaremos en la de la usurpación de identidad por medio de la tecnología.[136]

También se le conoce “robo de identidad”, “usurpación de identidad”, “suplantación de identidad”, “falsificación de la identidad y su uso indebido” de acuerdo con investigaciones internacionales por el Consejo Económico y Social, (ECOSOC) de la Organización de las Naciones Unidas, la Unión Europea, y la Organización para la Cooperación y el Desarrollo Económico (OCDE), es el delito de más rápido crecimiento sin que existan acciones legislativas, concretas y políticas públicas acertadas para sancionar esta conducta atípica en el plano penal.[137]

Este ciberdelito se orienta en la actualidad a sistematizar normativamente atentados contra los datos personales y la eventual invasión de la intimidad por medios informáticos.

Recientemente en el plano nacional e internacional, se han multiplicado sucesos, en los que, especialmente por medios informáticos se obtienen fraudulentamente datos personales para luego llevar a cabo ciertos hechos u operaciones con tales datos, por lo que es considerado el ciberdelito transnacional por excelencia del siglo XXI.[138]

También existe una lista de recomendaciones para evitar ser usurpado de la identidad;[139]

- ✓ Comprobantes, recibos o estados de cuenta. Evita los estados de cuenta impresos. Recibos telefónicos, de gas, estados bancarios o de seguros pueden ser robados de los buzones de las casas para obtener información importante como tus ingresos, RFC, CURP, etc. Exige a las empresas que detengan el envío de tu papelería impresa. Tu seguridad es razón suficiente para que dejen de hacerlo.
- ✓ El Buró de Crédito te avisa. Utiliza los servicios de Buró de Crédito como las alertas y el bloqueo para evitar que las empresas consulten tu historial sin que

---

[136] *ROMERO Flores Rodolfo, Óp. Cit.*
[137] *ROMERO FLORES RODOLFO, El robo de usurpación de identidad por medios informáticos o telemáticos: su tratamiento jurídico penal, en línea con dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/6/2958/20.pdf consultado 20-10-2020.*
[138] *ROMERO FLORES RODOLFO, óp. Cit.*
[139] *ROMERO Flores Rodolfo, Óp. Cit.*

te des cuenta. Esto te evitará dolores de cabeza si alguien pide un crédito con tus datos.

- ✓ Verifica a quién le das tus datos. No compartas tu información personal con cualquiera. Compartir tus datos en cualquier lugar donde te presentas puede ser peligroso. Al compartir tu información en sitios de Internet verifica que tengan certificados de seguridad, puedes verlo en la esquina superior derecha de tu explorador, como en la siguiente imagen. Los certificados SSL funcionan como las identificaciones: igual que presentas tu INE o pasaporte para comprobar que eres quien dice ser.
- ✓ No tengas una contraseña para todos tus servicios digitales. Lo ideal es tener una clave segura, mayor a 25 caracteres en cada servicio online donde te registras. Quizás eres de los que utilizan la misma contraseña de Facebook para tu correo y tu cuenta bancaria. Si ese es el caso lo recomendable es cambiarla. Actualmente existen herramientas para la administración de contraseñas, muy convenientes si tienes una cuenta en decenas de sitios.
- ✓ Utiliza contraseñas en tus dispositivos. La contraseña reduce las posibilidades de que puedan acceder a información sensible en tu dispositivo. Si bien no es un remedio definitivo te permite una ventana de tiempo para borrarlo de forma remota y proteger tus datos.
- ✓ No descargues o abras links sospechosos. Son comunes supuestas notificaciones del SAT o de los bancos con links o archivos adjuntos. Una manera fácil de identificar si los links de los correos que recibes son confiables es simplemente pasando el cursor por el botón o vínculo y podrás ver en la barra inferior de tu explorador el dominio a donde te re direcciona. Si el dominio es distinto al del SAT o tu banco; o está oculto tras una URL corta como bit.ly o goo.gl lo mejor es eliminar ese correo.
- ✓ No compartas documentos públicamente. El uso de aplicaciones como Google Drive o Dropbox pueden contribuir a la fuga de información sensible. En algunos casos estas URL públicas pueden ser rastreadas por los motores de búsqueda. Si vas a compartir este tipo de información es recomendable que el receptor de estos archivos también tenga una cuenta en la plataforma donde compartes los documentos así será visible únicamente por ustedes.

- ✓ Ten actualizado el antivirus de tu PC y sé precavido. No hagas operaciones bancarias o compras por Internet en equipos que pueden estar comprometidos, por ejemplo, PC públicas o que tu equipo se conecte a una red de Wi-Fi pública.

3.4.4. Delito cibernético del Malware:

Es un término utilizado para referirse al software o programas de cómputo que son introducidos en los sistemas de información de los usuarios para causarles algún daño o simplemente para modificar sus usos y obtener su control.

Es un vocablo que se origina del nexo de dos palabras de procedencia inglesa (malicious software), también se le conoce como software de actividades ilegales, es una categoría de código malicioso, que incluye virus, gusanos, caballos de Troya, también hace referencia a todo aquel software cuyo objetivo está en corromper la estructura del sistema operativo, así como recolectar información de manera ilegítima.[140]

El uso creciente de los sistemas informáticos ha causado que los hackers se sientan más atraídos a atacar las vulneraciones de las TIC mediante malas prácticas que afectan tanto a individuos como a empresas, ya sea para obtener un beneficio o sólo por el puro goce de perjudicar lo ajeno. Sin embargo, el problema no radica únicamente en esta situación, sino también en el hecho de lo que no se está haciendo para evitar que las intrusiones no deseadas sean nulas o cuando menos impedir que éstas no puedan obtener ningún tipo de malware.

Spyware	Estos son malware diseñados para recopilar datos del ordenador y sus usuarios. Lo hace con infiltración en el ordenador del usuario y monitorización de sus actividades. Se instala en el ordenador del usuario directamente o mediante explotación de huecos en la ciber seguridad.
	Tal y como su nombre indica, el ransomware es un software creado con el propósito de secuestrar datos del ordenador del

[140] *RAMIREZ Sánchez Jesús, Estudio descriptivo del malware en una dependencia académica de una institución pública de educación superior, en línea con dirección URL: https://www.uv.mx/iiesca/files/2016/11/06CA201601.pdf consultado 20-10-2020*

Ransomware	usuario. El software está diseñado para encriptar los datos delicados del objetivo. Entonces los creadores exigen dinero al usuario para desencriptar los datos.
Troyano informático	Este tipo de malware se ha creado para parecer un programa normal. Tanto es así que convence a los usuarios inconscientes para que lo instalen en su ordenador. Una vez instalado y ejecutado, el caballo de Troya puede empezar a realizar la función maliciosa para la que fue creado. Al contrario que los virus y los gusanos, los caballos de Troya rara vez intentan reproducirse y expandirse.
Rootkit	Este tipo de malware es creado para brindar a los cibercriminales permisos del nivel de administrador en el equipo objetivo. Este acceso les permite modificar el sistema del ordenador del usuario. Además, se usa para ocultar la presencia de otro malware en el sistema del ordenador
Virus Backdoor	Este tipo de malware crea una "entrada secreta" dentro del ordenador del objetivo. A través de esta puerta de atrás, los cibercriminales tienen la capacidad de acceder al ordenador sin el conocimiento del usuario. Los backdoors son creados por otros tipos de malware, como gusanos o caballos de Troya. Con el uso de backdoor, los cibercriminales también eluden los programas de seguridad del ordenador. Un tipo de virus backdoor es el Troyano de Acceso Remoto (RAT).

Cuadro elaborado con la finalidad de mostrar la cantidad de sistemas informáticos que se han creado para causar daño a todo dispositivo que tenga acceso a internet.[141]

Las formas de prevenir cualquier tipo de malware no siempre son seguras, y que no importa qué tipo de sistema operativo ni el tipo de dispositivo se utilice, sin embargo, existe una serie de medidas que podrían ayudar y son las siguientes:[142]

[141] *RAMIREZ Sánchez Jesús, Estudio descriptivo del malware en una dependencia académica de una institución pública de educación superior, en línea con dirección URL: https://www.uv.mx/iiesca/files/2016/11/06CA201601.pdf consultado 20-10-2020*

información que cause prejuicios.[142]

Existen tipos de malware que es importante conocer:

Virus informático	Un virus informático es la forma clásica de malware. Es un componente de código o programa que entra en su dispositivo sin que usted lo sepa. Una vez allí, puede causar una serie de daños, desde ralentizar su sistema, deshabilitar partes específicas o tomar el control por completo. Igual que con los virus biológicos, está diseñado para expandirse automáticamente a través de redes y dispositivos.

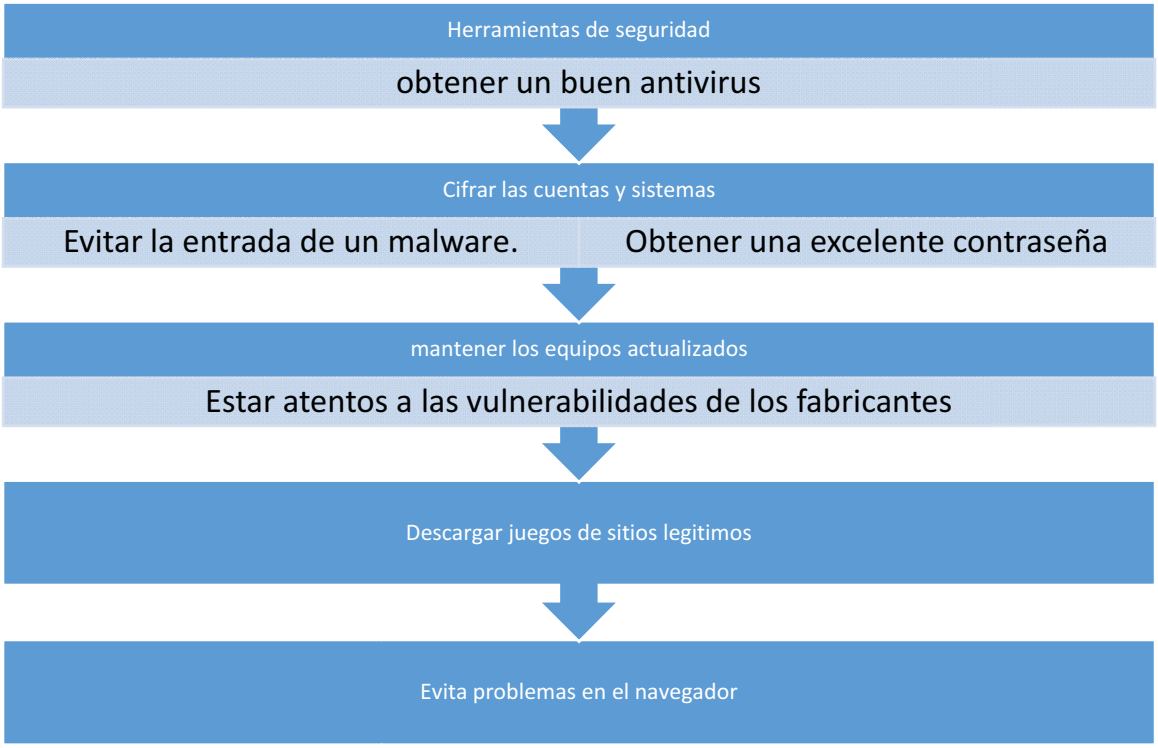


Diagrama con recomendaciones de herramientas para tener una mayor seguridad al momento de navegar a través de internet.[143]

3.4.5. Delito cibernético del Blanqueo de capitales:

cabe resaltar que es uno de los delitos que más se ha beneficiado de internet es el blanqueo de capitales, mejor conocido como “Money laundering”, en donde los criminales realizan transferencias inmediatas de dinero, fondos y capitales, a través

[142] *Consejos para prevenir la intervención del malware, en línea con dirección URL: https://www.redeszone.net/tutoriales/seguridad/consejos-proteger-equipos-entrada-malware/ consultado 21-10-2020.*
[143] *Consejos para prevenir la intervención del malware, en línea con dirección URL: https://www.redeszone.net/tutoriales/seguridad/consejos-proteger-equipos-entrada-malware/ consultado 21-10-2020*

de distintas cuentas bancarias ubicadas en paraísos fiscales, aprovechándose de varios factores como son la dificultad de rastrear el origen y destino de las transacciones; la utilización de identificaciones y datos falsos para ocultar el destino de los fondos y el anonimato del que gozan, sobre todo en países donde se privilegia el secreto bancario.[144]

Refiere Tondini que el término "lavado" tiene su origen en los Estados Unidos en la década de 1920, período en el cual las mafias establecieron una red de lavanderías para esconder la procedencia ilícita del dinero que alcanzaban con sus actividades ilegales. La operación consistía en que las ganancias derivadas de extorsión, tráfico de armas, contrabando y venta de alcohol y prostitución se combinaban con las de lavado de textiles y así se revelaban y/o reportaban al Servicio de Rentas Internas (Internal Revenue Service -IRS-) de los Estados Unidos. De esta forma, como el IRS no podía diferenciar entre los dólares que provenían de las actividades ilícitas y los que no, la mafia burló durante un considerable tiempo la ley.[145]

Fernández estima que el “lavado de dinero” consiste en el ocultamiento, mediante una serie de operaciones a efectos de poder legitimarlos, de los bienes que provienen de una actividad ilícita previa o delito grave como el tráfico ilegal de armas, de animales exóticos, de seres humanos o de sus órganos, la corrupción, el juego, el contrabando y el enriquecimiento ilícito de funcionarios públicos.

El blanqueo de capitales se entiende toda aquella operación o acción destinada específicamente a proyectar la apariencia de legalidad a dineros de origen ilícito. Esto significa ocultar, simular, encubrir o camuflar la existencia, la fuente ilegal, el movimiento y el destino o uso de bienes o fondos producto de actividades ilegales para hacerlos figurar o parecer como legítimos.

De esta manera, el blanqueo de capitales implica la colocación de los fondos dentro del sistema financiero mediante la ideación de operaciones bancarias, de manera que se imposibilite determinar el origen del dinero en cuestión, su real propietario y se viabilice su integración dentro de la economía legal que maneja la sociedad y, por

---

[144] *Consejos para prevenir la intervención del malware, en línea con dirección URL: https://www.redeszone.net/tutoriales/seguridad/consejos-proteger-equipos-entrada-malware/ consultado 21-10-2020.*

[145] *MARTINEZ, Julio Cesar, El blanqueo de capitales, en línea con dirección URL: https://eprints.ucm.es/41080/1/T38338.pdf consultado 21-10-2020*

ende, el Estado. De tal suerte, incurre en blanqueo de capitales cualquier persona, natural o jurídica, que adquiera, tenga bajo su cuidado, administre o se lucre de bienes obtenidos con dinero producto de actividades ilícitas y/o realice operaciones financieras con dichos fondos.

Las formas que se mencionara son solo algunas organizaciones de todas: las triadas chinas, la yukuza, los nuevos carteles colombianos, la guerrilla y los ex paramilitares, la mafia siciliana y la mafia rusa.

Los procedimientos que emplean en el blanqueo de capitales:

- Creación de sociedades ficticias. inversiones en el sector inmobiliario
- Investigación en activos opacos
- Suscripción de seguros
- Realización de un contrato de cesión temporal de un crédito,
- Sociedades de inversión filatélica
- Operaciones comerciales
- Declaración de beneficios de negocios superiores a las redes
- Juegos de azar
- Compra venta de piedras y animales preciosos
- Compraventa de obras de arte y antigüedades
- Manipulación de facturas
- Blanqueo mediante el exterior

En estos momentos, la doctrina discute ampliamente sobre la legitimación y la interpretación de tipos penales consagrados como el blanqueo de capitales y la eficacia de las medidas tomadas en su contra; por ejemplo, en Alemania se considera que son demasiado amplios y ponen en peligro la libertad ciudadana y, en consecuencia, se exige desde enmiendas legislativas hasta inversiones de prueba, a cargo del ciudadano.

El tema sobre el lavado de dinero o blanqueo de capitales es muy extenso, debido a la magnitud de delitos que vienen implicados, sumándole la herramienta de internet que lo hace más fácil para su ejecución,

La problemática sobre este ciberdelito, es porque quizá sea una construcción mancomunada mundial que sea combatida eficazmente mediante un mecanismo que

disminuya significativamente las diferencias de los vacíos regulatorios que existen entre las naciones y que posibilite tanto el intercambio de información como la estrategia de los criminales.

3.4.6. Delitos cibernéticos que impactan mayormente a la integridad de la persona y a sus derechos humanos.

En este apartado se detallará a los delitos exclusivos en los que se encuentra mayor infracción en los derechos relacionados contra atentados a la intimidad, el honor y la integridad moral.

El sexting empieza a tener auge a partir del año 2005, sobre todo en comunidades digitales anglosajonas, teniendo como origen los mensajes de texto a través de celulares y/o programas de chats. Diferentes estudios afirman que aproximadamente desde 2009, esta práctica se convirtió en un suceso cotidiano entre adolescentes, comúnmente relacionado al consumo de alcohol y drogas, pero también asociado a nuevas prácticas de demostrar algún compromiso y/o sentimiento pasional. Los casos de presión y chantaje, también aparecieron entre los orígenes asociados.

De acuerdo con el término que nos proporciona la Fundación en Movimiento, nos define que los términos son en inglés "sex" y "texting" y se refiere al envío de contenidos eróticos o pornográficos (principalmente fotografías y/o vídeos) por medio de medios digitales, casi siempre teléfonos celulares, tabletas y computadoras personales.

El envío de estos materiales, regularmente realizado de forma voluntaria, se ha convertido en una alarmante moda, principalmente entre adolescentes de 12 a 18 años (Aunque practicada por usuarios de casi cualquier edad), tomada como un aspecto natural de su vida sexual.

En cuanto a la regulación del caso de México, se han tomado iniciativas, sin embargo, aún no existe una ley que lo prescriba, debió a una contradicción ya que al enviar este tipo de material explicito no está restringido ni prohibido por norma alguna y recae directamente en la libertad de expresión.

Sin embargo, “puede ser tipificado como delito cuando la finalidad sea la exhibición de personas menores de edad, vaya dirigido a esas mismas o sea divulgado sin el

consentimiento de la persona mayor de edad que aparece en el mismo". El "sexting" es una práctica común y se debe regular porque "desde la perspectiva de los derechos humanos las consecuencias nocivas de ésta es una forma de violencia que propicia el señalamiento, la discriminación, la denigración, exclusión y marginación.[146]

Es muy importante hacer caso de los consejos sobre el sexting, debido a que es un ciberdelito muy concurrido:

- Evita al máximo enviar contenido tuyo íntimo por medio de internet.
- Cuando envíes material privado a otra persona, asegúrate que sea esta plena de confianza.
- Si envías fotos o videos, ten certeza que el material sea borrado tanto del dispositivo de envió como el de llegada.
- Mantén actualiza tus equipos con antivirus para evitar que sean hackeados.
- Ten contraseñas seguras en tus aparatos electrónicos para que en caso de pérdida o robo otras personas no puedan acceder a este material

Estudios demuestran que este caso se da por medio de los romances, coqueteos, popularidad, presión de amistades, venganza, intimidación y chantaje, pero recuerda que en ti mismo está la adopción de evitar que el sexting se salga de control.[147]

3.4.7. Delito Cibernético del Stalking o ciberstalking.

Palabra anglosajona que significa acecho y que describe un cuadro psicológico conocido como síndrome del acoso apremiante. El afectado, que puede ser hombre o mujer, persigue de forma obsesiva a la víctima: la espía, la sigue por la calle, la llama por teléfono constantemente, le envía regalos, le manda cartas y SMS, escribe su nombre en lugares públicos y, en casos extremos, llega a amenazarla y a cometer actos violentos contra ella.

---

[146] *FUNDACION EN MOVIMIENTO en línea con dirección URL: http://www.fundacionenmovimiento.org.mx/dvsexting?gclid=EAIaIQobChMI5rqtgZrb4AIVBNvACh0dAwpcEAAYAiAAEgJFTPD_BwE consultado 21-10-20*

[147] *Óp. Cit.*

También conocida como cyberstalking, es el término usado para referirse al trastorno que tiene una persona que lo lleva a espiar a su víctima. Principalmente el cybestalking se da en redes sociales como Facebook, Instagram o Twitter, donde la mayoría de las personas dejan su información disponible para cualquier persona, por medio del correo electrónico o por servicios de mensajería instantánea como WhatsApp.[148]

Consejos de cómo prevenir el stalking:

- Evitar dar tu información personal como correos electrónicos o números de teléfono, a desconocidos.
- No aceptes personas extrañas en tus redes sociales
- Configura la privacidad de tus redes sociales, según los intereses que consideres necesarios.
- Reporta los correos sospechosos
- Se precavido con las cosas que publicas en internet.
- Ante una situación sospechosa de alguien que te contacto por internet, acércate donde las autoridades pertinentes y cuenta les tu caso.
- Ten muy en cuenta que las fotografías son una de las formas de llamar la atención sin quererlo. Después de que publicas una imagen en internet cientos de personas la pueden ver y pierdes el control de lo que ellas puedan hacer con esa foto.[149]

3.4.8. Delito cibernético del Grooming.

Vivimos en una época donde el avance tecnológico se ha convertido en una herramienta indispensable para el desarrollo del ciudadano, como medio de trabajo, de ocio en incluso escolar y educativo. Los adolescentes están mucho más expuestos y sobre todo más desprotegidos a la hora de utilizar las redes sociales, ya que el uso del internet es accesible desde cualquier sitio, a cualquier hora, de forma totalmente anónima y sin un control adecuado para los diferentes contenidos, espacios y servicios que se pueden utilizar en la red.

[148] *FUNDACION EN MOVIMIENTO, Óp. Cit.*
[149] *Op. Cit.*

Es de gran importancia que nuestra población disponga de tipo de información para saber actuar frente a este tipo de situaciones.

Se considera que el delito del grooming se basa en una serie de conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad. Creando una conexión emocional con el mismo, con el fin de disminuir las inhibiciones del niño y poder abusar sexualmente de él.

En el caso de México, el ciberdelito del "grooming" plantea de cuatro a ocho años de prisión y una multa de 400 mil UMA´s, y sobre el "sexting" se fija la pena de seis meses a tres años de prisión y multa de 800 a dos mil UMA´s, pero cuando involucre a un menor de edad, la pena se incrementará hasta en la mitad de lo establecido.[150]

3.4.9. Delito cibernético del ciberbullying o ciberodio.

Internet ha cambiado las reglas del juego. Hoy puedes hacer casi todo con un solo clic: comprar, vender, leer, estudiar, ligar, enamorarte y odiar. La ausencia absoluta de límites y de normativa, el relativo anonimato y la facilidad de acceso a la red facilitan que se puedan difundir ideas, símbolos, lemas, actitudes e incluso conductas que menosprecian, atacan y humillan a otras personas. También se le conoce como delito del odio o del hate crime en la red.

El odio es intensa emoción humana que puede llevar a la comisión de acciones violentas: acciones físicas que pueden lesionar e incluso matar otra persona o manifestaciones verbales que lesionan bienes jurídicos protegidos por nuestra Constitución como son el derecho de honor y a la dignidad personal. Se odia por muchas razones, y lo preocupante hoy no solo es la persona que odia y desprecia intensamente a otra persona o personas por razones como la etnia, su orientación sexual, su religión o su nacionalidad. Lo que más nos debe alarmar es la incitación o

[150] *S/a, Revista sobre delitos cibernéticos en línea con dirección URL: https://revistaenterate.mx/index.php/legisladores-home/12010-propone-tipificar-al-sexting-y-grooming-como-delito. Consultado 16-08-2020*

llamamiento masivo que determinadas personas hacen a terceros para que también odien por las mismas razones que lo hacen ellos.[151]

El ciberodio surge de la intolerancia hacia el otro y la no aceptación de la diversidad abona el terreno para el crecimiento del discurso del odio en internet que se manifiesta principalmente a través de rumores, estereotipos, prejuicios y falsedades.

Anteriormente se odiaba en "petit comité", hoy se odia dando publicidad a ese odio y a través de las nuevas tecnologías. El ciberodio son todos aquellos mensajes que se vierten en la red a través de blogs, redes sociales, videos, imágenes, grupos de Facebook cerrados, páginas web específicas, foros de discusión, juegos online que insultan, degradan, humillan o incitan al odio o a la violencia contra una persona o un grupo de personas por su origen étnico, su nacionalidad, su orientación sexual, sus creencias, su condición social o su discapacidad. No estamos ante un odio genérico, sino todo lo contrario es un odio específico o concreto por razón del destinatario al que se dirige.

Difundir un mensaje en la red hacía unos destinatarios concretos, puede dar lugar a agresiones físicas y verbales, vulneración de derechos y discriminación ya que el receptor de dicho mensaje es una audiencia ilimitada de personas además que crece rápidamente de modo exponencial, al tener la posibilidad de poder compartir dicho mensaje.

Este tipo de conductas hacen de un modo directo o indirecto vulnere la convivencia pacífica de nuestra sociedad. Por ejemplo, actualmente, internet y las redes sociales son un medio utilizado por los terroristas yihadistas para difundir sus mensajes de odio hacia occidente y para captar a nuevos combatientes de cualquier lugar del planeta.

El ciberodio es un fenómeno creciente y global que crea un clima que normaliza la intolerancia hacia inmigrantes, personas sin hogar, musulmanes, judíos, gitanos, persona LGBT (lesbianas, gays, transexuales y bisexuales) y, en definitiva, de todas

[151] VELASCO De la Fuente, *Homo criminals*, en línea con dirección URL: https://criminal-mente.es/ consultado 25-09-20.

las personas que no encajen en las perspectivas de poder y de exclusión de grupos radicales que promueven el odio hacia colectivos vulnerables.[152]

Otro de los nuevos problemas relacionados con las tecnologías de información y comunicación es el ciberacoso que, aunque está relacionado, es diferente del ciberodio y se suele producir sobre todo en un contexto escolar.[153]

Internet resulta un medio muy efectivo para los grupos racistas y neonazis por las siguientes razones:

- Los usuarios que se conectan a internet superan los 3000 millones
- Impunidad legal de sus actividades de odio en la red en muchos países
- Internet es la pista principal de transmisión del discurso de odio. Es un medio difusor y organizador de grupos racistas, xenófobos y de intolerancia externa.[154]

En el caso de España el poder alcanzado por las redes sociales como medios de comunicación de masas, ya que ha sido un delito muy común y es alarmante, en los siguientes datos se muestra[155]:

- El 78% de los internautas españoles está inscrito en alguna red social.
- El 98% de los jóvenes españoles de 15 a 20 años está dado de alta en una red social.

-1000 millones de personas en todo el mundo están dadas de alta en Facebook.

En Facebook existen gran cantidad de páginas con denominaciones como[156]:

- Odio a los gitanos
- Contra la invasión del migrante
- Rudolf Hess vive
- Mata gays

---

[152] *CASTILLO Charo Alises, El Ciberodio con dirección URL: http://federacionkamira.com/wp-content/uploads/2017/01/PONENCIA-CHARO-ALISES-CIBERODIO.pdf consultado 19-11-20.*

[153] *CASTILLO Charo Alises, El Ciberodio con dirección URL: http://federacionkamira.com/wp-content/uploads/2017/01/PONENCIA-CHARO-ALISES-CIBERODIO.pdf consultado 19-11-20*

[154] *CASTILLO Charo Alises, El Ciberodio con dirección URL: http://federacionkamira.com/wp-content/uploads/2017/01/PONENCIA-CHARO-ALISES-CIBERODIO.pdf consultado 19-11-20*

[155] *CASTILLO Charo Alises, El Ciberodio con dirección URL: http://federacionkamira.com/wp-content/uploads/2017/01/PONENCIA-CHARO-ALISES-CIBERODIO.pdf consultado 19-11-20*

[156] *CASTILLO Charo Alises, El Ciberodio con dirección URL: http://federacionkamira.com/wp-content/uploads/2017/01/PONENCIA-CHARO-ALISES-CIBERODIO.pdf consultado 19-11-20*

- Hay que legalizar la violación
- Odio a los maricones y a los policías

Lamentablemente son pocos los países que contemplan el ciberodio de forma específica en su legislación. Los humanos somos sujetos emocionales y en muchas ocasiones, esas emociones los llevan a cometer ilícitos penales: un amor obsesivo puede llevar a dar muerte a tu pareja o ex pareja ejemplo (Otelo a su amor enfermizo) y un odio exacerbado puede dar pie a que una persona o un grupo de personas atenten contra derechos fundamentales de otros sujetos, simplemente por su elección sexual, por ser extranjeros, por ser de color o profesar otra religión. Los que odian deciden a quien odiar y porque odiar. Buscan y crean sus propias razones para odiar. Todos absolutamente todos nosotros, somos potenciales víctimas de ser odiadas por simplemente ser quienes somos. Para odiar no es necesario que el objeto de nuestra emoción sea un sujeto concreto, sino basta con que sea una determinada clase de persona.[157]

3.4.10. Delito cibernético del ciberataque o ciberterrorismo.

Hoy en día el concepto de ciberterrorismo es utilizado de modo más frecuente para referirse a una diversidad de ataques en contra de las comunicaciones, la información y de los sistemas informáticos que la contienen. Las comunicaciones estratégicas, los sistemas de salud, el control aéreo, la video vigilancia los transportes con sistema computarizado, las armas controladas por sistema de cómputo, la georreferenciación de vehículos, los objetos que requieren de conexión a la red, las propias redes sociales, los bancos de datos, los sistemas financieros, la telefonía, los mensajes de texto, internet, etc. Son solo algunos ejemplos de los objetivos que el ciberterrorismo persigue para su anulación temporal o definitiva.[158]
Acuñar el termino ciberterrorismo como la posibilidad de que sean atacados tanto los sistemas de información como las redes de datos o que sean utilizados por y para perpetrar actos terroristas, resulta poco afortunado, ya que todos los términos que

[157] ***CASTILLO Charo Alises, El Ciberodio con dirección URL: http://federacionkamira.com/wp-content/uploads/2017/01/PONENCIA-CHARO-ALISES-CIBERODIO.pdf consultado 19-11-20***
[158] *NAVA Garcés Alberto Enrique, Ciberdelitos" Instituto Nacional de Ciencias Penales, tirant lo Blanch, Ciudad de México 2019. P.160*

utilizan el prefijo “ciber” no son del todo exactos en tanto el objeto que pretenden describir. Otros autores definen al “ciberterrorismo” como cualquier ataque electrónico desde el ciberespacio desde redes internas y externas, en particular internet, inspirado en diferentes motivos y dirigido a objetivos en particular.[159]

Terrorismo cibernético puede referirse a ataques premeditados y de inspiración política realizados por grupos o agentes clandestinos en contra de información, sistemas computacionales, programas y demás datos informáticos que resulten en actos de violencia hacia objetivos no beligerantes. En ese sentido habría de distinguir cuando los considerados “terroristas” utilizan computadoras o sistemas informáticos para sus actividades, un claro ejemplo es el uso terrorista de internet y dichos instrumentos son un objetivo.[160]

Existe un gran error en cuanto al término ya que asimilan al ciberterrorismo con una comunidad religiosa y, de manera equívoca, estigmatizan a los miembros de un culto adosándoles el término de terroristas. El islam ha sido el pretexto de los grupos terroristas, pero considero que ello solo ha servido para estigmatizar un credo y a quienes pertenecen al mismo. Darles un sesgo religioso a las actividades ilícitas solo genera mayor intolerancia en este mundo al que parece que no le son pocas las causas para polarizarse.

El ciberterrorismo es un concepto utilizado para referirse a una diversidad de ataques en contra de las comunicaciones, la información y de los sistemas informáticos que la contienen, por ejemplo las comunicaciones estratégicas, los sistemas de salud, el control aéreo, la videovigilancia, los transportes con sistema computarizado, las armas controladas por sistema de cómputo, la georreferenciación de vehículos, los objetos que requieren conexión a la red, las propias redes sociales, los bancos de datos, los sistemas financieros, la telefonía, los mensajes de texto, internet, etc. estos son solo algunos ejemplos de objetivos que el ciberterrorismo persigue para su anulación temporal o definitiva .[161]

Ha habido a lo largo de la historia una inmensidad de ciberataques, sin embargo, por su poca regulación ha sido difícil de castigar este ciberdelito. Solo son pocos países

[159] *NAVA Garcés Alberto Enrique, Op. Cit. P 162*
[160] NAVA Garcés Alberto Enrique, Óp. Cit. P 163
[161] *NAVA Garcés Alberto Enrique, Óp. Cit P. 158.*

que se han encargado en desarrollar elementos en el ámbito del derecho penal interno para salvaguardar y proteger su estado.

3.4.11. Delito cibernético de la propiedad intelectual.

Delitos contra la propiedad intelectual: incluye a los derechos de autor, el cual con ánimos de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique en todo o parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de la propiedad intelectual o de sus cesionarios.

Hablar de propiedad intelectual se refiere al derecho que asiste a los acreedores de obras, artísticas o científicas siempre que sean originales y con independencia del medio o del soporte a través del que se expresen a disponer de ella de su voluntad, autorizando o no su reproducción, explotación, difusión, etc., también se conoce como derechos de autor.

La Ley de Propiedad Intelectual, la copia, instalación o utilización de cualquier programa de ordenador sin consentimiento del titular del derecho supone una reproducción ilegal que debe ser castigada.

Se catalogan también como delitos en contra de la confidencialidad, integridad y disponibilidad de datos. Se refiere a los accesos no autorizados a sistemas de cómputo, a datos, o se realizan interceptaciones, de manera no autorizada, a redes de comunicación; redes (LAN), de internet, telefónicas, de fax entre otras.

Cuando hablamos de “acceso no autorizado” nos referimos a que el infractor o el ciberdelincuente ingresa sin autorización, a los datos que posee el directamente afectado, este ingreso puede conllevar muchos agravantes, como el espionaje, la instalación de diferentes virus, bombas lógicas, etc., o la simple acción de ingresar de manera no autorizada, como satisfacción o reto personal o del “hacker”. Es importante diferenciar entre un acceso no autorizado y una intercepción ilegal, pues la segunda puede llegar a tener más agravantes en cuanto a las libertades individuales del o de la afectada.

En este sentido, nos referimos a interceptación cuando se ve vulnerado el derecho a la privacidad de las comunicaciones electrónicas, “este tipo de delitos es equivalente

a la violación de las comunicaciones privadas, tales como la grabación de conversaciones telefónicas entre sujetos, y es aplicable a todas las formas de transferencia electrónica de datos, ya sea mediante teléfono, fax. Correo electrónico o transferencia de archivos.

Cuando hablamos de la disponibilidad de datos y los posibles delitos que se pueden estar relacionados con los mismos, nos referimos a la obstaculización intencional del usos de los sistemas de cómputo, incluyendo equipos e infraestructura de telecomunicaciones mediante la utilización de sistemas de datos, y un ejemplo muy común sobre ataques a sistemas de cómputo es el “Ataque sobre denegación del servicio”, el cual se busca con este tipo de ataques es que los recursos de sistemas de cómputo y sus servicios se vean seriamente interrumpidos y afectados en su uso en determinados lugares.

Vinculados a los atentados contra la propiedad intelectual, es importante tener en cuenta que en internet circula mucho tipo de información o datos, que en algunos casos son de dominio público; pueden tener acceso libre, además de ser libres en su circulación de descarga y uso. Pero no todo el contenido que se encuentra en internet es de libre circulación y uso por ejemplo no todos los libros online pueden ser vistos o descargados de manera gratuita. Es en este sentido, que cuando se vulneran o se infligen las leyes de derechos de autor, se está atentando contra la propiedad intelectual, lo que es se conoce como delito cibernético que es muy concurrente y ha generado pérdidas millonarias a las empresas, casas disqueras, artistas, productoras de cine, etc.

La piratería está asociada con los delitos en contra de la propiedad intelectual, y es el internet y los diversos sistemas de cómputo, una herramienta para entrar en contra de los derechos de autor (copy right). Esta clasificación también se refiere a los derechos de los autores, derecho de los inventores o al Trade Mark o marcas y las patentes. En síntesis, podemos decir que se atenta contra la propiedad intelectual en el contexto de un delito cibernético cuando sin autorización, sin licencia, mediante el acceso ilícito, la utilización de códigos o el hackeo tradicional, se accede a la descarga o se utiliza material o datos informáticos protegidos bajo los derechos de autor.

Es importante mencionar que las disipaciones legales del copy right varían dependiendo de las legislaciones de cada país, aunque hay normativas dispuestas por la OMC o la Unión Europea, que establecen ciertas pautas, para no infringir los derechos de autor. Es de mencionar que amparar legalmente los derechos de autor se ha convertido complejo en la medida en que el internet ha permitido el acceso a "obras" o creaciones que son inmateriales, y que su contenido no se encuentra ubicado en un lugar "terrenal" especifico, sino que circula por la red, por lo que podríamos decir que existe una "aterritorialidad" inerte al contenido de internet, lo que complica que se apliquen las leyes de uno u otro país "el factor de cara a internet, por la aterritorialidad de la red y con el hecho de que las leyes de un Estado solo pueden aplicarse por los tribunales dentro del territorio geográfico de este mismo Estado.

3.4.12. Delito de la piratería informática.

La Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) define a la piratería como la reproducción y distribución de copias de obras protegidas por el derecho de autor, así como su transmisión al público o su puesta a disposición en redes de comunicación en línea, sin la autorización de los propietarios legítimos, cuando dicha autorización resulte necesariamente legal.[162]

Por su parte la Organización Mundial del Comercio (OMC) lo define como "Reproducción no autorizada de materiales protegidos por derechos de propiedad intelectual (como derecho de autor, marcas de fábrica o de comercio, patentes, indicaciones geográficas etc.) hecha con fines comerciales, y comercio no autorizado de los materiales reproducidos.[163]

La UNESCO señala que la piratería afecta a obras de distintos tipos, como la música, la literatura, el cine, los programas informáticos, los videojuegos, los programas y las señales audiovisuales.

---

[162] *AGUIRRE Quezada Juan Pablo, Piratería en México y sus efectos en la sociedad, en línea con dirección URL: http://www.bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/1950/CI-22.pdf?sequence=1&isAllowed=y consultado 22 de mayo de 2021.*

[163] AGUIRRE Quezada Juan Pablo, óp. Cit.

La piratería informática es un ciberdelito que engloba diferentes actividades como plagio de artículos o diseños, violaciones a la propiedad intelectual, industrial o robo de patentes, falsificaciones, adulteraciones del original entre otros aspectos. Esta práctica ha estado presente a lo largo de la historia universal en diferentes sociedades.

Es importante señalar que, pese a las leyes y normativa creadas por algunos países y organismos como la OMC, la Unión Europea y la OMPI que la regulen, persiste el problema debido a que no existe una norma o ley que ampare los derechos de autor por internet, debido a que resulta difícil rastrear su localización cuando suben el documento debido a que el internet se encuentra en todas partes.

3.4.13. Delito cibernético de la Pornografía infantil o ciber pornografía infantil.

El tema de la pornografía infantil se define al material audiovisual, en cualquier tipo de soporte, donde se muestren a menores de edad, con independencia de su sexo, en cualquier tipo de actitud sexualmente explicita o meramente erótica. Los delitos de la pornografía infantil engloban, en la práctica totalidad de legislaciones territoriales, la simple tenencia de este tipo de material, así como la distribución exhibición o el hecho de compartirlo con otras personas. En función de la normativa, se pueden prever, además, penas de cárcel más duras si el infractor ostenta alguna relación de parentesco con la víctima.

En internet, al igual que en el mundo territorial. La ciber pornografía infantil se castiga en muchos ordenamientos jurídicos territoriales como un delito ordinario de pornografía infantil, por lo que también han avanzado en establecer penas de cárcel más elevadas previstas por el delito de ciber pornografía infantil, cuando se comenten en el ciberespacio. El año de 1999 es un año de suma importancia porque se registró un gran incremento de la pornografía infantil denunciados y también fue el año en que se tuvo un ascenso sobre la comercialización de servicios de internet en países occidentales.

Otro tema que va de la mano, es la explotación sexual que tiene también la mujer y el hombre y que también es reproducida y llevada a cabo por este medio y que aún no está tan avanzada su regulación a comparación de los derechos del niño, agregando la trata de personas que resulta mayor facilidad, mayor ingreso

económico y lo más importante que puedes vender a cualquier parte del mundo y es muy difícil su localización por el ahora nuevo espacio y cada día más intensificado internet.

La UNICEF, se ha encargado en coordinación de Naciones Unidas en intensificar la regulación y cuidado de los niños, sin embargo, en la trata y pornografía de los adultos aún quedan grandes retos que realizar internacionalmente.

Este ciberdelito a comparación de los demás, se encuentra mejor regulado y se han tenido avances positivos, pero aun así día a día tiene el compromiso de adecuarse y desarrollarse a las situaciones de la sociedad interna e internacional.

3.5. El bitcoin (criptomonedas) relación con los ciberdelitos.

El bitcoin es una divisa digital que puede ser utilizada como medio de intercambio y que sus promotores usan como reserva del valor, no existe físicamente ni la controla ningún país. Hoy en día este tipo de moneda virtual se ha convertido, apoderado, apoyado o beneficiado al crimen organizado. Uno de los casos más conocidos donde las criptomonedas se vieron envueltas en actividades ilícitas fue el caso del WannaCry[164] que provocó un ciberataque masivo a nivel mundial dirigido a empresas y usuarios. Los criminales pedían un rescate en criptomonedas a cambio de liberar los equipos infectados.[165]

Este tipo de actividades, donde las criptomonedas se convierten en la forma de pago favorita de los ciberdelincuentes, se han vuelto cada vez más populares, ya sea mediante el secuestro de información, la minería de criptomonedas o el robo de carteras electrónicas o "wallets".

La cryptomenda ha penetrado por medio de las siguientes actividades ilícitas; cryptojaking[166], fake wallets[167], rasonware[168], otras actividades ilícitas como

---

[164] *Fue un ataque que comenzó el 12 de mayo de 2017, infectando en primeramente en Asia, creado por Park Jin Hyok, el cual por ser un gusano se extendió como pólvora en todo el mundo.*

[165] *OFICINA DE SEGURIDAD INTERNAUTA, en línea con dirección URL: https://www.osi.es/es/actualidad/blog/2019/08/07/sabias-que-las-criptomonedas-estan-involucradas-en-algunos-ciberdelitos consultado 29-06-2021.*

[166] *Se trata del secuestro de un dispositivo electrónico sin el consentimiento o conocimiento del usuario para el minado de criptomonedas. Con el paso del tiempo el sistema se ha ido perfeccionando, apareciendo métodos cada vez más difíciles de detectar. Una vez el software minero es ejecutado en el dispositivo, la app solo necesitará acceso a Internet para comenzar a ejecutar su tarea.*

[167] *Con la creciente popularidad de las criptomonedas, no es sorprendente ver aplicaciones maliciosas que se hacen pasar por carteras virtuales. Los ciberdelincuentes crean aplicaciones que simulan ser*

(financiación del terrorismo, chantajes y estafas como la sextorsión blanqueo de dinero y compra y venta de productos ilegales en la dark web, tales como drogas o medicamentos peligrosos que muchas veces son falsificados y puede provocar severos daños e incluso la muerte del consumidor.[169]

El problema principal es que, a causa del anonimato buscado en el diseño de la mayoría de las criptomonedas, no existe en muchos casos una manera eficiente de realizar un seguimiento a las transacciones hechas con criptomonedas que reduzca el riesgo de su uso para actividades ilícitas, tales como las ya señaladas u otras con impacto en ocasiones aún más grave y aunque los gobiernos y algunos creadores y desarrolladores se esfuercen en regular o mejorar la seguridad, las criptomonedas se crearon para estar al margen de muchas de estas regulaciones, por lo que las convierte en un arma de doble filo.

---

una "wallet" oficial. Utilizan el logo oficial y afirman que nos permitirá convertir nuestras criptomonedas en otras como Bitcoin, Ethereum y Litecoin, etc. Sin embargo, una vez que las criptomonedas se envían a las direcciones que figuran en la aplicación, desaparecen de nuestra app y acaban en manos del ciberdelincuente.

[168] *Los ciberataques basados en el secuestro de información o "ransomware" han experimentado un incremento desde la aparición de este tipo de monedas virtuales. El Bitcoin (BTC) es uno de los métodos de pago más utilizados, en los casos de infección por ransomware*.

[169] *OFICINA DE SEGURIDAD INTERNAUTA, en línea con dirección URL: https://www.osi.es/es/actualidad/blog/2019/08/07/sabias-que-las-criptomonedas-estan-involucradas-en-algunos-ciberdelitos consultado 29-06-2021.*

CAPITULO 4 Políticas y ordenamientos jurídicos estatales y marco legal internacional e institucional aplicables a los delitos cibernéticos.

4.1. Leyes extranjeras que prescriben a los Delitos Cibernéticos por medio del enfoque de las principales familias jurídicas.

Es de suma importancia las afinidades de las legislaciones, debido a que gran número de países fundamenta su régimen de asistencia judicial mutua en el principio de la doble discriminación, según el cual un delito debe ser considerado como tal tanto en el Estado que solicita la asistencia como el que la presta.[170]

Se dará un análisis comparativo de diversos países que han tenido avance en la creación de legislaciones y que permiten como se ha actuado en la relación a algunos casos de importante relevancia.

Una fecha histórica fue 1986 en la cual aprobaron la ley de privacidad de comunicaciones electrónicas (Electronic Communication Privacy Act, por sus siglas en Ingles) en Estados Unidos marco la primera vez que específicamente se había promulgado una pieza importante de legislación para el mandato de restricciones en el uso de equipos. Fue un momento histórico, no solo para ese país, sino para todo el mundo. En los años que surgieron tras el paso de la ECPA, muchas agencias federales desde el FBI y el servicio secreto comenzaron a aplicar este y otros actos legislativos, tratando de acabar en la nueva ola de delitos cibernéticos.[171]

Se ha hecho mucha investigación para mejorar la viabilidad de represión de delitos electrónicos. El FBI tiene ahora una red de escuadrones de delitos cibernéticos. El departamento de Justicia ha establecido un conjunto de directrices en el que esbozan procedimientos para aprovechar y buscar equipos. Incluso la población general estadounidense en su conjunto es ahora más adecuada sobre delitos

---

[170] *En lo que respecta al principio de la doble incriminación en las investigaciones de delitos cibernéticos, véanse: Manual de las Naciones Unidas sobre Prevención y Delitos Informáticos, Revista Internacional de Política Criminal, Núm. 43 y 44, Publicación de las Naciones Unidas, Núm. De venta S-94IV.5), p. 269, Documento de antecedentes de STEIN SCHOLBERG Y AMANDA HUBBARD titulado Harminizing national legal approaches on cybercrime, p.5.*

[171] *MONTOÑA Piña Javier Omar, "Delitos Federales cometidos a través de medios informáticos, capitulo II "los Delitos Informáticos en el plano internacional, p. 27.*

informáticos, y por lo general muchos saben qué hacer para protegerse a sí mismos.[172]

Lo que se pierde en este marco legal, que es el Internet, así como sus delitos de Internet se extienden mucho más allá de las fronteras de los Estados Unidos. De acuerdo con InterGov internacional, 39 % del tráfico de Internet se genera fuera de los Estados Unidos. Además, una Comisión de las Naciones Unidas de 1991 sobre delincuencia y justicia penal llego a la conclusión de que, en la encuesta de 3000 sitios de extensiones de dirección Virtual en decenas de países, más de 72% comunicaron un incidente de seguridad dentro de los últimos 12 meses. Claramente se puede notar que la aplicación de la ley en la frontera no es solo problema de Estados Unidos sino es un problema mundial.[173]

4.1.1. Familia jurídica Common Law.

El common Law es un término utilizado para referirse al grupo de normas y reglas de carácter no escrito pero castigadas por la costumbre o la jurisprudencia y que son ineludibles del derecho de los países anglosajones que a continuación mencionaremos junto con sus avances en materia del combate a los delitos cibernéticos.

Australia

La ley de Telecomunicaciones de 1991 y las secciones básicamente añadidas 74 y 76 del Código Penal australiano. En su sección 74, describe las definiciones de transportistas y datos. El gobierno de Australia ha presentado nuevas leyes con las que combatir de manera más eficaz la delincuencia en Internet, al hilo de los últimos ciberataques contra empresas multinacionales e instituciones públicas, como Google, el Fondo Monetario Internacional y el Senado de Estados Unidos.

En una ocasión, la red informática del parlamento se vio afectada por uno de estos ataques. “La creciente amenaza cibernética significa que ninguna nación por si sola puede superar eficazmente este problema y la cooperación internacional es esencial”, añade el fiscal. Más requisito de almacenamiento. Estas leyes aprobadas

[172] *MONTOÑA Piña Javier Omar Op. Cit. P.28*
[173] *MONTOÑA Piña Javier Omar Op. Cit. P.28*

por el Parlamento, permitirán que la policía y los servicios de inteligencia obliguen a las empresas telecomunicaciones a mantener en sus archivos información relevante.
Austria la ley de reforma del Código Penal de 22 de diciembre de 1987 contempla los siguientes delitos: Destrucción de datos. En este artículo se regulan no solo los datos personales sino también los no personales y los programas, estafa informática
Recientemente en abril del 2019 defensores de los derechos digitales y sector de tecnología de Australia buscan revertir el socavado de la ley de encriptado, a continuación, la nota de dicha noticia relevante;[174]
Esta ley puede favorecer a unos y desfavorecer a otros, sin embargo, se han creado y aprobado más de 75 leyes para el resguardo de la seguridad nacional, sin embargo, los efectos positivos y negativos se verán con el paso del tiempo, pero se especula que esta ley impactara a las financieras, a las industrias de información y tecnologías locales.
Canadá
Su integración económica con los Estado Unidos ha creado una red informática y la comunidad de internet muy dependiente a la de su vecino país del sur, junto con esta tecnología, sin embargo, también ha llegado delitos tanto de Estados Unidos, así como desde el interior. Canadá ha observado muy de cerca la proliferación de los delitos informáticos tanto de Estados Unidos, así como desee el interior. Canadá ha observado muy de cerca la proliferación de delitos informático y no ha tardado en la aplicación de medidas legislativas para corregir tal proliferación tal para que no le afecte, juntos con una aplicación bien definida y una estructura de mando han dado a Canadá una tasa de éxito casi inigualable en el trato con las piraterías. El gobierno canadiense ha sido muy agresivo en la aplicación de la legislación de los delitos informáticos. Existen básicamente dos secciones del código penal canadiense, secciones 342.1 está divida en dos partes. En Canadá la definición de los Delitos informáticos se ha tomado en la comunidad internacional Convenio sobre la Delincuencia que se produjo el 23 de noviembre de 2001, Canadá ha contribuido y es signatario, a este convenio internacional que implican el uso de los ordenadores:

[174] *GLOBAL VOICES, Noticias en línea con dirección URL: https://es.globalvoices.org/2019/07/04/defensores-de-derechos-digitales-y-sector-de-tecnologia-de-australia-buscan-revertir-ley-que-socava-encriptado/ consultado 04/03/2020.*

los delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, los delitos relacionados con la informática, delitos relativos al contenido, los delitos relacionados con infracciones de derechos de autor y derechos conexos, y la responsabilidad auxiliar. La Ley de Delitos contra la falsificación y el fraude relacionados con la informática el acceso ilegal, la intercepción ilegal, la interferencia de datos, la interferencia del sistema, mal uso de los dispositivos. Los delitos relacionados son: Pornografía infantil, los relativos a la violación de los derechos de autor y derechos conexos y los derechos digitales, los delitos de responsabilidad auxiliar incluyen cosas como la tentativa, la complicidad, y la responsabilidad corporativa. El robo, la falsificación de tarjetas de crédito y el uso no autorizado del equipo está regulado por la Sección 342. La privacidad está regulada por el artículo 184 y la suplantación de la sección 403, también algunos de los crímenes están regulados con la Ley C-46.

Estados Unidos

Es importante señalar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec 1030) que modificó el Acta de Fraude y Abuso Computacional) de 1986. Con la finalidad de eliminar los argumentos hipertónicos acerca de que es y que no es un virus, un gusano, un Caballo de Troya, etc. y en que difieren de los virus. Define dos niveles para el tratamiento de quienes crean este virus estableciendo para aquellos intencionalmente causan daño por la transmisión de un virus, el castigo es hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten solo de manera imprudente la sanción fluctúa entre una multa y un año de prisión.

Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple que se debe entender como acto delictivo. Mediante la creación de un régimen de protección, la DMCA exceptúa de responsabilidad a los proveedores de ciertos servicios por violaciones de derechos de autor cometidas por terceros. En este contexto, es importante en primer lugar poner de relieve que no todos los proveedores están abarcados en la limitación. Las limitaciones de responsabilidad se aplican únicamente a proveedores de servicio y proveedores de sistema de almacenamiento especial.

Código de Estados Unidos. La sección 1030. Fraude y otras actividades conexas relacionadas con las computadoras, el que a sabiendas acceso a una computadora sin autorización o excediendo el acceso autorizado, y por medio de dicha conducta con la información obtenida que ha sido determinado por el Gobierno de Estados Unidos en virtud de una Orden Ejecutiva o los estatutos que requieren una protección contra el uso no divulgación por razones de defensa nacional o las relaciones exteriores, o cualquier otra información restringida.

Reino Unido

Básicamente son dos leyes relativas a la utilización de equipo superior que han sido aprobados por el Gobierno británico, estas son la ley de protección de datos de 1984 y la ley del uso indebido de equipo de 1990. La primera trata generalmente de la adquisición y uso de datos personales, mientras que la segunda ley define los procedimientos y sanciones que rodean la entrada no autorizada en los equipos.

CAPITULO DE LA LEY DE LA POLICIA Y LA JUSTICIA 2006 MODIFICA LA LEY DE USO INDEBIDO DE ORDENADORES.

El acceso no autorizado a material informático: " Una persona culpable de una ofensa bajo esta sección ser responsable, a) en juicio sumario en Inglaterra y Gales, de prisión por un término no superior a los 12 meses o una multa que no exceda el máximo legal, o ambas; b) por condena sumaria, en Escocia, a una pena de prisión no superior a seis meses o una multa que no exceda el máximo legal o tanto, c) en caso de condena en la acusación, a una pena de prisión no superior a dos años o a una multa, o ambas. Para la sección 3 de Ley de 1990 (modificación no autorizada de material informático) es sustituido "tres actos no autorizados con la intención de perjudicar, o con temeridad en cuanto a alterar, el funcionamiento del equipo, etc.

4.1.2. Familia jurídica romano-germánica.

Es una de las familias que se pueden encontrar en la actualidad, ya que son herederos del derecho romano, tiene un énfasis en los valores de justicia y moral, impreso por el sistema religioso. Es la más antigua y difundida de las familias

Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos: Espionaje de Datos, Estafa informática, falsificación de datos probatoria junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad e ideológica, uso de documentos falsos, Alteración de datos es ilícito a cancelar, inutilizar o alterar datos inclusive la tentativa es punible.

Sabotaje informático se refiere a la destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa. Utilización abusiva de cheques o tarjetas de crédito (266b)

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de donde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeñaba un papel esencial la introducción del proceso electrónico de datos, así como acerca de que bienes jurídicos merecedores de protección penal resultaban así lesionados.

El gobierno de Alemania en 20 de septiembre propuso un nuevo proyecto de Ley Sobre el Delito Cibernético con el objetivo de cerrar las lagunas restantes. En su código Penal vigente penaliza todas aquellas conductas ilícitas respecto al manejo de datos de espionaje, alteración de los datos y el sabotaje de informático.

La última gran noticia que impacto a Alemania fue en el 2018 el cual habían estado ante la amenaza de las industrias, el cual representa un gran reto para erradicar y regular dicho ciberdelito.

La respuesta ante esta situación ha sido abordada por el Instituto Fraunhofer para la Investigación en Sistemas e Innovación. "Los resultados de sus encuestas demuestran que ninguna empresa puede sentirse segura", dice Esther Bollhöfer. Para el estudio, los investigadores analizaron diversos delitos, y, además, entrevistaron a docenas de expertos y cientos de empresarios. La dimensión real de los ataques podría ser mayor, puesto que muchas empresas callan, perciben

equivocadamente, o ni siquiera se percatan de ellos. Uno de cada cuatro ataques no fue denunciado ante las autoridades. Una de cada tres empresas se negó a describir su respuesta a ataque recibido. "En las empresas existe una gran inseguridad acerca del tema del espionaje", afirma Werner Heyer, de la Oficina de Investigación Criminal de Baden-Württemberg.[175]

Italia

La legislación de ese tipo está contenida en la sección de código italiano 547, que fue aprobada en diciembre de 1993 como parte de un proyecto de ley ms grande, básicamente fueron doce puntos en el proyecto de ley. Cuarto de los puntos de tratan de las posesión, alteración o destrucción de sistemas de datos o equipo. Otros cuatro establecen sanciones para el acceso no autorizado o pirateado en sistemas y posterior intercepción de comunicaciones, que conllevan una pena máxima de seis años. Los cuatro últimos puntos fueron más diversos en su naturaleza, uno analiza el crimen interceptar una transmisión electrónica, otro prohíbe la difusión de virus informáticos en la red, la tercera hace ilegal la posesión de dispositivos para interceptarse o interrumpir las comunicaciones, el punto final es probablemente el más intrigante, el cual establece penas más duras para la divulgación de información a otro sin buena causa.

El Senado del Parlamento italiano el 27 de febrero (2008) y aprobada ratificada la Convención sobre el Delito Cibernético del código penal el artículo 615 ter: El acceso no autorizado a una computadora o sistemas de telecomunicaciones:

España

La Ley de servicios de la sociedad de la información y del comercio electrónico tiene como objeto la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica.

El artículo 2 de la ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de Comercio Electrónico establece el ámbito de aplicación subjetivo de la ley a los prestadores de servicios establecidos en España.

En lo que respecta en la legislación de España al combate y regulación de los delitos cibernéticos se ha desarrollado enormemente no solo en el aspecto económico,

[175]*Made for maid, noticias en línea con dirección URL: https://www.dw.com/es/la-industria-de-alemania-ante-la-amenaza-de-los-hackers/a-47001762 consultado 05-03-2020.*

político sino en lo social y en la parte de derechos humanos ha evolucionado de manera positiva en cuanto a su legislación nacional, también ha firmado y ratificado tratados internacionales para contribuir a una regulación homogénea internacional.

Francia

Ley número 88-19 de 5 de enero de 1998 sobre el fraude informático. Tales como el acceso fraudulento a un sistema de elaboración de datos y el sabotaje informático. Así como el uso de documentos informatizados falsos. La ratificación del Consejo de Europa sobre la ciberdelincuencia se hizo el 10 de enero de 2006.

Venezuela

En el año 2001 se promulgo la Ley Especial contra los delitos informáticos por Asamblea Nacional de la República Bolivariana de Venezuela. De los Delitos Contra Sistemas que utilizan Tecnologías de la Información. De los delitos contra la propiedad intelectual, de los delitos contra la privacidad de las personas y de las comunicaciones, de los delitos contra los niños y niñas o adolescentes, de los delitos contra el orden económico, argumentados en 5 capítulos respectivamente.[176]

4.1.3. Familia Jurídica Asiática o Mixta.

Esta familia nace del poder judicial por medio de la jurisprudencia y hoy en día tiene una monarquía parlamentaria constitucional, Aunque el derecho japonés ha adoptado modelos extranjeros para sus códigos y busca integrar varios ordenamientos, no ha perdido su relación con la moral y el honor. El litigio no es más metodología ideal honorable para solucionar un conflicto, más bien participar de un juicio es considerado vergonzoso y moralmente indebido.

Japón

En efecto a partir del 3 de febrero 2000 mediante la Informática Ley de Acceso no autorizado. Además, se cuenta con el Convenio sobre Delincuencia, firmado desde 2004 por 31 países, exige a las partes criminalizar el acceso no autorizado a sistemas informáticos, el almacenamiento de pornografía infantil o la vulneración de derechos de autor.

[176] Ley Especial sobre los Delitos informáticos de Venezuela de 2001, texto completo http://www.tsj.gov.ve/lrgislacion/ledi.htm consultado 1 de mayo de 2019.

Tokio

El parlamento japonés aprobó hoy una ley que criminaliza la creación y distribución de virus informáticos, pese a las voces críticas que sostienen que podría infringir el derecho constitucional que garantiza la privacidad en las comunicaciones. Las autoridades niponas han tenido problemas para investigar ataques cibernéticos contra oficinas gubernamentales, corporaciones o individuos ante la ausencia de una ley nacional específicamente trazada para castigar la creación de virus y otros actos que dañen las redes informáticas.

Con la aprobación de la ley, el gobierno nipón tiene la intención de suscribir definitivamente el Convenio sobre Delincuencia que, pese ser aprobado por el Parlamento en 2004, no fue oficialmente ratificado ante la ausencia de normas antiguos de ámbito local en este terreno.

4.1.4. Familia Jurídica Socialista.

Es un mundo totalmente nuevo: los conceptos jurídicos, los principios, la estructura, las instituciones, los modos de vida y de pensamiento, y, en fin, las leyes, son diferentes a los de los restantes países no socialistas. En esta familia de derecho la base fundamental de la sociedad lo es la colectivización de los medios de producción y la planificación. En la familia de derechos socialista la ley constituye la principal fuente del derecho, es decir, existe una primacía de la ley. El derecho es un instrumento al servicio de la política del estado y del gobierno socialista.

China

Sin duda un punto donde China debe establecer normas para regular su creciente electrónica y la industria informática. Solo cabe esperar que esa legislación no de como resultado la persecución opresiva de la población.

El Ministerio de Industria de la Información (Departamento de Políticas, Leyes y Reglamentos) es una de las principales instituciones en la reforma de la ley vigente desde 1996.

Derecho Penal de la República Popular de China (14 de marzo de 1997) establece lineamientos para el uso de una computadora para el fraude financiero, robo, corrupción, malversación de fondos públicos, el robo de secretos de Estado o de otros delitos castigados conforme a las disposiciones pertinentes a esta ley.

Cabe destacar que el sistema que tiene China es que tiene su propio Internet y redes sociales, ya que YouTube, Google, Facebook, Wordpress, Instagram y twitter están bloqueadas China implemento su propio sistema tecnológico debido a que cuarta o resguarda la libertad de expresión y censura, porque las revelaciones que hizo Eduardo Snowden dice que controla toda la información de las redes sociales la Agencia nacional de Estados Unidos tiene acceso a todo y esto no le conviene para el Estado Chino.

Fue por eso que China decidió crear una guerra comercial ya que China combina la economía de mercado con un control muy fuerte sobre los sectores clave de la economía y al mismo tiempo tener un control estatal, busca promover una industria nacional por medio de un bloqueo y después dar apertura y competencia a otras industrias tecnológicas extranjeras. La copia de los servicios de Internet en China es; WeChat[177], Baido[178], Weibo[179], QQ[180], etc.

Se cuenta que el bloqueo que existe actualmente en China se debe a querer resguardar una serie de valores y costumbres de vida, aculturación, revolución cultural identidad tradicional que tiene China, sin embargo se ha pensado quitar en las zonas más turísticas este bloqueo ya que para los turistas entrar a China significa una desconexión total debido a que los sistemas tecnológicos no son los mismos que

[177] *Es una aplicación de mensajería instantánea con casi 500 millones de usuarios activos en China. "La mitad de los usuarios de teléfonos móviles del país accederán a la aplicación en 2017", informó eMarketer. A nivel mundial, el uso se estima entre 730 millones de usuarios activos de redes sociales, según Huileng Tan de CNBC, y 846 millones, según Hootsuite y We Are Social. Cualquiera que sea la cifra, la plataforma es demasiado grande como para ignorarla. En línea con dirección URL: https://ijnet.org/es/story/comprendiendo-las-redes-sociales-de-china consultado 05-03-2020.*

[178] *fue creado a finales de 1999 por Robin Li y Eric Xu con un diseño similar a Google, que brinda a los internautas chinos la posibilidad de buscar noticias, imágenes y archivos de audio. Este motor de búsqueda ofrece más de 740 millones de páginas web, 80 millones de imágenes y 10 millones de archivos multimedia, además de una enciclopedia colaborativa similar a Wikipedia, llamada Baidu Baike. En línea con dirección URL: https://ijnet.org/es/story/comprendiendo-las-redes-sociales-de-china consultado 05-03-2020*

[179] *Es conocido como el Twitter de China. Sin embargo, en términos de números puros, la red parece haber superado a Twitter, con 340 millones de usuarios activos (Twitter tiene 328 millones). Una razón clave de este crecimiento ha sido la evolución del servicio hacia una plataforma de blogs multimedia, con funcionalidades similares a las encontradas en Twitter, Pinterest y Tumblr combinadas, explica Yue Wang en Forbes. El resultado ha sido un aumento del uso por parte de los jóvenes, según el informe 2017 de Kantar sobre las redes sociales chinas. En línea con dirección URL: https://ijnet.org/es/story/comprendiendo-las-redes-sociales-de-china consultado 05-03-2020*

[180] *Fue lanzada hace 18 años y durante mucho tiempo fue la aplicación social más grande en China, solo superada por WeChat en el invierno pasado. Recientemente, QQ se cambió el nombre para centrarse en el entretenimiento y las subculturas jóvenes de China, con características similares a Snapchat, cuenta Rita Liao, de Technode. En línea con dirección URL: https://ijnet.org/es/story/comprendiendo-las-redes-sociales-de-china consultado 05-03-2020.*

hay en la mayor parte del mundo, por lo que se puede apreciar que en China existe una censura a la libertad de expresión con el mundo exterior. La única manera con la que algunos han podido conectarse con el mundo exterior es por medio de una red virtual que puede cruzar el gran cortafuego[181] que tiene China en lo tecnológico.

4.1.5. Familia Jurídica Supranacional.

Es una familia política en el cual determinados estados ceden parte de sus atribuciones de gobierno (en mayor o menor medida, dependiendo del grado de supranacionalidad) a organismos internacionales que afectan a más de una nación. Uno de los objetivos de las familias jurídicas supranacionales desde el punto de vista del globalismo es la internacionalización de la economía, la implantación de sistemas monetarios supranacionales, etc., aunque se pueden tener otros objetivos, como la regulación de las transacciones internacionales y la preservación de los derechos humanos, el medio ambiente y otros objetivos similares.

En esta familia jurídica política se advierte especialmente en que las decisiones de los organismos no necesitan ser refrendadas por los Estados para entrar en vigor (a diferencia de los tratados internacionales clásicos).

Unión Europea

Los poderes de la Unión Europea son limitados cuando se trata de legislar en la esfera del derecho penal. En efecto, la Unión solo tiene la posibilidad de armonizar el derecho penal de los Estados Miembros en esferas especiales, tales como la protección de los intereses financieros de la Unión Europea y el ciberdelito.

En 1999 la Unión Europea lanzó la iniciativa Europa, adoptando la Comunicación de la Comisión Europea publicó una comunicación que versaba sobre la creación de una sociedad de la información más segura, mejorando la seguridad de las estructuras de la información y luchando contra el ciberdelito. [182]

Tras participar en el Consejo de Europa y en los debates del G8, la Comisión reconoce la complejidad y la dificultad que plantean las cuestiones de procedimiento jurídico. En la decisión mencionada se toma nota que el convenio sobre la

[181] *Es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.*
[182] *Montoya Piña Javier Omar, Delitos Federales cometidos a través de Medios Informáticos.*

Delincuencia del Consejo de Europa se concentra en la armonización de las disposiciones del derecho penal sustantivo tendentes a proteger los elementos de las infraestructuras, que más adelante se explicara a detalle.

En cada una de las familias existe un avance por cuanto hacer a la legislación gubernamental o de uso exclusivo del Estado o Gobierno como es el caso de los Estados Unidos, Reino Unido, Japón y China; a la par en países como Italia, Alemania y España se ha logrado legislar sobre el acceso no autorizado a datos informáticos entre particulares, penando estas conductas ilícitas llevadas a cabo con el propósito de delinquir.

Con ellos se logra una regulación de los bienes informáticos, la protección de datos personales, la protección de la información exclusiva para el uso de gobierno, garantizando sus leyes que contienen prohibiciones, limites derivados de ordenamientos en su mayoría en materia penal que contiene conductas previstas y sancionadas, previniendo este tipo de conductas ilícitas y conflictos sociales derivados de ellas.

En México, el Capítulo II Segundo, Titulo IX Noveno del Código Penal Federal del "Acceso ilícito a sistemas y equipos de informática" protege y penaliza la información gubernamental, financiera y de seguridad publica restringida del Estado, protegidos por algún mecanismo de seguridad que se le impondrán" sin tomar en cuenta la protección a la seguridad del manejo de información por parte de los particulares.

A continuación, se mostrarán los organismos e instrumentos internacionales en materia de combate de los delitos informáticos.

4.1.6. Familia Jurídica. Caso de Rusia.

En el caso de Rusia se han hecho muchos intentos para poder identificar el sistema jurídico ruso haciendo hincapié a las varias revoluciones en las cuales sobrevivió y las cuales derivo en la transición del país del autoritarismo a la democracia moderada. Como se sabe la división tradicional de los sistemas jurídicos generalmente aceptada incluye al sistema Romano Germánico, el anglosajón y también tuvo sus especialidades, lo que provocó numerosas discusiones en la

ciencia jurídica. También sabemos que la iglesia ortodoxa ha tenido una gran influencia en el territorio ruso en la cual involucra su sistema jurídico. [183]

Rusia se ha caracterizado por convertirse en un paraíso de los ciberdelitos y un gran ejemplo de ello es la problemática que existe con el rasonwear que ya se explicó a detalle en el capítulo anterior, lo cual no han hecho nada sobre el asunto y lo catalogan como una superpotencia de los ciberdelitos en gran parte porque la línea entre el Gobierno y el crimen organizado es deliberadamente borrosa.[184]

Afirma el antiguo director de tecnología de la empresa de seguridad en la nube Crowdstrike y presidente del grupo de expertos centrado en la tecnología de Washington (EE. UU.) Silverado Policy Accelerator, Dmitri Alperovitch. "Hay 20 años de historia de Rusia albergando ciberdelincuentes. Como mínimo, hacen la vista gorda con los ciberdelincuentes; como máximo les apoyan, los animan, se lo ponen fácil.[185]

De acuerdo con el derecho internacional, los Estados tienen la responsabilidad de no permitir a sabiendas que su territorio se utilice para cometer delitos internacionales. Esto ocurre con mayor frecuencia en la piratería informática, pero también se aplica al terrorismo y al crimen organizado. Los acuerdos globales significan que los gobiernos están obligados a poner fin a esa actividad delictiva o, si no tienen la capacidad, a obtener ayuda para hacerlo. Sin embargo, se sabe que Rusia protege a sus hackers e incluso se asocia con ellos para llevar a cabo ataques en su nombre. Más a menudo, simplemente tolera e ignora a los delincuentes siempre que el país en sí no se vea afectado. Eso significa que los hackers omitirán rutinariamente cualquier ordenador que use el idioma ruso, por ejemplo, como un reconocimiento implícito para seguir el juego.

Mientras tanto, el Kremlin se suele resistir enérgicamente a los esfuerzos internacionales para dominar a los hackers limitándose a arrojar acusaciones al resto del mundo, sin reconocer que existe un problema y negándose a ayudar. El 11 de mayo, por ejemplo, poco después de la declaración de Biden, el portavoz del

---

[183] *MIRONOW Nicolas, Sistema jurídico de Rusia en línea con dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/7/3376/27.pdf consultado 29-06-2021.*

[184] *MIRONOW Nicolas, Sistema jurídico de Rusia, p.p 612.*

[185] *Noticia publicada el 1 de junio de 2021, más información en: https://www.technologyreview.es//s/13405/la-gravedad-del-ransomware-sigue-creciendo-ante-la-inaccion-de-rusia consultado 29-06-2021.*

Kremlin, Dmitry Preskov, negó públicamente la participación rusa. En cambio, criticó a Estados Unidos por "no querer cooperar con nosotros para contrarrestar las ciberamenazas".

Hay numerosos ejemplos de ciberdelincuentes profundamente entrelazados con la inteligencia rusa. El enorme hackeo de 2014 contra Yahoo acabó con cargos contra oficiales de inteligencia rusos y conspiradores ciberdelincuentes. El hacker Evgeniy Bogachev, que antes era el pirata informático bancario más prolífico del mundo, ha sido vinculado al espionaje ruso. Y en las raras ocasiones en las que los piratas informáticos acaban detenidos y extraditados, Rusia acusa a Estados Unidos de "secuestrar" a sus ciudadanos. Los estadounidenses replican que el Kremlin protege a sus propios criminales al impedir la investigación y su arresto.[186]

El beneficio para Rusia es difícil de medir claramente, pero hay algunas variables notables: los ataques ransomware desestabilizan a los adversarios de Moscú y transfieren la riqueza a los amigos de Moscú, todo sin muchas consecuencias negativas.

En cuanto a los ordenamientos de regulación en los ciberdelitos en Rusia son muchos con gran dificultad de traducir además son documentos que solo se pueden conseguir internamente por lo que se me ha obstaculizado y o solo mencionaré los siguientes:

- Ley Federal N ° 187-FZ sobre la seguridad de la infraestructura de información crítica de la Federación de Rusia

La ley, aprobada en julio de 2017, establece los principios básicos para garantizar la seguridad de la infraestructura de información crítica, los poderes relacionados de los organismos estatales rusos, así como los derechos, obligaciones y responsabilidades de las personas que poseen instalaciones con infraestructura de información crítica, proveedores de comunicaciones y sistemas de información que proporcionan interacción.[187]

---

[186] *HOWELL O´neill Patrick, MIT TECNOLOGY REVIEW, en línea con dirección URL: https://www.technologyreview.es//s/13405/la-gravedad-del-ransomware-sigue-creciendo-ante-la-inaccion-de-rusia consultado 29-06-2021.*

[187] *HOWELL O´neill Patrick, MIT TECNOLOGY REVIEW, en línea con dirección URL: https://www.technologyreview.es//s/13405/la-gravedad-del-ransomware-sigue-creciendo-ante-la-inaccion-de-rusia consultado 29-06-2021.*

Se entiende que los elementos de la infraestructura de información crítica son: sistemas de información, redes de telecomunicaciones de las autoridades estatales, sistemas y redes para la gestión de procesos tecnológicos que se utilizan en la defensa del estado, asistencia sanitaria, transporte, comunicación, finanzas, energía, industrias de combustible, industria nuclear, aeroespacial, minería, metalmecánica y química.[188]

Todas estas industrias se consideran críticas para la economía y deben protegerse contra cualquier amenaza cibernética. La ley requiere la implementación de medidas de protección, asignando la categoría de protección (de acuerdo con los estatutos) y luego registrándose en el Servicio Federal de Control Técnico y de Exportación, que estará a cargo de la supervisión en este campo.[189]

- Ley Federal N.º 152-FZ sobre datos personales

La Ley de datos personales, aprobada en julio de 2006, cubre casi todos los aspectos de la protección de datos. Por ejemplo; qué se considera datos personales, qué tipos de datos se pueden recopilar y procesar, cómo y en qué casos se pueden recopilar y procesar datos, y qué medidas técnicas y organizativas deben ser aplicado por empresas o individuos que recopilan datos.[190]

A diferencia de la legislación europea, la Ley de datos personales no distingue entre controladores de datos y procesadores de datos. Por lo tanto, cualquier persona o entidad que trabaje con datos personales se considera un operador de datos personales y se rige por la regulación de la Ley de Datos Personales.

También hay varias regulaciones específicas, aclarando las disposiciones de la Ley de Datos Personales. Dichas regulaciones son emitidas por el gobierno ruso, la autoridad de protección de datos rusa (el Servicio Federal de Supervisión en la

---

[187] *CIBERSEGURIDAD, ley rusa, en línea con dirección URL:https://ciberseguridad.com/normativa/rusia/ consultado 29-06-2021.*

[188] *HOWELL O´neill Patrick, MIT TECNOLOGY REVIEW, en línea con dirección URL: https://www.technologyreview.es//s/13405/la-gravedad-del-ransomware-sigue-creciendo-ante-la-inaccion-de-rusia consultado 29-06-2021.*

[188] *CIBERSEGURIDAD, ley rusa, en línea con dirección URL:https://ciberseguridad.com/normativa/rusia/ consultado 29-06-2021.*

[189] *CIBERSEGURIDAD, ley rusa, en línea con dirección URL:https://ciberseguridad.com/normativa/rusia/ consultado 29-06-2021.*

[190] *CIBERSEGURIDAD rusa, en línea con dirección URL:https://ciberseguridad.com/normativa/rusia/ consultado 29-06-2021*

Esfera de Comunicación, Tecnología de la Información y Comunicaciones Masivas) o las autoridades responsables de varios problemas de seguridad en Rusia, como el Servicio Federal de Control Técnico y de Exportación (FSTEK) o el Servicio Federal de Seguridad (FSB).[191]

La Ley de localización de datos fue muy criticada por las empresas y los medios de comunicación, pero entró en vigor en septiembre de 2015. Si bien esta ley generó una gran ganancia para los centros de datos rusos, también generó altos costes para las empresas, que debieron rediseñar su infraestructura de almacenamiento de datos.[192]

- Ley Federal No. 149-FZ sobre Información, Tecnologías de la Información y Protección de la Información (la Ley de Información)

Esta ley se fortaleció sustancialmente con algunas enmiendas adicionales y afecta a las industrias de telecomunicaciones e Internet de Rusia. En particular, los operadores móviles necesitarán almacenar las grabaciones de todas las llamadas telefónicas y el contenido de todos los mensajes de texto durante un período de seis meses, lo que conlleva enormes costes.[193]

Además, exige que dichos operadores proporcionen dichas comunicaciones a la policía y la inteligencia rusas a petición suya e instalen sistemas especiales utilizados para fines de investigación o concilien el uso de software y hardware con las autoridades. Y proporcionar a las autoridades de seguridad las claves de descifrado si los mensajes están encriptados.[194]

Otras normas que han implementado para regular los delitos cibernéticos a partir del 1 de noviembre del 2017 Rusia lanzo una iniciativa la cual consiste en la prohibición de los servicios de redes privadas virtuales (VPN) que no cooperan con el gobierno,

[191] *CIBERSEGURIDAD rusa, en línea con dirección URL:https://ciberseguridad.com/normativa/rusia/ consultado 29-06-2021*
[192] *CIBERSEGURIDAD rusa, en línea con dirección URL:https://ciberseguridad.com/normativa/rusia/ consultado 29-06-2021*
[193] *CIBERSEGURIDAD rusa, en línea con dirección URL:https://ciberseguridad.com/normativa/rusia/ consultado 29-06-2021*
[194] *CIBERSEGURIDAD ley rusa, IBID.*

por ejemplo, en relación con los derechos de autor, la protección de datos u otras infracciones de la ley.[195]

Otro mecanismo que es de suma importancia destacar, al igual que China, pero este apenas está comenzando es la idea de tener su propio internet para estar protegidos, lo cual promover un sistema nacional de Internet que será utilizado como una alternativa a la web más amplia, según informes de noticias locales. Aún no se sabe con claridad en qué etapa se encuentra el país, pero se está buscando la obtención de un Internet sólido, y seguramente más sencillo de controlar.

Rusia se ha inclinado cada vez más hacia ese enfoque, con el presidente Putin firmando una ley a principios de este año, Runet,[196] que construiría la infraestructura necesaria para mantener un Internet interno separado en caso de que tal cosa sea necesaria (o conveniente).

No es una tarea pequeña, lo que Rusia está intentando. Y aunque se habla aparentemente de soberanía e infraestructura robusta, las tensiones entre EEUU, Rusia, China, Corea del Norte y otros países con capacidades avanzadas de guerra cibernética también son parte de ella.

Una Internet rusa desconectada del mundo probablemente en este momento sería casi no funcional. Rusia, como todos los demás, depende de recursos ubicados en otras partes del mundo. Y la duplicación de muchos de esos recursos sería necesaria para que Internet funcione de manera normal, en caso de que el país decida retirarse a su caparazón por lo que sea razón.[197]

4.2. El papel de los principales organismos internacionales frente al tratamiento y combate de los Delitos Cibernéticos.

El crimen organizado ha ido desarrollándose e incrementando masivamente y operando con múltiples ataques a empresas, instituciones, públicas o de manera individual a niveles internacionales de manera veloz sirviéndose de la aparición y del

---

[195] *CIBERSEGURIDAD rusa, en línea con dirección URL:https://ciberseguridad.com/normativa/rusia/ consultado 29-06-2021*

[196] *Está dirigido solo a prevenir las consecuencias adversas de la desconexión global de la red global, que está controlada en gran medida desde el extranjero. Este es el punto, esto es lo que es la soberanía: tener recursos propios que puedan activarse para evitar la desconexión.*

[197] *CIBERSEGURIDAD rusa, en línea con dirección URL:https://ciberseguridad.com/normativa/rusia/ consultado 29-06-2021.*

alcance, así como de los beneficios del internet que nulifica la barrera de espacio y tiempo entre los países.

Existen lagunas en la legislación internacional y regional siguen siendo todavía mayores, por lo que es difícil hacer un seguimiento eficaz a los delincuentes. El principal problema es la falta de armonización internacional en materia de legislación de los delitos cibernéticos.

La investigación y el enjuiciamiento son difíciles, si la clasificación de delitos varía de país en país. Algunos de los esfuerzos para hacer frente a este reto se han realizado, y aunque muy valiosa, continúan siendo insuficientes. El internet es una herramienta de comunicación internacional y, por lo tanto, cualquier solución para asegurarlo debe buscarse a nivel mundial.

4.2.1 Organización de las Naciones Unidas (ONU).

En el 8 Congreso de las Naciones Unidos sobre prevención del delito y tratamiento del delincuente (celebrado en la Habana, Cuba del 27 agosto al 7 de septiembre de 1990). La Asamblea General de Naciones Unidas adoptó una Resolución que tenía por objeto la legislación contra el ciberdelito. Basándose en esta Resolución que tenía por (Resolución 45/121 (1990), las Naciones Unidas publicaron en 1994 un Manual sobre la prevención y el control de delitos informáticos.[198]

En 2000 la Asamblea General aprobó una Resolución sobre la lucha contra la utilización de la tecnología de la información con fines delictivos, que presenta cierta semejanza con el Plan de Acción de Diez Puntos adoptado por el G8 en 1997.[199]

En 2002 la Asamblea General aprobó otra Resolución sobre la lucha contra la utilización de la tecnología de la información con fines delictivos[200]. En la que señalan los métodos existentes en el plano internacional para combatir el ciberdelito y destacan varias soluciones, por citar algunas: elaborar leyes políticas nacionales y al adoptar prácticas para luchar contra la utilización de la tecnología de la información con fines delictivos, etc.

---

[198] *Manual de las Naciones Unidas para Prevención y el Control de los delitos informáticos en línea con dirección URL:*

[199] *El texto completo de la resolución http://www.unjin.org/Documents/EighthCongress.html consultado 11-06-19*

[200] *Óp. Cit.*

El sistema de Naciones Unidas se han aprobado Decisiones, Resoluciones y Recomendaciones sobre temas relacionados con el ciberdelito y entre las cuales, cabe citar por su importancia, las siguientes:

La Comisión de Prevención del Delito y Justicia Penal (Oficina de las Naciones Unidas contra la Droga y el Delito). En 2004 el Consejo Económico y Social de las Naciones Unidas, adopto una Resolución sobre cooperación internacional para prevenir, investigar, enjuiciar y castigar el fraude, la delictiva y la falsificación de identidad y delitos afines.[201] En 2007 el Consejo adopto una Resolución sobre cooperación internacional para impedir, investigar, enjuiciar y castigar el fraude económico y los delitos de usurpación de identidad conexos.[202]

En 2004 el Consejo adopto una Resolución sobre la venta de drogas ilícitas a través de Internet en la que se contemplaban expresamente el fenómeno relacionado con un delito cibernético.

El 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, organizado en Bangkok, Tailandia, en 2005, se aprobó una Declaración en la que se destaca la necesidad de unificar el combate contra el ciberdelito. Señalando "la práctica de los instrumentos vigentes y la preparación de medidas nacionales y el desarrollo de la cooperación internacional en el ámbito, que entre, de modo tal que se tome en consideración el fortalecimiento y la ampliación de medidas, en particular, contra el ciberdelito".

El 12º Congreso aprobó la Declaración de Salvador, que, entre otras cosas, abrió la puerta a los debates sobre nuevas respuestas nacionales e internacionales a la delincuencia cibernética e invito a reforzar la capacidad de los sistemas de justicia penal en la lucha contra el delito, y determino medios de prevenir y controlar las nuevas formas de delincuencia en todo el mundo.

Actualmente el 14º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal se celebrará en Kyoto (Japón) del 20 de abril de 2020 al 27 de abril de 2020, cuyos temas que se abordaran sobre este campo es sobre las "Tendencias

---

[201] *Resolución del ECOSOC 2004/26 Cooperación internacional en la prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados, http://www.un.org/ecosoc/docs/2004/Resolution%202004.-26pdf*

[202] *ECOSOC 2007/20 Resolución sobre la cooperación internacional en la prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados, http://www./ecosoc/docs/2007/Resolution 202007. Pdf.*

delictivas actuales, fenómenos recientes y soluciones emergentes, en particular la utilización de nuevas tecnologías como medio e instrumento contra el delito. Entre otros.

4.2.2. Unión Internacional de Telecomunicaciones (UIT.

Como organismo especializado del sistema de las Naciones Unidas, la Unión Internacional de Telecomunicaciones (UIT)[203] desempeña un cometido rector en lo que concierne a la normalización y el desarrollo de las telecomunicaciones, así como a los diferentes aspectos de la ciberseguridad. Entre otras actividades, la UIT hizo las veces de organismo rector de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) que se organizó en dos fases, la primera en Ginebra Suiza, (2003) y la segunda en Túnez (2005). En la Cumbre de gobiernos, formuladores de políticas y expertos de todo el mundo intercambiaron ideas y experiencias acerca de la forma más adecuada de abordar las cuestiones que empezaba a plantear el desarrollo de una sociedad de la información mundial, lo que incluía la definición de normas y leyes compatibles.

La confianza y la seguridad son unos de los pilares más importantes de la Sociedad de la Información; los gobiernos, en cooperación con el sector privado, deben prevenir, detectar y responder la ciberdelincuencia y el uso indebido de las TIC.

El delito cibernético se discutió en Túnez en 2005. En la Agenda de Túnez para la sociedad de la Información se hacía hincapié en la necesidad de promover la cooperación internacional para combatir el ciberdelito.

En 2007, el secretario general de la UIT, destacó la importancia de la cooperación internacional en lo que respecta a la lucha contra el ciberdelito y anuncio el lanzamiento de la Agenda sobre Ciberseguridad Global de la UIT. La Agenda contiene siete objetivos clave, basados, a su vez, en cinco pilares estratégicos, entre otros, la elaboración de estrategias para la información de legislación modelo contra el ciberdelito. Los objetivos precitados como “preparar estrategias que promuevan el desarrollo de una legislación modelo sobre ciberdelito, definir estrategias”

---

[203] *Con sede en Ginebra, fue fundada como la Unión Telegráfica Internacional en el año 1865. Se trata de un organismo especializado de las Naciones Unidas. La UIT cuenta con 191 Estados Miembros y más de 700 Miembros de Sector y Asociados*.

Los resultados de la Cumbre se consignan en la Declaración de Principios de Ginebra, el compromiso de Túnez y la Agenda de Túnez para la Sociedad de la información.

4.2.3. Organización de Cooperación y Desarrollo Económicos (OCDE).[204]

En 1983 inició un estudio sobre la posibilidad de emprender una armonización internacional del derecho penal vigente para abordar el problema que representa el delito cibernético. La OCDE público en 1985 un Informe que analizaba la legislación vigente y formulo propuestas para combatir el ciberdelito.

En 1990 el Comité de Políticas de Información, Informática y Comunicación (ICCP) creo un Grupo de Expertos para preparar un conjunto de directrices de seguridad de la información que se determinaron de redactar en 1992 y fueron adoptadas ese año por el Consejo de la OCDE. En 2001 un segundo Grupo de expertos, que actualizo las directrices.

En 2002 una nueva versión de las directrices de seguridad de los sistemas y redes de información en el marco de una cultura de seguridad de la OCDE se adoptaron como recomendación del Consejo de la OCDE las directrices contienen 9 principios complementarios como sensibilización, responsabilidad, respuesta ética, democracia, evaluación del riesgo diseño e implementación en materia de seguridad, gestión de la seguridad y revaluación.

La OCDE afirmo en 2015 que México es el país más inseguro en cuanto a delitos derivados de las Tecnologías de la Información y la Comunicación (TIC´s) ya que se han ampliado las posibilidades de la delincuencia y la impunidad a niveles impensables a través de la manipulación fraudulenta de computadoras, destrucción de programas o datos, y afectación indebida de la privacidad, por ejemplo, se comenten fraudes electrónicos, clonación de tarjetas, robo de base de datos, bloqueo de portales, jaqueo de cuentas de correo, pornografía infantil, grooming y sexting, entre otros, sin que las autoridades mexicanas puedan enfrentarlos porque carecen de un marco legal, recursos humanos e infraestructura adecuados para ello.

---

[204] La Organización para la Cooperación y el Desarrollo fue fundada 1961, cuenta con 36 Estados miembros y se basa en París. Mas información, http://www.oecd.org/ consultado 24-10-20.

4.2.4. INTERPOL (Organización Internacional de Policía Criminal).

Es una organización intergubernamental que cuenta con 194 países miembros. Ayudamos a la policía de estos países a colaborar entre sí para hacer del mundo un lugar más seguro. Facilita el intercambio y acceso a información sobre delitos y delincuentes. También les ofrecemos apoyo técnico y operativo de diversa índole, tiene su sede en Lyon, Francia.

El principal ámbito de acción del Programa de INTERPOL sobre Ciberdelincuencia es abordar la "ciberdelincuencia pura", delitos contra ordenadores y sistemas de información en los que el objetivo es acceder sin autorización a un dispositivo o denegar el acceso a un usuario legítimo (típicamente mediante el uso de software malicioso). No obstante, INTERPOL reconoce la importancia de la lucha contra los delitos cibernéticos en los que el uso de ordenadores y sistemas de información amplifican el delito, como el fraude financiero y el uso terrorista de los medios sociales. Además, existe una creciente demanda de especialistas forenses informáticos para apoyar la lucha contra muchos tipos de delitos.[205]

La INTERPOL contiene un modelo operativo el cual hace mención que los delitos cibernéticos actuales son más complejos. Están interconectados y están a escala mundial, tanto en un ámbito físico como virtual. La cooperación policial multilateral es más necesaria hoy en día para hacer frente a los problemas de seguridad que afectan a las sociedades.

Esta organización está en una situación idónea para trabajar con las fuerzas del orden de todo el planeta a fin de reforzar su capacidad para prevenir la delincuencia e identificar y detener a los delincuentes. Las alianzas con otras organizaciones regionales e internacionales intensifican el enfoque combinado para afrontar los problemas comunes.[206]

Las actividades de INTERPOL giran en tomo a tres programas sobre delincuencia a escala internacional- lucha contra el terrorismo, delincuencia organizada y nuevas tendencias delictivas, y ciberdelincuencia para cada uno de los cuales se ha

[205] *Organización Internacional de Policía Criminal, en línea con dirección URL: https://www.interpol.int/es consultado 17-04-2021.*
[206] *INTERPOL, IBID.*

desarrollado una estrategia que abarca el periodo 2016-2020. Estas estrategias, y las iniciativas que engloban, irán evolucionando para adecuarse a la naturaleza dinámica del entorno operativo.

Los mencionados programas cuentan con el apoyo de un conjunto de capacidades policiales que la Organización proporciona a los miembros, a saber: gestión de datos policiales, análisis de información criminal, apoyo en materia forense, apoyo a las investigaciones sobre prófugos, Centro de Mando y Coordinación, capacitación y formación, innovación y proyectos especiales. Aunque es de gran importancia estar al día con este tema debido al gran desarrollo que tiene ante la sociedad internacional y sus circunstancias.[207]

4.2.5. Consejo de Europa.[208]

En 1989, el Comité Europeo para Asuntos Delictivos adopto el Informe de expertos sobre el delito cibernético, en la cual se analizaban las disposiciones de derecho penal sustantivas que exigía la lucha contra nuevos tipos de delitos electrónicos, incluido el fraude cibernético y la falsificación cibernética. Reunido en 1989, el Comité de ministros adopto una Recomendación, en donde se destacaba concretamente la índole internacional del ciberdelito:

De conformidad con el Articulo 15.b del “considerado que el delito cibernético suele tener carácter transfronterizo…”

En abril de 2009 firmaron el Convenio sobre la Ciberdelincuencia que más adelante se explicará a detalle 46 Estados y 25 Estados lo habían ratificado. Países tales como Argentina, Pakistán, Filipinas, Egipto, Botswana y Nigeria han redactado ya partes de su legislación con arreglo al Convenio. Si bien dichos países no han firmado aún el Convenio apoyan el proyecto de armonización y normalización propuesto por los redactores del Convenio. Actualmente, se reconoce que el Convenio es un importante instrumento internacional para luchar contra el ciberdelito y como tal ha recabado el apoyo de diferentes organizaciones internacionales.

---

[207] *INTERPOL, IBID.*

[208] *El Consejo de Europa, con sede en Estrasburgo y fundada en 1949, es una organización internacional que representa a 47 miembros Estados de la región Unión El consejo de Europa no debe ser confundido con el Consejo de la Unión Europea y la Unión Europea.*

Algunos países en los que se protege apreciablemente el principio de libertad de expresión señalaron con preocupación que si se incluían disposiciones en el Convenio que violaran la libertad de expresión, no podrían firmar el Convenio. De ahí que estas cuestiones se integrasen en un Protocolo separado. En octubre de 2008 habían firmado el Protocolo Adicional 20 Estados y 13 Estados lo habían ratificado.
Dada su óptica de mejorar la protección de menores contra la explotación sexual, el Consejo de Europa preparo un nuevo Convenio en 2007.[209] Uno de los objetivos esenciales del Convenio es unificar las disposiciones de derecho penal encaminados a proteger a los menores contra la explotación sexual.

4.2.6. Unión Africana.

Durante la Conferencia extraordinaria de Ministros de la Unión Africana encargados de las tecnologías de la comunicación y la información que se celebró en Jhonaesburgo en 2009, los participantes abordaron distintos temas relacionados con las TIC en los países africanos que la Comisión de la Unión Africana junto a la Comisión de la Unión Africana junto con la Comisión Económica de África de las Naciones Unidas debía elaborar un marco legal para los países Africanos en el que se abordan cuestiones como las transacciones electrónicas, la ciberseguridad y la protección de datos.[210]
En 2011, la Unión Africana ha presentado el proyecto de Convenio de la Unión Africana sobre el Establecimiento de un Marco Legal Fiable para la Ciberseguridad en África. La intención de sus redactores es fortalecer la legislación en vigor en los Estados Miembros en lo que respecta a las tecnologías de la información y la comunicación. En lo que atañe al mandato, éste no se limita al ciberdelito, sino que incluye otras cuestiones de la sociedad de la información tales como la protección de los datos y las transacciones electrónicas.

---

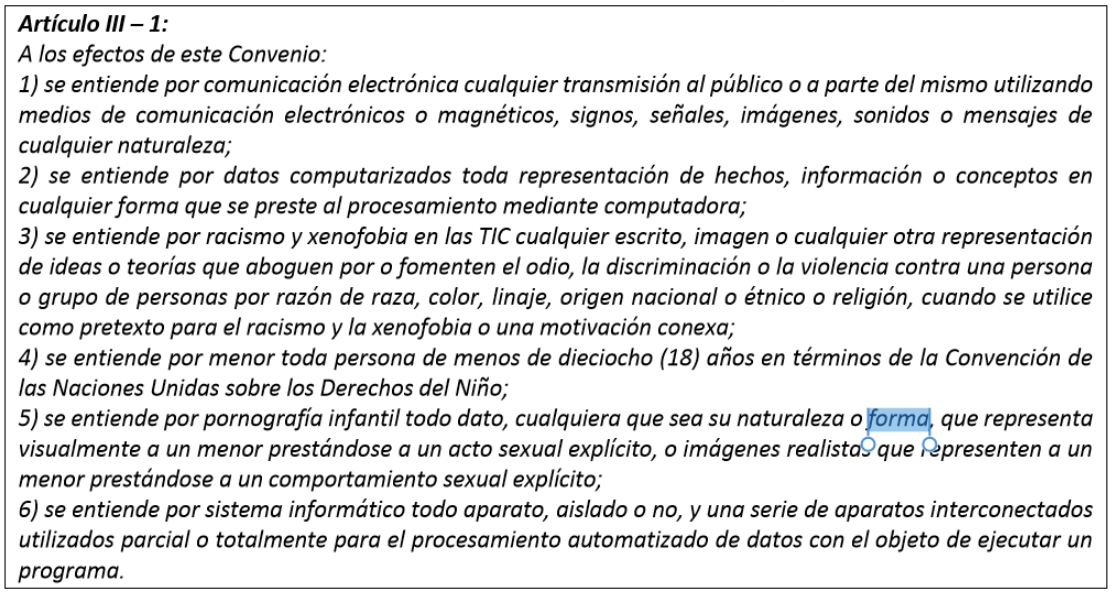
[209] *Consejo de Europa, Consejo de Europa sobre la Protección de los Niños contra la Explotación Sexual y Sexual Abuso (CETS No. 201)*
[210] *UIT, Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica en línea con dirección URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf consulta 27-03-2020.*

El Convenio tiene un alcance más global que la mayoría de los demás enfoques regionales. Se divide en cuatro partes. La primera parte se refiere al comercio electrónico, y aborda distintos aspectos tales como la responsabilidad contractual de un proveedor electrónico de bienes y servicios, la presentación de las obligaciones del tratado en formato electrónico y la seguridad de las transacciones electrónicas. La segunda parte trata de cuestiones relativas a la protección de los datos. La tercera parte se refiere a la lucha contra el ciberdelito. La Sección 1 se divide en cinco capítulos. Incluye un conjunto de seis definiciones (comunicación electrónica, datos computarizados, racismo y xenofobia en las TIC, el menor, la pornografía infantil y los sistemas informáticos, Además, en la tercera parte se aborda la necesidad de una política nacional de ciberseguridad y de una estrategia en esta materia. El segundo Capítulo trata de aspectos generales relacionados con las medidas legales. Se incluyen normas relacionadas con las autoridades reglamentarias, los principios democráticos, la protección de la infraestructura de información esencial, la armonización, la doble criminalidad y la cooperación internacional.

El tercer Capítulo aborda cuestiones relacionadas con un sistema nacional de ciberseguridad. Trata, entre otros temas, una cultura de la seguridad, el papel del gobierno, las asociaciones público-privadas, la educación y la formación y la sensibilización del público. El Capítulo cuatro está dedicados a las estructuras nacionales de vigilancia de la ciberseguridad.

El Capítulo cinco trata de la cooperación internacional. La diferencia principal respecto de otros marcos regionales comparables, tales como el Convenio del Consejo de Europa sobre la Ciberdelincuencia, radica en el hecho de que –de no existir otro instrumento de cooperación internacional en esta materia– el proyecto de Convenio de la Unión Africana no puede utilizarse con este fin. La diferencia de concepto se manifiesta expresamente en los Artículos 21 y 25.[211]

[211] *UIT, Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica en línea con dirección URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf consulta 27-03-2020..*



Artículo III – 1:
A los efectos de este Convenio:
1) se entiende por comunicación electrónica cualquier transmisión al público o a parte del mismo utilizando medios de comunicación electrónicos o magnéticos, signos, señales, imágenes, sonidos o mensajes de cualquier naturaleza;
2) se entiende por datos computarizados toda representación de hechos, información o conceptos en cualquier forma que se preste al procesamiento mediante computadora;
3) se entiende por racismo y xenofobia en las TIC cualquier escrito, imagen o cualquier otra representación de ideas o teorías que aboguen por o fomenten el odio, la discriminación o la violencia contra una persona o grupo de personas por razón de raza, color, linaje, origen nacional o étnico o religión, cuando se utilice como pretexto para el racismo y la xenofobia o una motivación conexa;
4) se entiende por menor toda persona de menos de dieciocho (18) años en términos de la Convención de las Naciones Unidas sobre los Derechos del Niño;
5) se entiende por pornografía infantil todo dato, cualquiera que sea su naturaleza o forma, que representa visualmente a un menor prestándose a un acto sexual explícito, o imágenes realistas que representen a un menor prestándose a un comportamiento sexual explícito;
6) se entiende por sistema informático todo aparato, aislado o no, y una serie de aparatos interconectados utilizados parcial o totalmente para el procesamiento automatizado de datos con el objeto de ejecutar un programa.

Esta imagen es solo una muestra de todo lo que la Unión Africana ha ido desarrollando para regular, combatir y erradicar a los delitos cibernéticos y más aspectos que van de la mano.

4.2.7. Liga Árabe y el Consejo de Cooperación del Golfo.

Varios países de la Región Árabe han tomado ya medidas nacionales y adoptando diferentes enfoques para luchar contra el ciberdelito, o se encuentran preparando legislación al respecto. Entre estos países, cabe citar: Pakistán Egipto y Emiratos Árabes Unidos. El Consejo de Cooperación del Golfo recomendó en una Conferencia celebrada en 2007 que los países del Consejo de Cooperación del Golfo intentasen definir un enfoque común en el que se tomaran en consideración diferentes normas internacionales.

Recientemente varios países de la Región Árabe ya han tomado medidas en el plano nacional y adoptado diferentes enfoques para luchar contra el ciberdelito, o se encuentran preparando legislación al respecto. Entre estos países, cabe citar: Pakistán, Egipto y los Emiratos Árabes Unidos (EAU). Con el fin de armonizar la legislación en la región, los EAU presentaron una legislación modelo a la Liga Árabe (Ley de Orientación para la Lucha contra el Crimen de IT). En 2003, el Consejo Árabe de ministros del Interior y el Consejo Árabe de ministros de Justicia adoptaron la legislación. En una Conferencia celebrada en 2007, el Consejo de Cooperación del

Golfo recomendó que los países que lo integran intentasen definir un enfoque común en el que se tomaran en consideración diferentes normas internacionales.[212]

4.2.8. Organización de los Estados Americanos (OEA).

Desde 1999 ha venido ocupándose activamente de la cuestión en la región. Entre otras cosas, la Organización ha celebrado una serie de reuniones dentro del mandato y alcance de la Reunión de ministros de Justicia o ministros o Procuradores Generales de las Américas (REMJA).

En el año 2000, los ministros de Justicia o ministros o Procuradores Generales de las Américas abandonaron el tema que representaba el ciberdelito y convinieron en una serie de recomendaciones. Estas recomendaciones entre las cuales cabe citar las siguientes, fueron reiteradas en la reunión de 2003.

Que se apoye el examen de las recomendaciones efectuando por el Grupo de Expertos Gubernamentales en su reunión inicial, como contribución de la REMJA a la elaboración de la Estrategia Comprensiva Interamericana de la OEA para combatir amenazas a la ciberseguridad cibernética, señalada en la Resolución de la Asamblea General de la OEA AG/RES. /XXXIII-0/03), y pedir al grupo que, a través de su presidente, siga apoyando la preparación de la Estrategia.

Los ministros de Justicia o ministros o Procuradores Generales de las Américas (REMJA) han celebrado siete reuniones hasta la fecha. Las reuniones más recientes fueron las organizadas en Washington D.C, Estados Unidos, en abril del 2006 y abril de 2008. Entre las recomendaciones formuladas en la reunión de 2006 pueden citarse las siguientes:

Que prosiga el fortalecimiento de la cooperación con el Consejo de Europa. Así mismo, que sigan realizando esfuerzos para fortalecer los mecanismos de intercambio de información y cooperación con otras organizaciones internacionales en la esfera del ciberdelito, tales como las Naciones Unidas, la Unión Europea, el Foro de Cooperación y con otras organizaciones Internacionales en la esfera del ciberdelito, tales como las Naciones Unidas, las Unión Europea, el Foro de

[212] *UIT, Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica en línea con dirección URL: https://www.itu.int/en/ITUD/Cybersecurity/Documents/Cybercrime2014_S.pdf consulta 27-03-2020.*

Cooperación Económica Asia-Pacifico, la OCDE, el G7, la Commonwealth e Interpol, para que los Estados Miembros de la OEA aprovechen los progresos alcanzados en dicho foros.

Han establecido miembros unidades especializadas para investigar el ciberdelito e identificar a las autoridades que se encargan de la coordinación a este respecto. Estas recomendaciones fueron retiradas en la reunión de 2008. Que las secretarias del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Trabajo sobre Ciberdelito, sigan realizando actividades permanentes de coordinación y cooperación para garantizar la implementación de la Estrategia Compresiva Interamericana de la OEA para combatir amenazas a la seguridad cibernética, adoptada por la Asamblea General de la OEA en la Resolución AG/RES.

Por lo que respecta a América Latina, Costa Rica es el único país que cuenta con presencia internacional en el tema, mediante la adhesión en el Convenio sobre la Ciberdelincuencia hecho en Budapest el 23 de noviembre de 2001, siendo invitado por el Comité de ministros del Consejo de Europa de conformidad con su artículo 37.

En el Caribe en diciembre de 2008, la UIT[213] y la Unión Europea presentaron el proyecto titulado "Mejora de la competitividad en el Caribe a través de la armonización de las políticas, la legislación y los procedimientos reglamentarios relativos a las TIC" (HIPCAR) destinado a promover el sector de las TIC en la región del Caribe. Este proyecto se inscribe en el programa "ACP-Tecnologías de la información y la comunicación" y el noveno Fondo Europeo de Desarrollo. Los beneficiarios son 15 países del Caribe. El objetivo del proyecto es prestar asistencia a los países del CARIFORUM para que armonicen sus políticas y marcos jurídicos en el ámbito de las TIC.[214]

En el marco de este proyecto, se definieron nueve áreas de trabajo en las que se desarrollaron políticas modelo y textos legislativos modelo para facilitar la formulación y armonización de la legislación en la región. El ciberdelito era una de las nueve áreas de trabajo. La elaboración del modelo de texto legislativo se desarrolló

[213] *Organización Internacional de Telecomunicaciones*.
[214] *MONTOYA Piña Javier Omar, "Delitos Federales cometidos a través de Medios Informáticos, Capitulo 1, pp.49*

en tres fases. En la primera fase, se recopiló y examinó la legislación existente en los países beneficiarios. En paralelo, se determinaron prácticas óptimas regionales e internacionales. Se dio prioridad a las normas que fueran directamente aplicables en al menos uno de los países beneficiarios (por ejemplo, la Ley modelo de la Commonwealth de 2002). No obstante, el examen también incluyó las prácticas óptimas de otras regiones, tales como la UE y África. El informe de evaluación incluía una visión general de la legislación existente, así como un análisis jurídico comparativo entre la legislación existente y las prácticas óptimas regionales e internacionales. Con el fin de preparar un análisis sobre las carencias detectadas, el informe de evaluación definió además las necesidades específicas de la región (tales como la legislación sobre el spam) que no son abordadas necesariamente por las prácticas óptimas internacionales. En un taller celebrado en 2010, se discutió el citado informe de evaluación con las partes interesadas de los países beneficiarios. Sobre la base del informe de evaluación y del análisis de carencias, las partes interesadas elaboraron unas directrices políticas modelo.[215]

En la segunda fase, se desarrolló un texto legislativo modelo que tenía en cuenta las directrices políticas. En un segundo taller, expertos en materia de políticas, redactores legislativos y otras partes interesadas de los países beneficiarios discutieron y enmendaron el proyecto de texto legislativo modelo que fue preparado para la reunión, y lo adoptaron. El texto legislativo modelo tiene tres objetivos clave: proporciona un modelo de lenguaje específico que se ajusta a las prácticas óptimas internacionales, responde a las demandas específicas de la región, y se desarrolla teniendo presentes las prácticas en materia de redacción legislativa de la región, a fin de velar por la facilidad de su aplicación. El texto legislativo modelo incluye un conjunto complejo de definiciones, así como disposiciones penales sustantivas, incluidas las que tratan de cuestiones como el SPAM, que tienen un carácter prioritario para la región pero que no estaban necesariamente recogidas en marco regionales tales como el Convenio del Consejo de Europa sobre la Ciberdelincuencia.[216]

---

[215] *MONTOYA Piña Javier Omar, "Delitos Federales cometidos a través de Medios Informáticos, Capitulo 1, pp.50*

[216] Op. Cit. p.p. 51

La UIT y la UE, en paralelo con el proyecto cofinanciado por ellas en la región del Caribe, han presentado un proyecto en el Pacífico (ICB4PAC). El proyecto tiene como finalidad –sobre la base de una solicitud formulada por los países insulares del Pacífico– proporcionar capacitación en materia de políticas y reglamentos de TIC. A este respecto, se centra en el desarrollo de la capacidad humana e institucional en el ámbito de las TIC recurriendo para ello a medidas de formación y educativas y al intercambio de conocimientos. Los beneficiarios son 15 países insulares del Pacífico. En marzo de 2011 se celebró un taller que trataba de la actual legislación en materia de ciberdelito en la región del Pacífico, que tuvo lugar en Vanuatu. Durante el taller se presentó un análisis jurídico comparativo global que facilitó una visión general acerca de la legislación en vigor en la región, así como una comparación con las prácticas óptimas seguidas en otras regiones. En agosto de 2011, y como continuación de este taller, se organizó en Samoa una conferencia para tratar de las técnicas de elaboración de las políticas y la legislación en materia de ciberdelito. Durante la conferencia se presentaron prácticas óptimas de otras regiones y se desarrollaron estructuras para lograr una legislación y una política armonizadas. Se abordaron la legislación penal sustantiva, la legislación procesal, la cooperación internacional, la responsabilidad de los proveedores de servicios de Internet (ISP), las pruebas electrónicas y las medidas de prevención del delito.[217]

En abril de 2011, la Secretaría de la Alianza del Pacífico organizó una conferencia relacionada con la lucha contra la ciberdelincuencia en el Pacífico El evento fue coorganizado por el Consejo de Europa. Durante la conferencia se trataron aspectos relacionados con la legislación penal sustantiva, la legislación procesal y la cooperación internacional.

México no ha asignado ninguno de los instrumentos mencionados en el tema solo ha servido como observador, motivo por el cual no cuenta con los instrumentos jurídicos para aplicarlos al caso concreto.

Este convenio es considerado como el estándar mundial en esta materia, lo que ha cerrado la posibilidad de que se elabore un Convenio Interamericano sobre Delitos Informáticos, como se sugirió en Foro Legislativo en Materia de Delitos Cibernéticos

[217] Op. Cit.p.p. 52

llevado a cabo en la Ciudad de México en el año 2004. En indispensable que México participe como miembro activo en las comunidades citadas, en virtud de que el no contar con la facultad para aplicar algún convenio en la materia representa la perdida valiosa de integración al consenso internacional en la persecución de las nuevas formas de delincuencia ejecutadas a través de los medios informáticos.[218]

4.2.9. EL G7.

En1997 el Grupo de los Ocho (formado por Canadá, Francia, Alemania, Italia, Japón, Gran Bretaña, Estados Unidos y Rusia[219]). La Presidencia del grupo que representa a más del 60% de la economía mundial.) (G7) estableció un Subcomité[220] sobre delitos de alta tecnología y cuyo objetivo es luchar contra el ciberdelito[221] además de mejorar la aplicación de las cuarenta recomendaciones adoptados por los jefes de Estado del G7 en 1996. Durante la reunión del G7, celebrada en Washington D.C Estados Unidos, los ministros de Justicia y del Interior del G7 adoptaron Diez Principios y un Plan Acción de diez puntos para combatir el delito de alta tecnología.

---

[218] *MONTOYA Piña Javier Omar, "Delitos Federales cometidos a través de Medios Informáticos, Capitulo 1, pp.48*

[219] Desde 2014 acordaron dar una exclusión provisional a Rusia debido a la tensión provocada entre las principales potencias occidentales y Rusia por la declaración de independencia de Crimea de Ucrania y su posterior anexión a la Federación Rusa, los antiguos miembros del G7 acordaron boicotear el encuentro previsto en Sochi (Rusia) y reunirse alternativamente en Bruselas, declarando que no habría más encuentros con Rusia en el contexto del G8 hasta nuevo aviso. Sin embargo, y en todo caso, no se trata de una suspensión de pertenencia o una expulsión como tal, dado que el G8 es un club informal que carece de estatutos. En línea con dirección URL:https://www.teinteresa.es/mundo/potencias-excluyen-Rusia-G8-cambie_0_1107491304.html#sr=g&m=o&cp=or&ct=-tmc&st=(opu%20qspwjefe)&ts=1394304595 consultado 30/01/2023.

[220] *La idea de la creación de cinco subgrupos- entre ellos, uno en delitos de alta tecnología, fue mejorar la aplicación de las cuarenta recomendaciones adoptados por los jefes de Estado del G8 en 1996.*

[221] *El establecimiento del Subgrupo (también descrito como el Subgrupo del "Grupo de Lyon") continuos esfuerzos del G8 (en ese momento G7) en la lucha contra el crimen organizado, que se inició con el lanzamiento del Grupo de expertos de alto nivel sobre los crímenes organizados (el "Grupo de Lyon") en 1995. En la cumbre de Halifax en 1995 del G8 expresaron "Reconocemos que el éxito final requiere que todos los gobiernos establezcan medidas efectivas para prevenir el blanqueo de capitales procedentes del tráfico de drogas y otros delitos graves. Para llevar a cabo nuestros compromisos en la lucha contra la delincuencia organizada transnacional, hemos establecido un grupo de expertos de alto nivel con un mandato temporal para ver los arreglos existentes para la cooperación tanto bilateral como multilateral para identificar lagunas importantes y las opciones para para mejorar coordinación y proponer acciones concretas para colmar esas lagunas".*

Los jefes de Estado apoyaron ulteriormente estos principios, entre los cuales cabe citar lo siguiente:

“No puede haber refugios para aquellos que utilizan de forma abusiva las tecnologías de la información; todos los Estados interesados habrán de investigar la comisión de delitos internacionales de alta tecnología, así como el enjuiciamiento de sus autores, con los correspondientes daños, entre otros”.

En 1999 el G7 especifico la actuación que tenía prevista para luchar contra el delito de alta tecnología en la Conferencia Ministerial sobre la Lucha contra el Delito Transnacional celebrada en Moscú, Federación de Rusia. Los participantes en el G7 expresaron su preocupación acerca de los delitos tales como la pornografía infantil, así como sobre la posibilidad de rastrear las transacciones y el acceso transfronterizo para almacenar datos. En el comunicado publicado con motivo de la Conferencia se consigna varios principios sobre la lucha del ciberdelito, que figuran actualmente en una serie de estrategias internacionales.

Uno de los logros prácticos de las tareas efectuadas por varios Grupos de expertos ha sido la preparación de una red internacional de contactos las 24 horas del día 7 días por semana, red que exige que los países participantes establezcan, coordinados de las investigaciones transnacionales que se realicen, coordinadores que deberán estar accesibles las 24 horas del día y 7 días por semana.[222]

En 2004, los ministros de Justicia y del Interior del G7 expidieron un comunicado en el que señalaron que había que considerar la necesidad de crear capacidades mundiales para combatir la utilización delictiva de Internet.[223]

---

[222] *La idea de una red 24/7 ha sido recogida por una serie de enfoques internacionales en la lucha contra la ciberdelincuencia. Un ejemplo es el artículo 35 de la Convención sobre el Delito Cibernético: (1) Cada Parte designara un punto de contacto disponible las veinticuatro horas, siete días a la semana base, a fin de garantizar la prestación de asistencia inmediata con el objetivo de las investigaciones o procedimientos relativos a delitos relacionados con la informática sistemas y datos, o para la obtención de pruebas en formato electrónico de una infracción penal. Dicha asistencia incluirá la facilitación, o, si lo permite su legislación y practica nacionales, directamente a la realización de las medidas: a) la prestación de asesoramiento técnico; b) la conservación de los datos de conformidad con los artículos 29 y 30; c) la obtención de pruebas, el suministro de información jurídica, y la localización de los sospechosos.*

[223] *G8 Comunicado de Justicia e Interior, Washington DC, 11 de mayo 2004.*

4.2.10. Foro de Cooperación Económica Asia-Pacifico (APEC).[224]

El Foro de Cooperación Económica Asia-Pacífico (APEC) identificó al ciberdelito como un importante ámbito de actividad y los dirigentes del APEC hicieron un llamamiento para promover una cooperación más estrecha entre los funcionarios que participan en la lucha contra el ciberdelito. En la Declaración adoptada por los ministros de Comunicaciones e Información del APEC reunidos en Bangkok, Tailandia, en 2008, se destacaba la importancia de proseguir la colaboración contra el ciberdelito. Hasta la fecha, el APEC no ha facilitado ningún marco jurídico sobre el ciberdelito, aunque se ha referido a normas internacionales tales como el Convenio sobre la Ciberdelincuencia de Budapest. Además, ha estudiado a fondo la legislación nacional sobre el ciberdelito de varios países, mediante la encuesta correspondiente, y ha elaborado una base de datos con los distintos enfoques con el fin de ayudar a los países a elaborar y revisar su legislación. El cuestionario utilizado para la encuesta se basó en el marco jurídico que figura en el Convenio sobre la Ciberdelincuencia de Budapest que más adelante abordaremos de manera detallada.[225]

Declaración relativa a la lucha contra el terrorismo (2002)

En 2002 los dirigentes del APEC presentaron una declaración relativa a la lucha contra el terrorismo y al fomento del crecimiento para promulgar leyes integrales relacionadas con el ciberdelito y desarrollar capacidades nacionales para la investigación del ciberdelito. Se comprometieron a esforzarse en elaborar antes de octubre de 2003 un conjunto integral de leyes sobre ciberdelito y ciberseguridad que fuera coherente con las disposiciones de los instrumentos jurídicos internacionales, incluidos la Resolución 55/63 de la Asamblea General de las Naciones Unidas y el Convenio sobre la Ciberdelincuencia del Consejo Europeo. Además, se

[224] *Es un foro de Cooperación Económica Asia-Pacifico) es un foro multilateral creado en 1989, con el fin de consolidar el crecimiento y la prosperidad de los países alrededor del Pacifico, que trata temas relacionados con el intercambio comercial, coordinación económica y cooperación entre sus integrantes son 21 miembros.*

[225] *UIT, Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica en línea con dirección URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf consulta 31-03-2020.*

comprometieron a identificar unidades nacionales de ciberdelito, determinar puntos de contacto para la asistencia internacional de alta tecnología y crear, cuando no existieran, esas capacidades y poner en marcha instituciones que intercambiaran evaluaciones de amenazas y vulnerabilidades (tales como equipos de respuesta ante emergencias informáticas) antes del mes de octubre de 2003. [226]

Conferencia sobre legislación en materia de ciberdelito (2005)

El APEC ha organizado diversas conferencias e hizo un llamamiento para promover una cooperación más estrecha entre los funcionarios que participan en la lucha contra el ciberdelito. En 2005 el APEC organizó la Conferencia sobre Legislación en materia de Ciberdelito. Los principales objetivos de dicha Conferencia eran promover la preparación de marcos jurídicos cabales para combatir el ciberdelito y fomentar la ciberseguridad; ayudar a las autoridades encargadas de hacer cumplir la ley a responder a los urgentes desafíos y problemas que plantea el progreso de la tecnología y promover la cooperación entre los investigadores y el ciberdelito en la región. [227]

Grupo de Trabajo sobre telecomunicaciones e información

El Grupo de Trabajo sobre telecomunicaciones e información del APEC participó activamente en la definición de enfoques del APEC para acrecentar la ciberseguridad. En 2002 el Grupo de Trabajo adoptó la estrategia de ciberseguridad del APEC. El Grupo de Trabajo expresó su posición en cuanto a la legislación sobre el ciberdelito, remitiéndose para ello a los enfoques internacionales adoptados por instituciones que van de las Naciones Unidas al Consejo de Europa. En el contexto del Grupo de Tareas Especiales sobre ciberseguridad del Grupo de Trabajo de Telecomunicaciones e Información reunidos en dos conferencias en Bangkok,

---

[226] *UIT, Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica en línea con dirección URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf consulta 31-03-2020.*

[227] *UIT, Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica en línea con dirección URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf consulta 31-03-2020.*

Tailandia, en 2003 se abordó la experiencia adquirida en materia de elaboración de legislación relativa al ciberdelito.[228]

4.2.11. La Commonwealth o Mancomunidad de Naciones.[229]

Habida la cuenta de la creciente importancia del ciberdelito los ministros del interior de la Commonwealth decidieron constituir un Grupo de Expertos para preparar un marco jurídico que permitiera luchar contra el ciberdelito, basándose en el Convenio sobre la Ciberdelincuencia del Consejo de Europa. Para definir este enfoque de armonización legislativa en el seno de la Commonwealth y fomentar la cooperación internacional se tuvo presente, entre otras cosas, el hecho de que dicho enfoque requeriría la adopción de no menos de 1272 tratados bilaterales en el marco de la Commonwealth para abordar la cooperación internacional sobre el particular. El grupo de expertos presento su Informe y recomendaciones en marzo de 2002. En dicho año se presentó el proyecto de Ley Modelo sobre el ciberdelito y los actos delictivos afines.

Además de la promulgación de leyes, la Commonwealth ha organizado varias actividades de formación. La red de la Commonwealth para las TI y el desarrollo (COMNET- IT) coordinación cursos de formación sobre el ciberdelito en 2007.

En 2009 se celebró en Malta el tercer programa de formación de la Commonwealth sobre un Marco jurídico para las TIC, con el apoyo del fondo de la Commonwealth para la Cooperación técnica. En 2011 se organizó otro curso.

En 2011 la Commonwealth presento la iniciativa sobre el ciberdelito, el principal objetivo de la iniciativa fue asistir a los países de la Commonwealth en la creación de capacidades institucionales humanas y técnicas en relación con la política, la legislación, la reglamentación, con la investigación y el cumplimiento de la ley.

---

[228] *UIT, Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica en línea con dirección URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf consulta 31-03-2020.*

[229] *Es una organización compuesta por 54 países, soberanos independientes y semindependientes, que con la excepción de Mozambique y Ruanda comparten lazos históricos con Reino Unido. Su principal objetivo es la cooperación internacional en el ámbito político y económico.*

Pretende permitir a todos los países de la Commonwealth tener una cooperación efectiva en la lucha contra el ciberdelito.[230]

4.2.12 Foro de Gobernanza de Internet (FGI).

Es un espacio para el dialogo sobre cuestiones relacionadas con el desarrollo de internet. Reúne a todas las partes interesadas del ecosistema de internet, incluyendo a los gobiernos, el sector privado, la sociedad civil, la comunidad técnica y la académica, en igualdad de condiciones y mediante un proceso abierto e inclusivo. Desde julio de 2006 se ha establecido y creado reuniones desde ese año en distintas partes del mundo, el cual han abarcado temas relacionados con el futuro de internet y crear soluciones que tengan un impacto global, abordando temas como:

- Desafíos y oportunidades para los Derechos humanos en línea.
- Spam
- Seguridad y Confidencialidad.
- Vigilancia omnipresente en línea
- Desarrollo de la infraestructura
- Cómo hacer para que la gobernanza Internet deviene más inclusiva.

Ofrece un espacio único para expresarte libremente en pie de igualdad, sin limitaciones vinculadas a las negociaciones de resultados formales, para compartir información y desarrolle soluciones sobre problemas clave de internet. Es un ángulo importante de internet mundial y la gobernanza local con la participación de más de 140 países.

4.2.13. FBI (El Buró Federal de Investigaciones) Estados Unidos.

Es una agencia de investigación federal e inteligencia y jurisdicción sobre una gran variedad de delitos federales incluyendo asuntos de seguridad y espionaje, secuestro o extravió de menores, crimen organizado, corrupción pública y delitos cibernéticos. Es una organización de seguridad nacional que corresponde a amenazas y que es regida por la recopilación e interpretación de información. Su principal objetivo es

[230] *UIT, Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica en línea con dirección URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf consulta 26-03-2020.*

proteger y defender a los Estados Unidos contra amenazas terroristas y de inteligencia extranjera, defender y hacer cumplir las leyes del código penal de los Estados Unidos, y proporcionar liderazgo y servicios de justicia penal a agencias federales, estatales, municipales e internacionales, así como otros socios.[231]

4.2.14. Policía de Investigación Federal (México).

Así como Estados Unidos tiene su propia agencia de investigación México también, solo que antes de esta institución ha habido 2 anteriores como el AFI (Agencia Federal de Investigación y la Policía Federal Ministerial). Encargada de salvaguardar y contrarrestar, diseñar, dirigir y operar sistemas de recopilación, clasificación, registro y explotación de información policial, al fin de encontrar datos que sustenten el desarrollo de acciones contra la delincuencia. Analiza e identifica las estructuras y modos de operación de las organizaciones delictivas de organizaciones, grupos o individuos que intenten alterar el orden y la paz públicos. También establece líneas de investigación policial a partir del análisis de la información respecto a sus estructuras y modos de operación de las organizaciones criminales.[232]

Aplica los procedimientos de intercambio de información policial, asesora y supervisa a las instituciones de seguridad pública de las entidades federativas que así lo solicitan y entre vista a las personas que pudieran aportar algún dato o elemento en la investigación para la prevención, en el ámbito de competencia de la institución, el combate a los delitos.

Se conforma de siete subdivisiones:

- División de inteligencia
- División de Seguridad Regional
- División Científica (de aquí una rama que desemboca a la Policía Cibernética)
- División de Antidrogas
- División de Fuerzas Federales
- Unidad de Asuntos Internos

---

[231] *FBI en línea con dirección URL: www.fbi.gov consultado 10-05-2021.*

[232] *Policía Federal de Investigación, en línea con dirección URL :https://www.gob.mx/policiafederal/articulos/division-de-investigacion-de-la-policia-federal?idiom=es consultado 06-06-2021*

- División de Gendarmería

4.2.15. La Policía Cibernética en México.

Son cuerpos policiales especializados en las investigaciones de los distintos delitos informáticos o fraudes cometidos a través del internet, estas organizaciones policiales son quienes descubren los individuos o grupos de personas que violan un sistema informático que acceden de manera ilegal a robar información privada de alguna de algún ciudadano así como también el robo o usurpación de la identidad de alguien, también se encarga de investigar los fraudes cometidos al momento de una compra online, así como también del robo de información financiera mediante una transacción bancaria realizada , el ciberacoso, el ciberbullyng, la pornografía infantil, etc.[233]

Su principal objetivo es realizar acciones para desarticular e identificar las distintas bandas dedicadas a los delitos informáticos, recolectar las distintas pruebas después que la víctima interponga con denuncia por el delito sufrido para poder dar con el paradero de los delincuentes, implementar el patrullaje antihacker a través del internet.

Mantienen un monitoreo y patrullaje las 24 horas del día en redes sociales y fuentes abiertas de internet. El objetivo principal es identificar publicaciones y/o actividades que pudieran ser constitutivas de un incidente cibernético.[234]

Actualmente existen nuevos grupos de respuesta ante emergencia de seguridad informática (CERT/CISRT) [235], una particularidad de estos grupos es la existencia de una conexión de todo el mundo ante incidentes de seguridad informática y las entidades a las que estos protegen, dicha conexión se establece por medio de un Esquema de Gestión de Información y Eventos de Seguridad (SIEM) referencia es

---

[233] *Policía Cibernética en línea con dirección URL: https://www.ssc.cdmx.gob.mx/organizacion-policial/subsecretaria-de-inteligencia-e-investigacion-policial/policia-cibernetica consultado 07-06-2021.*

[234] *Policía Cibernética ibid.*

[235] *(CERT/CISRT por sus siglas en inglés) los cuales al obtener la certificación por parte de la Universidad de Carnegie Mellon pueden incluir en su nombre la sigla CERT. También se debe hacer una distinción en las instituciones públicas, como el caso del CERT-UNAM y aquellos que forman parte de la oferta de empresas privadas, como puede ser el CERT-IQSec. (es una empresa de ciberseguridad que incluye a uno de los 11 CSIRT que hay en México y que además están certificados por la universidad antes mencionada.)*

una tecnología que realiza el análisis en tiempo real de los incidentes de ciberseguridad que presentan tanto el hardware de los dispositivos que integran la red.

4.3. Semblanza de los principales instrumentos jurídicos internacionales celebrados para el tratamiento y combate de los Delitos Cibernéticos.

4.3.1. Convención de Palermo.[236]

Es un tratado multilateral en materia de Trata de personas y para la protección y asistencia de víctimas de estos delitos, se integra de 4 partes y 20 artículos, la finalidad del protocolo es:

Prevenir y combatir la trata de personas, con especial atención a las mujeres y niños, proteger y ayudar a las víctimas de dicha trata, respectando plenamente sus derechos humanos y promover la cooperación entre los Estados parte para lograr los fines.

Hago mención de este documento porque habla sobre la protección de personas sobre delitos a nivel internacional y aunque no hable específicamente sobre delitos cibernéticos, se relaciona con las personas que lo cometen y a las víctimas, ya que es un nuevo escenario para las relaciones internacionales, por lo que es nuestro deber resguardar y evitar conflictos entre naciones, sin embargo los múltiples ciberdelitos que acontecen día a día de manera invisible y cada vez más difícil de perseguir debido a que no tienen fronteras, ni tiempo ni espacio, debido a que se puede cometer desde cualquier rincón del mundo con algún dispositivo electrónico que tiene acceso a internet, por lo que estos delitos se han desarrollado o pasado a ser crimen transnacional.[237]

Esta Convención se basa de tres protocolos de suma importancia, tales como; Protocolo de las Naciones Unidas para Prevenir, Reprimir y Sancionar la Trata de

---

[236] *La Convención contra la Delincuencia Organizada Transnacional, más conocida como la Convención de Palermo, es un tratado multilateral patrocinado por Naciones Unidas en contra del crimen organizado transnacional, fue adoptado en 2000.*

[237] *UIT, Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica en línea con dirección URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf consulta 01-04-2020.*

Personas, Especialmente Mujeres y Niños, protocolo de las Naciones Unidas contra el Contrabando de Migrantes por Tierra, Mar y Aire y Protocolo de las Naciones Unidas contra la fabricación y el tráfico ilícito de armas de fuego.[238]

Todos estos tres instrumentos contienen elementos de las actuales leyes internacionales sobre trata de personas y el tráfico ilegal de armas. La convención y el protocolo están bajo la jurisdicción de Oficina de Naciones Unidas contra la Droga y el Delito.[239]

La convención entró en vigor el 29 de septiembre de 2003. Para 6 de octubre de 2008, la convención de Palermo contaba con 147 estados miembros El Convenio contiene temas y leyes muy amplias relacionados con los delitos cibernéticos, tales como, la trata de personas, trabajo forzado, prostitución tanto en mujeres, y niños, solo que falta la especificación de las tecnologías, sin embargo considero que van de la mano y que se requiere una ampliación y actualización sobre este tema debido a que es un delito transnacional, es decir que es diferente perspectiva en cada país por su derecho interno y familia jurídica.[240]

4.3.2. La Convención de Budapest y el Protocolo Adicional de Ciberdelincuencia.

También conocido como el Convenio de Cibercriminalidad o ciberdelincuencia es el primer tratado internacional referente a combatir a los delitos cibernéticos y los delitos de internet por medio de la armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones firmantes. Fue creado por el Consejo de Europa en Estrasburgo, con la participación activa de Canadá, Japón, y China como Estados observadores.[241]

Fue firmado el 23 de noviembre de 2001 y entro en vigor el 1 de julio de 2004, sin embargo, el 38 de octubre de 2010 30 estados firmaron, ratificaron y se agregaron a

[238] Op. Cit.
[239] Op. Cit.
[240] Op. Cit.
[241] *CENTENO Dayna, México y el Convenio de Budapest, edición Marianne Diaz, junio 2018, en línea con dirección URL: https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf consultado 01-03-2020.*

la convención, mientras que otros 16 estados firmaron la convención, pero no la ratificaron.[242]

Esta convención se compone de 48 artículos los cuales toca temas como derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de la seguridad en las redes, la intercepción de comunicaciones privadas.

Hasta el momento se conoce como el único tratado internacional vinculante en la materia y contiene una especie de guía, "ley modelo" o "acuerdo marco" para que los Estados Parte:[243]

1. Implementen dentro de su ordenamiento jurídico nacional la legislación pertinente para investigar y perseguir penalmente aquellos delitos cometidos en contra de sistemas o medios informáticos o mediante el uso de los mismos.
2. Se busca facilitar la cooperación internacional en este sentido.

El Convenio está abierto a ratificación para Estados no parte Consejo de Europa, debido a que se ha incrementado considerablemente la presión internacional para que más países, sobre todo aquellos que no pertenecen al consejo, se adhieran al tratado. Sin embargo, no todos los Estados parten de los mismos contextos ni enfrentan los mismos problemas en materia de delitos relacionados con las tecnologías de la información y las comunicaciones, así como de respeto al Estado de derecho y a los derechos humanos.[244]

Las condiciones y obstáculos que enfrentan los países que forman parte del Consejo son muy diferentes a aquellos que confrontamos a América Latina. Por tanto, resulta fundamental analizar caso por caso, la pertinencia e implicaciones de adherirse a un tratado penal internacional "modelo" como el convenio para los países de este lado del hemisferio cuyo contexto demuestra la comisión generalizada de violaciones a derechos humanos y al Estado de Derecho.[245]

Primordialmente el convenio requiere que los Estados parte implementen dentro de su ordenamiento interno dos cuestiones. Primera criminalizar ciertas conductas enlistadas y definidas por el mismo convenio, como delitos de orden nacional.

---

[242] *MONTOYA Op. Cit.*
[243] *OECD en línea con dirección URL:http://www.oecd.org/ Op. Cit.*
[244] *OECD, Ibid.*
[245] *OCDE Ibid.*

Segunda dotar a las autoridades en materia de procuración de justicia penal de las facultades y herramientas procedimentales necesarias para investigar la comisión de estos delitos, incluyendo expandir capacidades de inteligencia y vigilancia, tales como cateo, incautación de bienes, monitoreo de contenido en línea, retención y transferencia e intervención de comunicaciones privadas.[246]

El Convenio pide establecer la tipificación de 4 amplias categorías de delitos: delitos cometidos contra la confidencialidad, integridad y disponibilidad de sistemas y datos informáticos, delitos cometidos mediante el uso de las tecnologías de la información y telecomunicaciones, delitos por su contenido (pornografía infantil), delitos en materia de derechos de autor.

Conforme al Convenio las facultades y herramientas procedimentales referidas aplicables para toda aquella evidencia contenida en medios informáticos, con independencia del delito de que se trate. Es decir, su ejecución no se circunscribe a la comisión de delitos informáticos exclusivamente. Por consiguiente, el ámbito de aplicación del tratado resulta ser sumamente amplio. Todo lo antes mencionado representa diversos problemas a la hora de adoptar e implementar el Convenio en los ordenamientos nacionales.[247]

Hay una lista por continentes que muestra cuales son los países que han firmado y ratificado este Convenio, se puede ver en el (anexo 2):[248]

Como podemos observar México no se encuentra dentro de estos cuadros debido a que el artículo 1 de la Constitución Política de los Estados Unidos Mexicanos sitúa a los tratados internacionales en materia de derechos humanos al mismo nivel jerárquico de las leyes federales e incluso que la propia Carta Magna, debiendo prevalecer en caso de conflicto derivado de “restricciones expresas contenidas en la Constitución” la aplicación de esta última. Por lo que, al adoptarse, los tratados internacionales son incorporados directamente al ordenamiento jurídico nacional. Ello implica que inmediatamente pueden aplicarse, siempre y cuando sean compatibles con la Carta Magna. Sin embargo, existen diversos tratados internacionales que

---

[246] *OCDE, Ibid.*
[247] *OCDE Ibid.*
[248] *Consejo de Europa y derechos humanos, en línea https://www.coe.int/en/web/conventions/fulllist//conventions/treaty/185/signatures?p_auth=hZgYFWlA consultado 28-02-2020.*

obligan a los Estados contratantes a llevar a cabo ciertas modificaciones a la legislación existente para lograr su efectiva implementación y aplicación en los ordenamientos jurídicos nacionales.[249]

Los artículos 14 y 16 de la Constitución establecen la obligatoriedad de observar el principio de legalidad o el principio de ***nullum crime sine lege***, es decir que existe una prohibición constitucional de imponer pena alguna que no esté prevista por una ley exactamente aplicable al delito de que se trate.[250]

El Convenio de Budapest deja un amplio margen de discrecionalidad para ciertos delitos debido a la vaguedad, imprecisión, apertura o amplitud, de su definición. Por ejemplo, los delitos de acceso ilícito, previstos en el artículo 2, intercepción lícita, previsto en el artículo 3, ataques a la Tecnologías de datos, previsto en el artículo 4 ataques a la integridad del sistema previsto en el artículo 5; abusos de dispositivos, previstos en el artículo 6; falsificación informática previsto en el artículo 7; y fraude informático previsto en el artículo 8, requieren de mayor especificación respecto de lo que debería entenderse como "ilegitimo". El artículo 6 del convenio necesita precisar porque además como debería interpretarse el término "posesión ".[251]

Legislación Mexicana relacionada con las Tecnologías de la Información y la Comunicación

Es importante señalar que en México no hay leyes que tengan en específico delitos cibernéticos como tal, sin embargo, no significa que no estén contemplados en apartados específicos en las distintas leyes y reglamentos que conforman el Derecho positivo mexicano que aplican en el abatimiento de todas las conductas delictivas envueltas en las Tecnologías de la Información y Comunicación.

Protocolo adicional sobre el ciberdelito y ciberseguridad.

Durante el Foro para la Gobernanza de Internet celebrado en Egipto en 2009, Schönberg y Ghernaouti-Helie presentaron una propuesta de Protocolo Mundial sobre Ciberseguridad y Ciberdelito. El Artículo 1-5 se refiere al ciberdelito y recomienda la aplicación de disposiciones penales sustantivas, de medidas contra el

[249] *Ibid.*
[250] *Ibid.*
[251] *Ibid.*

uso indebido de Internet por los terroristas, de medidas para la cooperación mundial y el intercambio de información, y de medidas en materia de derecho a la intimidad y derechos humanos. La legislación modelo que se incluye en el apéndice al Protocolo se basa en gran medida (Artículos 1-25) en una repetición literal de las disposiciones del Convenio del Consejo de Europa sobre la Ciberdelincuencia.[252]

En junio de 2014, Schönberg presentó la 9ª edición de un proyecto de Tratado de las Naciones Unidas sobre un Tribunal Penal Internacional o Tribunal del Ciberespacio. El enfoque científico, que no se funda en un mandato oficial de las Naciones Unidas, destaca las dificultades relativas a la jurisdicción en el ciberespacio y elabora el concepto de tribunal internacional con jurisdicción limitada que es comparable al de la Corte Internacional de Justicia permanente.

4.3.3. El Manual de las Naciones Unidas para la prevención y control de delitos informáticos.

La ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

a) Falta de acuerdos globales acerca de qué tipo de conductas deben construir delitos informáticos.
b) Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
c) Falta de especialización de los policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
d) No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
e) Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

[252] *Preparatory Process IGF 2009 Planning meeting, en línea con dirección URL: www.intgovforum.org consultado 10-04-2020.*

f) Ausencia de tratados de extradición, acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta de vigor de la Cooperación Internacional y al crimen organizado.[253]

4.3.4. Mención especial a la Ley Olimpia del Estado mexicano.

La ley Olimpia surge como iniciativa para proteger el derecho a la intimidad personal y el ejercicio libre y protegido de los derechos sexuales para salvaguardar la integridad de las personas, por un video de Olimpia Melo Cruz, el cual fue difundido en redes sociales en 2014 por su anterior pareja sin el consentimiento de ella.

Se le denomina un conjunto de reformas legislativas que reconoce la violencia digital como un tipo de delito y se sanciona con multas económicas o penas de cárcel para quien viole la intimidad sexual de las personas a través de medios digitales(ciberviolencia)[254]

Fue impulsada en Puebla para reformar el Código Penal de dicha entidad federativa, en el 2014. En el 2018, se logró reconocer la violencia digital o ciberacoso como delito y se sancione con 6 años de prisión a quienes comparten materiales íntimos sin consentimiento. Por lo que es notorio que genera violencia sexual en internet, por lo que se ha luchado estos años para crear conciencia a través de la ley General de Acceso a las mujeres entre las instituciones sobre los derechos sexuales, la violencia digital y su difusión de este entre los ciudadanos. Esta ley fue aprobada el 3 de diciembre de 2019, por lo que desde ese año se puede hacer una denuncia ante el MP. A partir del 2022 la ley aplica a toda la República Mexicana.[255]

Por lo que es importante conocer que la Ley Olimpia sanciona: difundir, compilar, publicar, hacer visibles contenidos íntimos reales o alterados, videos, fotografías, imágenes sin el consentimiento de las personas (delitos contra la intimidad sexual). Incluso la sexualización / cosificación a través de difusión o producción de videos o

---

[253] Lopez Calvo Pedro, Derechos Humanos Victimologia, Terrorismo y sus diversas modalidades Delictivas, Flores Editor y Distribuidor, 2015, p.p. 442.

[254] Universidad Abierta y a Distancia de México, en línea con dirección URL: https://gaceta.unadmexico.mx/historico-anual/66-2022/marzo-abril-2022/genero/112-de-que-trata-la-ley-olimpia#:~:text=Es%20un%20conjunto%20de%20reformas,de%20medios%20digitales%20(ciberviolencia). Consultado 03/01/23

[255] Universidad Abierta y a Distancia de México, Op. Cit.

imágenes. Así como, el acoso o insultos relacionados a la difusión de imágenes audios y videos de contenido intimo sexual.[256]

Otros datos importantes que debemos conocer son los siguientes:

Quienes tienen y comparten videos de personas que no dan el consentimiento para ello, pueden ser cómplices.

Esta ley que tipifica la violencia digital protege a las mujeres y sus cuerpos al castigar el delito de violación a la intimidad sexual - con agravante si es cometido por alguien con quien la víctima haya tenido una relación sentimental, afectiva o de confianza (se incrementa el doble o triple de pena) o exista alguna amenaza.

En cada estado o cada tipo de violencia digital se sanciona de manera diferente, por ejemplo, en Nuevo León desde el 2019 se aprobó y actualmente se castiga con 8 años de cárcel.

“9.4 millones de mujeres han sufrido ciberacoso, en el que el 55% de los agresores son hombres”.

Actualmente, en Zacatecas hay 88 casos de violencia digital, siendo las víctimas mujeres de entre 18 y 29 años de edad.

Este es un claro ejemplo que México ha ido involucrándose y avanzando, sin embargo, tiene una enorme tarea para continuar el análisis y desarrollo de este tema.

[256] Jessica Fernández García (s.f.). Más Allá del Rosa-Ley Olimpia con Olimpia Coral. Youtube. https://www.youtube.com/watch?v=__0p-o7g71Q consultado 05/01/23.

CONCLUSIONES

La llegada de la tecnología y el internet han sido crucial no solo para las relaciones internacionales sino también para la humanidad, desde la manera de comunicarnos tanto física, verbal y espiritual, ahora se ha convertido a través de un dispositivo que tenga acceso a internet y con imágenes o videos podemos describir nuestro sentir en segundos.

El ciberespacio es un lugar intangible y un tema no muy abordado y novedoso para las Relaciones Internacionales, que día a día exige nuevas formas de jurisdicción, prevención debido a su constate evolución y desarrollo, también busca erradicar conductas delictivas que ya se convertido en crímenes transnacionales.

Los delitos cibernéticos internacionales cada vez se expanden y se crean nuevos, sin embargo, debido a que no existe un acuerdo a nivel internacional para que se pueda prevenir y castigar dichos delitos por falta de normas jurisdiccionales internacionales debido a que existirían un choque con el derecho interno de cada Estado. Los delitos internacionales siempre se han analizado mayormente desde el plano económico, sin embargo como en el capítulo segundo en donde se aborda los tipos de delitos cibernéticos en donde mayormente se impactan a los derechos humanos de los niños con el grooming, cyberbullyng, sexting, que son conductas que se dirigen mayormente a la prostitución y trata de personas, es urgente que se continúe creando más mecanismos para la defensa y protección de estos delitos para que pueda existir delito que se castigue de lo contrario esto continuará pasando, hasta convertirse en una plaga sin salida.

En los Derechos Humanos, sabemos que todos ser humano los adquiere desde el día que nace, sin embargo, no hay una fuente de divulgación masiva para que toda la humanidad los conozca y pueda exigirlos. También pudimos observar que al paso que la humanidad avanza o evoluciona, todos lo que está a su alrededor exige a su vez un cambio, las casi 5 generaciones de los derechos humanos si todos los países los aplicaran a su derecho interno y lo hicieran valer, se podrían lograr grandes acuerdos y leyes que puedan castigar y erradicar dichos delitos.

Los Derechos Humanos desde su creación han traído grandes cambios y han evitado muchas muertes y eventos trágicos, no hay que olvidar a la Carta de los derechos Humanos creada en Virginia en 1948, ya que sin este documento de vital

importancia la humanidad no tendría un giro radical y positivo, sin embargo, se requiere mayor difusión y gente que pueda explicar de manera práctica para que todos los seres humanos podamos comprender su función y objetivo. A pesar de todos los instrumentos e instituciones que existen sobre los Derechos Humanos se requiere dar mayor importancia a ejercer y hacer cumplir cada norma jurisdiccional que adopta cada estado.

Las bases de la jurisdicción a nivel internacional todavía están dispersas, ya que cada país va a su paso y conforme su situación, todavía existen algunos países que no se consideran delitos a los delitos cibernéticos como graves y que se requiera castigarlos, debido a que su persona física no ha sido afectada en su mayoría, sin embargo si lo enfocamos desde la perspectiva mental y psíquica, se estarían cometiendo el mayor delito ya que estamos hablando de su ser interno el cual transmite emociones a su físico exterior y que si afecta mayormente a un ser humano, se requiere trabajar el enfoque cívico y ético a mayor profundidad ya que siempre se han dedicado a la parte financiera y cosas materiales y han dejado de lado el estado emocional y mental del ser humano que considero es de suma importancia para poder tener una sociedad sana, libre y que pueda seguir reglas. Ya que, si una sociedad tiene valores de respeto, compromiso, honestidad, responsabilidad tanto para sí mismos como para su entorno tendríamos una sociedad internacional pacífica y la tecnología no nos dominaría como hoy en día.

Se requiere mayor esfuerzo en las áreas de los tratados, convenios, artículos y normas que tengan la misma visión para poder erradicar y castigar estos delitos que día a día se cometen y dañan a la sociedad.

A pesar de las grandes iniciativas de leyes, de nuevos organismos, de foros, de congresos, de todas las actividades que realizan las instituciones, siguen mostrando grandes deficiencias tanto internas como internacionales, debido al gran desacuerdo y falta de organización para poder liderar de manera uniforme a la ciberdelincuencia que diariamente presenta grandes y nuevos desafíos para la ciberseguridad internacional.

En el caso de China y Rusia son potencias mundiales y han elegido desarrollar su propio sistema de internet, pero solo podría ser para dos cosas: la primera, para fines de seguridad interna (crear su caparazón) o para fines de colaboración con la

ciberdelincuencia internacional. Además, también es un claro ejemplo de cómo están violando los derechos humanos de sus nacionales, tales como la libertad de expresión, el acceso a la información, el derecho a elegir libremente el contenido de información, entre otros derechos.

En cuanto a todos los delitos cibernéticos que cada día se desarrollan e intensifican y que han sido favorecidos por el covid-19 para acrecentar y delinquir en todo el mundo, lo cual hace cada día más difícil crear medidas únicas porque es un tema que está en constante movimiento.

Otro factor que se debe destacar es que todos estamos expuestos a ser víctimas de la ciberdelincuencia debido a las nuevas formas de realizar nuestras actividades cotidianas enfatizando mayormente el plano laboral, las finanzas y las compras en línea. Los niños en cuanto al abuso que ya existía y que ahora con la pandemia se puede afirmar que conviven más tiempo con el enemigo en casa y eso origina un problema más difícil de perseguir y castigar.

También es necesario reconocer y actuar sobre las medidas de prevención y regulación de la trata de personas y explotación sexual en las redes porque para el ciberdelincuente se le ha facilitado delinquir y obtener mejores ingresos por este nuevo espacio que aún tiene retos que quizá sean imposibles de concretarse debido a su desmesurado desarrollo.

PROSPECTIVA

En cuanto a la prospectiva del tema se puede observar que aún es un tema nuevo y que siempre estará latente y que se está introduciendo como una nueva forma de vivir virtualmente en el ser humano. La cual presenta un nuevo escenario o campo de estudio, para las relaciones internacionales y el derecho internacional, para crear normas, nuevos mecanismos, nuevas organizaciones, más foros, mayores medios de comunicación o difusión de campañas que expliquen a la sociedad la realidad que se nos está presentando en nuestras vidas para poder también desarrollarnos y asimilando el nuevo estilo de vida con la tecnología. Es un tema que seguirá en el estudio y cuidado de mucha gente especializada y que además quiera aportar para el conocimiento de la sociedad internacional.

La tecnología nos facilita la vida, pero también ofrece nuevas herramientas a los delincuentes que dan lugar a los delitos cibernéticos; como ejemplo podrían crear nuevas formas de hackeos y espionajes como; secuestrar tu casa inteligente accediendo desde el puerto del hardware al sistema, otro podría ser hackear las pantallas, espiar tus webcams. También suena alarmante las impresoras 3D que han prometido revolucionar el mercado en los próximos años, por lo que podrías crear e imprimir tus propias armas, así como el nuevo dron que se puede manejar solo y cargar 40 kilos y así mismo poder cometer cualquier delito, por último el internet ha prometido conectar cualquier objeto a internet, para controlarlo desde el celular, la cafetera, el aire acondicionado etc., por alguna razón podrían hackear tu cuenta y acceder a manipular tus artículos poniendo en riesgo tu vida con tan solo un clic.

Todo lo mencionado anteriormente suena alarmante, sin embargo, es para tener conocimiento a lo que nos enfrentamos actualmente y solo así podremos crear medidas de seguridad que nos permitan contrarrestar estos nuevos delitos cibernéticos que día a día todo el mundo y Organizaciones se dedican a proteger y contrarrestarlos.

ANEXOS

Anexo 1

Lista de instrumentos Universales, regionales y tratados de los que se apoya el Derecho Internacional de los Derechos Humanos y otras ramas.

INTERNACIONALES

Vinculantes[257]

- CARTA DE LAS NACIONES UNIDAS.
- CONVENCIÓN CONTRA LA TORTURA Y OTROS TRATOS O PENAS CRUELES INHUMANOS O DEGRADANTES.
- CONVENCIÓN INTERNACIONAL CONTRA EL APARTHEID EN LOS DEPORTES.
- CONVENCIÓN INTERNACIONAL CONTRA LA TOMA DE REHENES, ABIERTA A FIRMA EN LA CIUDAD DE NUEVA YORK EL 18 DE DICIEMBRE DE 1979.
- CONVENCIÓN INTERNACIONAL PARA LA PROTECCIÓN DE TODAS LAS PERSONAS CONTRA LAS DESAPARICIONES FORZADAS.
- CONVENCIÓN INTERNACIONAL PARA LA SUPRESIÓN DE LA TRATA DE MUJERES Y MENORES.
- CONVENCIÓN INTERNACIONAL RELATIVA A LA REPRESIÓN DE LA TRATA DE MUJERES MAYORES DE EDAD.
- CONVENCIÓN INTERNACIONAL SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACIÓN RACIAL.
- CONVENCIÓN INTERNACIONAL SOBRE LA PROTECCIÓN DE LOS DERECHOS DE TODOS LOS TRABAJADORES MIGRATORIOS Y DE SUS FAMILIARES.
- CONVENCIÓN INTERNACIONAL SOBRE LA REPRESIÓN Y EL CASTIGO DEL CRIMEN DE APARTHEID.

[257] Se refiere a que los Estados que de adhieran son los que están obligados a cumplir lo estipulado al pie de la letra.

- CONVENCIÓN PARA LA PREVENCIÓN Y LA SANCIÓN DEL DELITO DE GENOCIDIO.
- CONVENCIÓN PARA LA REPRESIÓN DE LA TRATA DE PERSONAS Y DE LA EXPLOTACIÓN DE LA PROSTITUCIÓN AJENA.
- CONVENCIÓN RELATIVA A LA ESCLAVITUD.
- CONVENCIÓN RELATIVA A LA LUCHA CONTRA LAS DISCRIMINACIONES EN LA ESFERA DE LA ENSEÑANZA 1960.
- CONVENCIÓN SOBRE ASILO DIPLOMÁTICO.
- CONVENCIÓN SOBRE ASILO POLÍTICO.
- CONVENCION SOBRE ASILO TERRITORIAL.
- CONVENCION SOBRE ASILO TERRITORIAL.
- CONVENCIÓN SOBRE EL CONSENTIMIENTO PARA EL MATRIMONIO, LA EDAD MÍNIMA PARA CONTRAER MATRIMONIO Y EL REGISTRO DE LOS MATRIMONIOS.
- CONVENCIÓN SOBRE EL ESTATUTO DE LOS REFUGIADOS.
- CONVENCIÓN SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACIÓN CONTRA LA MUJER.
- CONVENCIÓN SOBRE LA IMPRESCRIPTIBILIDAD DE LOS CRÍMENES DE GUERRA Y DE LOS CRÍMENES DE LESA HUMANIDAD, ADOPTADA POR LA ASAMBLEA GENERAL DE LAS NACIONES UNIDAS EL VEINTISÉIS DE NOVIEMBRE DE MIL NOVECIENTOS SESENTA Y OCHO.
- CONVENCIÓN SOBRE LA NACIONALIDAD DE LA MUJER CASADA.
- CONVENCIÓN SOBRE LA PROTECCIÓN DE MENORES Y LA COOPERACIÓN EN MATERIA DE ADOPCIÓN INTERNACIONAL.
- CONVENCIÓN SOBRE LOS ASPECTOS CIVILES DE LA SUSTRACCIÓN INTERNACIONAL DE MENORES.
- CONVENCIÓN SOBRE LOS DERECHOS POLÍTICOS DE LA MUJER.
- CONVENCIÓN SOBRE LOS DERECHOS DE LAS PERSONAS CON DISCAPACIDAD.
- CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO.

- CONVENIO 100, RELATIVO A LA IGUALDAD DE REMUNERACIÓN ENTRE LA MANO DE OBRA MASCULINA Y LA MANO DE OBRA FEMENINA POR UN TRABAJO DE IGUAL VALOR. .
- CONVENIO 102 DE LA ORGANIZACIÓN INTERNACIONAL DEL TRABAJO, RELATIVO A LA NORMA MÍNIMA DE LA SEGURIDAD SOCIAL.
- CONVENIO 111, RELATIVO A LA DISCRIMINACIÓN EN MATERIA DE DESEMPLEO Y OCUPACIÓN.
- CONVENIO 135, RELATIVO A LA PROTECCIÓN Y FACILIDADES QUE DEBEN OTORGARSE A LOS REPRESENTANTES DE LOS TRABAJADORES EN LA EMPRESA
- CONVENIO 159 DE LA ORGANIZACIÓN INTERNACIONAL DEL TRABAJO, SOBRE LA READAPTACIÓN PROFESIONAL Y EL EMPLEO DE PERSONAS INVÁLIDAS.
- CONVENIO 169 SOBRE PUEBLOS INDÍGENAS Y TRIBALES EN PAÍSES INDEPENDIENTES.
- CONVENIO 58, POR EL QUE SE FIJA LA EDAD MÍNIMA DE ADMISIÓN DE LOS NIÑOS AL TRABAJO MARÍTIMO.
- CONVENIO 87, SOBRE LA LIBERTAD SINDICAL Y LA PROTECCIÓN DEL DERECHO DE SINDICACIÓN.
- CONVENIO 90, RELATIVO AL TRABAJO NOCTURNO DE LOS MENORES EN LA INDUSTRIA.
- CONVENIO 95 DE LA ORGANIZACIÓN INTERNACIONAL DEL TRABAJO, RELATIVO A LA PROTECCIÓN DEL SALARIO.
- CONVENIO I DE GINEBRA PARA MEJORAR LA SUERTE DE LOS HERIDOS Y LOS ENFERMOS DE LAS FUEZAS ARMADAS EN CAMPAÑA.
- CONVENIO II DE GINEBRA PARA MEJORAR LA SUERTE DE LOS HERIDOS, LOS ENFERMOS Y LOS NÁUFRAGOS DE LAS FUERZAS ARMADAS EN EL MAR.
- CONVENIO III DE GINEBRA RELATIVO AL TRATO DE LOS PRISIONEROS DE GUERRA.

- CONVENIO INTERNACIONAL PARA LA SUPRESIÓN DEL TRÁFICO DE TRATA DE BLANCAS, FIRMADO EN PARÍS EL 4 DE MAYO DE 1910, ENMENDADO POR EL PROTOCOLO FIRMADO EN LAKE SUCCESS, NUEVA YORK, EL 4 DE MAYO DE 1949.
- CONVENIO IV DE GINEBRA RELATIVO A LA PROTECCIÓN DE PERSONAS CIVILES EN TIEMPO DE GUERRA.
- CONVENIO SOBRE LA PROHIBICIÓN DE LAS PEORES FORMAS DE TRABAJO INFANTIL Y LA ACCIÓN INMEDIATA PARA SU ELIMINACIÓN, ADOPTADO POR LA CONFERENCIA GENERAL DE LA ORGANIZACIÓN INTERNACIONAL DEL TRABAJO.
- ESTATUTO DE LA CORTE INTERNACIONAL DE JUSTICIA.
- ESTATUTO DE ROMA DE LA CORTE PENAL INTERNACIONAL.
- PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS.
- PACTO INTERNACIONAL DE DERECHOS ECONÓMICOS, SOCIALES Y CULTURALES.
- PROTOCOLO ADICIONAL A LOS CONVENIOS DE GINEBRA DEL 12 DE AGOSTO DE 1949 RELATIVO A LA PROTECCIÓN DE LAS VÍCTIMAS DE LOS CONFLICTOS ARMADOS SIN CARÁCTER INTERNACIONAL (PROTOCOLO II).
- PROTOCOLO ADICIONAL A LOS CONVENIOS DE GINEBRA RELATIVO A LA PROTECCIÓN DE LAS VÍCTIMAS DE LOS CONFLICTOS ARMADOS INTERNACIONALES.
- PROTOCOLO FACULTATIVO DE LA CONVENCIÓN CONTRA LA TORTURA Y OTROS TRATOS O PENAS CRUELES, INHUMANOS O DEGRADANTES.
- PROTOCOLO FACULTATIVO DE LA CONVENCIÓN SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACIÓN CONTRA LA MUJER.
- PROTOCOLO FACULTATIVO DE LA CONVENCION SOBRE LOS DERECHOS DE LAS PERSONAS CON DISCAPACIDAD.

- PROTOCOLO FACULTATIVO DE LA CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO RELATIVO A LA PARTICIPACIÓN DE NIÑOS EN LOS CONFLICTOS ARMADOS.
- PROTOCOLO FACULTATIVO DE LA CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO RELATIVO A LA VENTA DE NIÑOS, LA PROSTITUCIÓN INFANTIL Y LA UTILIZACIÓN DE LOS NIÑOS EN LA PORNOGRAFÍA.
- PROTOCOLO FACULTATIVO DEL PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS.
- PROTOCOLO PARA MODIFICAR LA CONVENCIÓN RELATIVA A LA ESCLAVITUD FIRMADA EN GINEBRA EL 25 DE SEPTIEMBRE DE 1926.
- PROTOCOLO PARA PREVENIR, REPRIMIR Y SANCIONAR LA TRATA DE PERSONAS, ESPECIALMENTE MUJERES Y NIÑOS, QUE COMPLEMENTA LA CONVENCIÓN DE LAS NACIONES UNIDAS CONTRA LA DELINCUENCIA ORGANIZADA TRANSNACIONAL, ADOPTADO POR LA ASAMBLEA GENERAL DE LAS NACIONES UNIDAS EL QUINCE DE NOVIEMBRE DE DOS MIL
- PROTOCOLO QUE MODIFICA EL CONVENIO PARA LA REPRESIÓN DE LA TRATA DE MUJERES Y MENORES DEL 30 DE SEPTIEMBRE DE 1921 Y EL CONVENIO PARA LA REPRESIÓN DE LA TRATA DE MUJERES MAYORES DE EDAD, DEL 11 DE OCTUBRE DE 1933.
- PROTOCOLO SOBRE EL ESTATUTO DE LOS REFUGIADOS.
- SEGUNDO PROTOCOLO FACULTATIVO DEL PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS DESTINADO A ABOLIR LA PENA DE MUERTE.

No vinculantes

- CÓDIGO DE CONDUCTA PARA FUNCIONARIOS ENCARGADOS DE HACER CUMPLIR LA LEY
- CONJUNTO DE PRINCIPIOS PARA LA PROTECCIÓN DE TODAS LAS PERSONAS SOMETIDAS A CUALQUIER FORMA DE DETENCIÓN O PRISIÓN

- DECLARACIÓN DE COMPROMISO EN LA LUCHA CONTRA EL VIH/SIDA
- DECLARACIÓN DE LAS NACIONES UNIDAS SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACIÓN RACIAL
- DECLARACIÓN DE LAS NACIONES UNIDAS SOBRE LOS DERECHOS DE LOS PUEBLOS INDÍGENAS.
- DECLARACIÓN DE LOS DERECHOS DE LOS IMPEDIDOS.
- DECLARACIÓN DE LOS DERECHOS DEL NIÑO.
- DECLARACIÓN DE LOS DERECHOS DEL RETRASADO MENTAL.
- DECLARACIÓN DEL MILENIO.
- DECLARACIÓN SOBRE EL ASILO TERRITORIAL.
- DECLARACIÓN SOBRE EL DERECHO AL DESARROLLO.
- DECLARACIÓN SOBRE EL DERECHO DE LOS PUEBLOS A LA PAZ.
- DECLARACIÓN SOBRE EL DERECHO Y EL DEBER DE LOS INDIVIDUOS, LOS GRUPOS Y LAS INSTITUCIONES DE PROMOVER Y PROTEGER LOS DERECHOS HUMANOS Y LAS LIBERTADES FUNDAMENTALES UNIVERSALMENTE RECONOCIDOS.
- DECLARACIÓN SOBRE EL FOMENTO ENTRE LA JUVENTUD DE LOS IDEALES DE LA PAZ, RESPETO MUTUO Y COMPRENSIÓN ENTRE LOS PUEBLOS.
- DECLARACIÓN SOBRE EL PROGRESO Y EL DESARROLLO EN LO SOCIAL.
- DECLARACIÓN SOBRE LA CONCESIÓN DE LA INDEPENDENCIA A LOS PAÍSES Y PUEBLOS COLONIALES.
- DECLARACIÓN SOBRE LA ELIMINACIÓN DE LA DISCRIMINACIÓN CONTRA LA MUJER.
- DECLARACIÓN SOBRE LA ELIMINACIÓN DE LA VIOLENCIA CONTRA LA MUJER.
- DECLARACIÓN SOBRE LA ELIMINACIÓN DE TODAS LAS FORMAS DE INTOLERANCIA Y DISCRIMINACIÓN FUNDADAS EN LA RELIGIÓN O LAS CONVICCIONES.

- DECLARACIÓN SOBRE LA PROTECCIÓN DE TODAS LAS PERSONAS CONTRA LA TORTURA Y OTROS TRATOS O PENAS CRUELES, INHUMANOS O DEGRADANTES.
- DECLARACIÓN SOBRE LA PROTECCIÓN DE LA MUJER Y EL NIÑO EN ESTADOS DE EMERGENCIA O DE CONFLICTO ARMADO.
- DECLARACIÓN SOBRE LA PROTECCIÓN DE TODAS LAS PERSONAS CONTRA LAS DESAPARICIONES FORZADAS.
- DECLARACIÓN SOBRE LA RAZA Y LOS PREJUICIOS RACIALES.
- DECLARACIÓN SOBRE LA UTILIZACIÓN DEL PROGRESO CIENTÍFICO Y TECNOLÓGICO EN INTERÉS DE LA PAZ Y EN BENEFICIO DE LA HUMANIDAD.
- DECLARACIÓN SOBRE LOS DERECHOS DE LAS PERSONAS PERTENECIENTES A MINORÍAS NACIONALES O ÉTNICAS, RELIGIOSAS Y LINGÜÍSTICAS.
- DECLARACIÓN SOBRE LOS DERECHOS HUMANOS DE LOS INDIVIDUOS QUE NO SON NACIONALES DEL PAÍS EN QUE VIVEN.
- DECLARACIÓN SOBRE LOS PRINCIPIOS FUNDAMENTALES DE JUSTICIA PARA LAS VÍCTIMAS DE DELITOS Y DEL ABUSO DE PODER.
- DECLARACIÓN SOBRE LOS PRINCIPIOS FUNDAMENTALES RELATIVOS A LA CONTRIBUCIÓN DE LOS MEDIOS DE COMUNICACIÓN DE MASAS AL FORTALECIMIENTO DE LA PAZ Y LA COMPRENSIÓN INTERNACIONAL, A LA PROMOCIÓN DE LOS DERECHOS HUMANOS Y A LA LUCHA CONTRA EL RACISMO, EL APARTHEID Y LA INCITACIÓN A LA GUERRA.
- DECLARACIÓN SOBRE LOS PRINCIPIOS SOCIALES Y JURÍDICOS RELATIVOS A LA PROTECCIÓN Y EL BIENESTAR DE LOS NIÑOS, CON PARTICULAR REFERENCIA A LA ADOPCIÓN Y LA COLOCACIÓN EN HOGARES DE GUARDA, EN LOS PLANOS NACIONAL E INTERNACIONAL.
- DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS.
- DECLARACIÓN UNIVERSAL SOBRE EL GÉNOMA HUMANO Y LOS DERECHOS HUMANOS.

- DECLARACIÓN UNIVERSAL SOBRE LA ERRADICACIÓN DEL HAMBRE Y LA MALNUTRICIÓN.
- DECLARACION Y PROGRAMA DE ACCION DE VIENA.
- DIRECTRICES DE LAS NACIONES UNIDAS PARA LA PREVENCIÓN DE LA DELINCUENCIA JUVENIL (DIRECTRICES DE RIAD).
- DIRECTRICES SOBRE LA FUNCION DE LOS FISCALES.
- NORMAS UNIFORMES SOBRE LA IGUALDAD DE OPORTUNIDADES PARA LAS PERSONAS CON DISCAPACIDAD.
- PRINCIPIOS BÁSICOS PARA EL TRATAMIENTO DE LOS RECLUSOS.
- PRINCIPIOS BÁSICOS RELATIVOS A LA INDEPENDENCIA DE LA JUDICATURA.
- PRINCIPIOS BÁSICOS SOBRE EL EMPLEO DE LA FUERZA Y DE ARMAS DE FUEGO POR LOS FUNCIONARIOS ENCARGADOS DE HACER CUMPLIR LA LEY.
- PRINCIPIOS BÁSICOS SOBRE LA FUNCIÓN DE LOS ABOGADOS.
- PRINCIPIOS DE COOPERACIÓN INTERNACIONAL EN LA IDENTIFICACIÓN, DETENCIÓN, EXTRADICIÓN Y CASTIGO DE LOS CULPABLES DE CRÍMENES DE GUERRA, O DE CRÍMENES DE LESA HUMANIDAD.
- PRINCIPIOS DE ÉTICA MÉDICA APLICABLES A LA FUNCIÓN DEL PERSONAL DE SALUD, ESPECIALMENTE LOS MÉDICOS, EN LA PROTECCIÓN DE PERSONAS PRESAS Y DETENIDAS CONTRA LA TORTURA Y OTROS TRATOS O PENAS CRUELES, INHUMANOS O DEGRADANTES.
- PRINCIPIOS RELATIVOS A LA INVESTIGACIÓN Y DOCUMENTACIÓN EFICACES DE LA TORTURA Y OTROS TRATOS O PENAS CRUELES, INHUMANOS O DEGRADANTES.
- PRINCIPIOS RELATIVOS A UNA EFICAZ PREVENCIÓN E INVESTIGACIÓN DE LAS EJECUCIONES EXTRALEGALES, ARBITRARIAS O SUMARIAS.
    - PRINCIPIOS Y DIRECTRICES BÁSICOS SOBRE EL DERECHO DE LAS VÍCTIMAS DE VIOLACIONES MANIFIESTAS DE LAS NORMAS

INTERNACIONALES DE DERECHOS HUMANOS Y DE VIOLACIONES GRAVES DEL DERECHO INTERNACIONAL HUMANITARIO A INTERPONER RECURSOS Y OBTENER REPARACIONES.

- PROTOCOLO DE ESTAMBUL. MANUAL PARA LA INVESTIGACIÓN Y DOCUMENTACIÓN EFICACES DE LA TORTURA Y OTROS TRATOS O PENAS CRUELES, INHUMANOS O DEGRADANTES.
- R111 RECOMENDACIÓN SOBRE LA DISCRIMINACIÓN (EMPLEO Y OCUPACIÓN).
- R125 RECOMENDACIÓN SOBRE LAS CONDICIONES DE EMPLEO DE LOS MENORES (TRABAJO SUBTERRÁNEO), 1965.
- R14 RECOMENDACIÓN SOBRE EL TRABAJO NOCTURNO DE LOS MENORES (AGRICULTURA).
- R146 RECOMENDACIÓN SOBRE LA EDAD MÍNIMA, 1973.
- R190 RECOMENDACIÓN SOBRE LAS PEORES FORMAS DE TRABAJO INFANTIL.
- R41 RECOMENDACIÓN SOBRE LA EDAD MÍNIMA (TRABAJOS NO INDUSTRIALES), 1932.
- R52 RECOMENDACIÓN SOBRE LA EDAD MÍNIMA (EMPRESAS FAMILIARES).
- R79 RECOMENDACIÓN SOBRE EL EXAMEN MÉDICO DE APTITUD PARA EL EMPLEO DE LOS MENORES.
- R80 RECOMENDACIÓN SOBRE EL TRABAJO NOCTURNO DE LOS MENORES (TRABAJOS NO INDUSTRIALES), 1946.
- RECOMENDACIÓN SOBRE EL CONSENTIMIENTO PARA EL MATRIMONIO, LA EDAD MÍNIMA PARA CONTRAER MATRIMONIO Y EL REGISTRO DE LOS MATRIMONIOS.
- REGLAS DE LAS NACIONES UNIDAS PARA LA PROTECCIÓN DE LOS MENORES PRIVADOS DE LIBERTAD.
- REGLAS MÍNIMAS DE LAS NACIONES UNIDAS PARA LA ADMINISTRACIÓN DE LA JUSTICIA DE MENORES “REGLAS DE BEIJING”.

- REGLAS MÍNIMAS DE LAS NACIONES UNIDAS SOBRE LAS MEDIDAS NO PRIVATIVAS DE LIBERTAD "REGLAS DE TOKIO".
- REGLAS MÍNIMAS PARA EL TRATAMIENTO DE LOS RECLUSOS.

REGIONALES

Vinculantes

- CARTA DE LA ORGANIZACIÓN DE LOS ESTADOS AMERICANOS.
- CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS PACTO DE SAN JOSE DE COSTA RICA
- CONVENCIÓN INTERAMERICANA PARA LA ELIMINACIÓN DE TODAS LAS FORMAS DE DISCRIMINACIÓN CONTRA LAS PERSONAS CON DISCAPACIDAD.
- CONVENCIÓN INTERAMERICANA PARA PREVENIR Y SANCIONAR LA TORTURA, ADOPTADA EN LA CIUDAD DE CARTAGENA DE INDIAS, COLOMBIA.
- CONVENCIÓN INTERAMERICANA PARA PREVENIR, SANCIONAR Y ERRADICAR LA VIOLENCIA CONTRA LA MUJER, CONVENCIÓN DE BELÉM DO PARÁ.
- CONVENCIÓN INTERAMERICANA SOBRE CONCESIÓN DE LOS DERECHOS POLÍTICOS A LA MUJER.
- CONVENCIÓN INTERAMERICANA SOBRE DESAPARICIÓN FORZADA DE PERSONAS, ADOPTADA EN LA CIUDAD DE BELÉM, BRASIL, EL NUEVE DE JUNIO DE MIL NOVECIENTOS NOVENTA Y CUATRO.
- CONVENCIÓN INTERAMERICANA SOBRE LA CONCESIÓN DE LOS DERECHOS CIVILES A LA MUJER.
- ESTATUTO DE LA COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS.
- ESTATUTO DE LA CORTE INTERAMERICANA DE DERECHOS HUMANOS
- PROTOCOLO A LA CONVENCION AMERICANA SOBRE DERECHOS HUMANOS RELATIVO A LA ABOLICION DE LA PENA DE MUERTE.

- PROTOCOLO ADICIONAL A LA CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS EN MATERIA DE DERECHOS ECONÓMICOS, SOCIALES Y CULTURALES PROTOCOLO DE SAN SALVADOR
- REGLAMENTO DE LA COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS.
- REGLAMENTO DE LA CORTE INTERAMERICANA DE DERECHOS HUMANOS.

No vinculantes

- DECLARACIÓN AMERICANA DE LOS DERECHOS Y DEBERES DEL HOMBRE.
- DECLARACIÓN DE PRINCIPIOS SOBRE LIBERTAD DE EXPRESIÓN.
- DECLARACION DE RIO DE JANEIRO SOBRE LA INSTITUCION DEL REFUGIO.
- DECLARACIÓN DE SAN JOSÉ SOBRE REFUGIADOS Y PERSONAS DESPLAZADAS.
- DECLARACIÓN DE TLATELOLCO SOBRE ACCIONES PRÁCTICAS EN EL DERECHO DE LOS REFUGIADOS EN AMÉRICA LATINA Y EL CARIBE, 1999.
- DECLARACIÓN DEL DECENIO DE LAS AMÉRICAS: POR LOS DERECHOS Y LA DIGNIDAD DE LAS PERSONAS CON DISCAPACIDAD (2006-2016).
- DECLARACIÓN Y PLAN DE ACCIÓN DE MÉXICO PARA FORTALECER LA PROTECCIÓN INTERNACIONAL DE LOS REFUGIADOS EN AMÉRICA LATINA.
- PRINCIPIOS Y BUENAS PRÁCTICAS SOBRE LA PROTECCIÓN DE LAS PERSONAS PRIVADAS DE LIBERTAD EN LAS AMÉRICAS.
- PROGRAMA DE ACCIÓN PARA EL DECENIO DE LAS AMÉRICAS POR LOS DERECHOS Y LA DIGNIDAD DE LAS PERSONAS CON DISCAPACIDAD (2006-2016).

ANEXO 2

Africa [editar]

País	Convenio Cibercrimen		APCoC		Observaciones
	Firmado	Ratificado	Firmado	Ratificado	
Cabo Verde	—	19 de junio de 2018[1]	—	—	
Ghana	—	—	—	—	invitado
Marruecos	—	29 de junio de 2018[1]	29 de junio de 2018[2]	—	
Nigeria	—	—	—	—	invitado
Mauricio	—	15 de noviembre de 2013[1]	—	—	
Senegal	—	16 de diciembre de 2016[1]	16 de diciembre de 2016[2]	—	
Sudáfrica	23 de noviembre de 2001[1]	—	04 de abril de 2008[2]	—	
Túnez	—	—	—	—	invitado

América [editar]

País	Convenio Cibercrimen		APCoC		Observaciones
	Firmado	Ratificado	Firmado	Ratificado	
Argentina	—	05 de junio de 2018[1]	—	—	
Canadá	23 de noviembre de 2001[1]	08 de julio de 2015[1]	08 de julio de 2005[2]	—	
Chile	—	20 de abril de 2017[1]	—	—	
Colombia	—	—	—	—	invitado
Costa Rica	—	22 de septiembre de 2017[1]	—	—	
Panamá	—	05 de marzo de 2014[1]	—	—	
Paraguay	—	30 de julio de 2018[1]	—	30 de julio de 2018[2]	
Perú	—	—	—	—	obs 4.
República Dominicana	—	07 de febrero de 2013[1]	—	—	
Estados Unidos	23 de noviembre de 2001[1]	29 de septiembre de 2006[1]	—	—	

Asia [editar]

País	Convenio Cibercrimen		APCoC		Observaciones
	Firmado	Ratificado	Firmado	Ratificado	
Filipinas	—	28 de marzo de 2018[1]	—	—	
Israel	—	09 de mayo de 2016[1]	—	—	
Japón	23 de noviembre de 2001[1]	03 de julio de 2012[1]	—	—	
Sri Lanka	—	29 de mayo de 2015[1]	—	—	

Europa [editar]

País	Convenio Cibercrimen		APCoC		Observaciones
	Firmado	Ratificado	Firmado	Ratificado	
Albania	23 de noviembre de 2001[1]	20 de junio de 2002[1]	26 de mayo de 2003[2]	26 de noviembre de 2004[2]	
Andorra	23 de abril de 2013[1]	16 de noviembre de 2016[1]	23 de abril de 2013[2]	16 de noviembre de 2016[2]	
Armenia	23 de noviembre de 2001[1]	12 de octubre de 2006[1]	28 de enero de 2003[2]	12 de octubre de 2006[2]	
Austria	23 de noviembre de 2001[1]	13 de junio de 2012[1]	30 de enero de 2003[2]	—	
Azerbaiyán	30 de junio de 2008[1]	15 de marzo de 2010[1]	—	—	
Bélgica	23 de noviembre de 2001[1]	20 de agosto de 2012[1]	28 de enero de 2003[2]	—	
Bosnia y Herzegovina	09 de febrero de 2005[1]	19 de mayo de 2006[1]	09 de febrero de 2005[2]	19 de mayo de 2006[2]	
Bulgaria	23 de noviembre de 2001[1]	07 de abril de 2005[1]	—	—	
Croacia	23 de noviembre de 2001[1]	17 de octubre de 2002[1]	26 de marzo de 2003[2]	04 de julio de 2008[2]	
Chipre	23 de noviembre de 2001[1]	19 de enero de 2005[1]	19 de enero de 2005[2]	23 de junio de 2005[2]	
República Checa	09 de febrero de 2005[1]	22 de agosto de 2013[1]	17 de mayo de 2013[2]	07 de agosto de 2014[2]	
Dinamarca	22 de abril de 2003[1]	21 de junio de 2005[1]	11 de febrero de 2004[2]	21 de junio de 2005[2]	
Estonia	23 de noviembre de 2001[1]	12 de mayo de 2003[1]	28 de enero de 2003[2]	—	
Finlandia	23 de noviembre de 2001[1]	24 de mayo de 2007[1]	28 de enero de 2003[2]	20 de mayo de 2011[2]	
Francia	23 de noviembre de 2001[1]	10 de enero de 2006[1]	28 de enero de 2003[2]	10 de enero de 2006[2]	
Georgia	01 de abril de 2008[1]	06 de junio de 2012[1]	—	—	
Alemania	23 de noviembre de 2001[1]	09 de marzo de 2009[1]	28 de enero de 2003[2]	10 de junio de 2011[2]	
Grecia	23 de noviembre de 2001[1]	25 de enero de 2017[1]	28 de enero de 2003[2]	25 de enero de 2017[2]	

Hungría	23 de noviembre de 2001[1]	04 de diciembre de 2003[1]	—	—
Islandia	30 de noviembre de 2001[1]	29 de enero de 2007[1]	09 de octubre de 2003[2]	—
Irlanda	28 de febrero de 2002[1]	—	—	—
Italia	23 de noviembre de 2001[1]	05 de junio de 2008[1]	09 de noviembre de 2011[2]	—
Letonia	05 de mayo de 2004[1]	14 de febrero de 2007[1]	05 de mayo de 2004[2]	14 de febrero de 2007[2]
Liechtenstein	17 de noviembre de 2008[1]	27 de enero de 2016[1]	17 de noviembre de 2008[2]	—
Lituania	23 de junio de 2003[1]	18 de marzo de 2004[1]	07 de abril de 2005[2]	12 de octubre de 2006[2]
Luxemburgo	28 de enero de 2003[1]	16 de octubre de 2014[1]	28 de enero de 2003[2]	16 de octubre de 2014[2]
Malta	17 de enero de 2002[1]	12 de abril de 2002[1]	28 de enero de 2003[2]	—
Mónaco	02 de mayo de 2013[1]	17 de marzo de 2017[1]	17 de marzo de 2017[2]	17 de marzo de 2017[2]
Montenegro	07 de abril de 2005[1]	03 de marzo de 2010[1]	07 de abril de 2005[2]	03 de marzo de 2010[2]
Países Bajos	23 de noviembre de 2001[1]	16 de noviembre de 2006[1]	28 de enero de 2003[2]	22 de julio de 2010[2]
Noruega	23 de noviembre de 2001[1]	30 de junio de 2006[1]	29 de abril de 2008[2]	29 de abril de 2008[2]
Polonia	23 de noviembre de 2001[1]	20 de febrero de 2015[1]	21 de julio de 2003[2]	20 de febrero de 2015[2]
Portugal	23 de noviembre de 2001[1]	24 de marzo de 2010[1]	17 de marzo de 2003[2]	24 de marzo de 2010[2]
Moldavia	23 de noviembre de 2001[1]	12 de mayo de 2009[1]	25 de abril de 2003[2]	15 de febrero de 2017[2]
Rumania	23 de noviembre de 2001[1]	12 de mayo de 2004[1]	09 de octubre de 2003[2]	16 de julio de 2009[2]
Rusia	—[1]	—[1]	—	—
San Marino	17 de marzo de 2017[1]	—[1]	19 de mayo de 2017[2]	—
Serbia	07 de abril de 2005[1]	14 de abril de 2009[1]	07 de abril de 2005[2]	14 de abril de 2009[2]
Eslovaquia	04 de febrero de 2005[1]	08 de enero de 2008[1]	—	—
Eslovenia	24 de julio de 2002[1]	08 de septiembre de 2004[1]	26 de febrero de 2004[2]	08 de septiembre de 2004[2]
España	23 de noviembre de 2001[1]	03 de junio de 2010[1]	27 de noviembre de 2013[2]	18 de diciembre de 2014[2]
Suecia	23 de noviembre de 2001[1]	—[1]	28 de enero de 2003[2]	—
Suiza	23 de noviembre de 2001[1]	21 de septiembre de 2011[1]	09 de octubre de 2003[2]	—
Macao	23 de noviembre de 2001[1]	15 de septiembre de 2004[1]	14 de noviembre de 2005[2]	14 de noviembre de 2005[2]
Turquía	10 de noviembre de 2010[1]	29 de septiembre de 2014[1]	19 de abril de 2016[2]	—
Ucrania	23 de noviembre de 2001[1]	10 de marzo de 2006[1]	08 de abril de 2005[2]	21 de diciembre de 2006[2]
Reino Unido	23 de noviembre de 2001[1]	25 de mayo de 2011[1]	—	—

Oceanía [editar]

País	Convenio Cibercrimen		APCoC		Observaciones
	Firmado	Ratificado	Firmado	Ratificado	
Australia	—	30 de noviembre de 2012[1]	—	—	
Tonga	—	30 de noviembre de 2012[1]	—	—	

FUENTES DE CONSULTA

AGUSTINA, José Ramón*, La Pornografía; sus efectos sociales y criminógenos, una aproximación multidisciplinar*, Traducción de Miguel Garzón, España, Madrid, España, Edisofer Libros Jurídicos, 2011.

AZPILCUETA Hermilio, Tomas. *Derecho Informático*. Editorial Abeledo-Perrot Buenos Aires Argentina 1996.

CÁMPOLI, Gabriel Andrés. *Derecho Penal Informático en México*. Editorial INACIPE, México 2004.

CALVO López Pedro*, Derechos Humanos Victimología*, Terrorismo y sus diversas modalidades.

CARRANCÁ Y Trujillo, Raúl y Carrancá Y Rivas, Raúl. *Derecho Penal Mexicano***. (Parte general).** Vigésima tercera edición. Editorial Porrúa. México 2007.

CASTELLANOS Tena, Fernando. *Lineamientos elementales de Derecho Penal. **(Parte General);*** Cuadragésima séptima edición actualizada por Horacio Sánchez Sodi, primera reimpresión. Editorial Porrúa, México 2007.

CORREA, Carlos M. Carlos, *Derecho Informático***.** Editorial Desalma Buenos Aires Argentina 1994.

CUELLO Calón, Eugenio. *Derecho Penal.* **Parte General.** Décima octava edición. Editorial Nacional. México 1980.

DAVARA Fernández de Marcos Laura, Derecho Digital. Perspectiva Interdisciplinar, capitulo 7, Régimen jurídico de las redes sociales

DONDÉ Matute Francisco Javier (Coordinador) Delitos Transnacionales, Inacipe, tirant lo Blanch Ciudad de México, 2018.

DUVENGER, Maurice, Instituciones Políticas y Derecho Constitucional. Ed. Tecnos, Madrid, 1970

GÓMEZ Sánchez, Alejandro, *Nueva Legislación sobre delitos cibernéticos*, Revista Mexicana de Justicia.

HASKIN, David. *Multimedia fácil***.** (Traducción. Sánchez García Gabriel). Editorial Prentice Hall. México 1995.

HERRERA Ortiz, Margarita, *Manual de Derechos Humanos,* 4ª ed., México, Porrúa, 2003,

JIJENA Leiva Renato, *El Derecho y la Sociedad de la Información*: la importancia de internet en el mundo actual.

JIMÉNEZ DE ASÚA, Luis. *La Ley y el Delito***.** Décima primera edición, Editorial Sudamericana, Buenos Aires Argentina. Mayo 1980.

JIMÉNEZ DE ASÚA, Luis. *Tratado de Derecho Penal***.** Tomo III, Tercera edición actualizada. Editorial Losada, S.A. Buenos Aires 1965.

JIMÉNEZ HUERTA, Mariano. *Derecho Penal Mexicano***.** Tomo I. Quinta edición, Editorial Porrúa. México 1992.

KAPELLMAN Daniel, *México y el multilateralismo* La gobernanza del Ciberespacio y la incipiente participación de México, la SER, 2006. P.426- 457.

Lira Arteaga Oscar Manuel, *Cibercriminalidad, Fundamentos de investigación en México*, INACIPE, segunda edición, 2014.

LÓPEZ BETANCOURT, Eduardo. *Teoría del delito***.** Décima cuarta edición. Editorial Porrúa, México 2007.

LÓPEZ Calvo Pedro, Derechos Humanos, Victimología, Terrorismo y sus Diversas Modalidades Delictivas, capítulo V, pág. 440.

MALO CAMACHO, Gustavo. *Derecho penal mexicano. teoría general de la ley penal. Teoría general del delito. Teoría de la culpabilidad y el sujeto responsable, teoría de la pena.* Sexta edición Editorial Porrúa. México 2005.

MENENDEZ Mato, Juan Carlos, *Derecho e informática; Ética y Legislación*, [Barcelona]: Bosh, 2014.

MONTOYA Piña, Javier Omar, *Delitos Federales cometidos a través de medios informáticos*/ México, DF: Flores Editor y Distribuidor, [2015]

NAVA Garcés Alberto Enrique, *Ciberdelitos" Instituto Nacional de Ciencias Penales*, tirant lo Blanch, Ciudad de México 2019

NOGUEIRA Jorge*, Vinicius Higor, "Crimes Ciberneticos e a policía,Manual de Educacion Digital, IMMES, Brasil 2020.*

PEREZ Bes Francisco, "El Derecho de Internet: La Protección del honor, la intimidad y la propia imagen en internet, editorial, Salvador contreras Navidad"

PEREZ Luño Antonio Enrique, *Internet y Derechos Humanos, Derecho y Conocimiento* vol. 2, Facultad de Derecho Universidad de Huelva, 2014.

PEREZ Luño Antonio Enrique*, La Tercera Generación de los Derechos Humanos*, Thomson Aranzadi, Tirant lo Blanch, Valencia 2014.

PEREZ Luño Antonio Enrique, *Nuevas Tecnologías y Derechos Humanos*. Tirant lo Blanch, Valencia 2014

REYNOSO DÁVILA, Roberto. *Teoría general del delito*. Sexta edición. Editorial Porrúa. México 2006.

RIQUERT Marcelo Alfredo (Coordinador) *Ciberdelitos*, Ed. Hammurabi, Buenos Aires, Armeria, 2014. Pp.381.

RODAO, Jesús de Marcelo. *Piratas cibernéticos. cyberwars, seguridad Informática e Internet*. Editorial- Ra-ma. España 2005.

ROJAS Amandi, Víctor Manuel. *El uso de la Internet en el derecho*. Segunda Edición. Editorial Oxford, México 2001.

S/a, *La constitución del Ciberespacio*, México Porrúa: Universitatis Computensis, facultas Iuris: Red Internacional de Juristas para la Integración Americana 2015.

S/a, *Ciberdelitos: Grooming, Stalking, Bullying, Sexting, Ciberodio, Propiedad intelectual, Ciberpornografia infantil* Buenos Aires: Hammurabi,2014.

TÉLLEZ Valdés Julio. *Derecho Informático*. Tercera Edición. Editorial Mc Graw Hill, México 2003.

TORRES López, Mario Alberto; *Las Leyes Penales*. Editorial Porrúa. Quinta Edición. México 2005.

VELÁZQUEZ Elizarrarás Juan Carlos*, El estudio de caso en las relaciones Jurídicas Internacionales. Modalidades de aplicación del Derecho Internacional*, Libro PAPIME 2007. Pp. 1-35.

VELÁZQUEZ Elizarrarás Juan Carlos, *Líneas Generales sobre la Regulación Internacional del Ciberespacio* (2007)

VELÁZQUEZ Elizarrarás Juan Carlos *Casos y Aplicaciones Actuales del Derecho Internacional Penal*. Caso 14 Instauración de un marco legal Internacional de Internet y el control de la Piratería Informática, 2007.

VOLIO Fernando, Algunas Tipologías de Derechos Humanos. Universidad de Costa Rica, Costa Rica, 1978.

LIBROS ELECTRONICOS

AUCURIO del Pino Santiago, Delitos cibernéticos, en línea con dirección url: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf consulta 10-07-17

Bailón Corres Moisés Jaime, Derechos Humanos, generaciones de derechos, derechos de minorías y derechos de los pueblos indígenas; algunas consideraciones generales, en línea con dirección URL: https://www.corteidh.or.cr/tablas/r28614.pdf

BERNAL, Écija Álvaro, Ciberespacio un mundo sin ley, en línea con dirección URL: http://ciberderecho.com/El_ciberespacio_un_mundo_sin_ley.pdf

BUSTAMANTE, Donas Javier, Hacia la Cuarta Generación de los Derechos Humanos: repensando la condición humana en la Sociedad Tecnológica, Revista Iberoamericana de Innovación en línea con dirección URL: http://www.oei.es/revistacts/numero1/Bustamante.htm&gt

BRUNNER, J.J.: Cibercultura: la aldea global dividida. Mesa redonda sobre Cibercultura, Hannover, 2000, en línea con dirección URL: http://www.geocities.com/brunner_cl/cibercult.html consultado 14/09/18

CARBONELL, José Miguel, Capitulo II, El Acceso a Internet como derecho humano en línea con dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3647/8.pdf

CARPIZO Jorge/ Carbonell Miguel, Derecho a la Información y Derechos Humanos, en línea con dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/1/7/0.pdf

CASTAÑEDA, Mireya, El Derecho Internacional de los Derechos Humanos y su recepción nacional, Comisión Nacional de los Derechos Humanos, México, 2018, en línea con dirección URL: http://appweb.cndh.org.mx/biblioteca/archivos/pdfs/Observaciones-Comite-ONU-vol-II.pdf

CASTILLO Charo Alises, El Ciberodio con dirección URL: http://federacionkamira.com/wp-content/uploads/2017/01/PONENCIA-CHARO-ALISES-CIBERODIO.pdf

FLORES, Salgado Lucerito Ludmila, Temas actuales de los derechos humanos de última generación, Benemérita Universidad Autónoma de Puebla, Puebla México, 1era edición 2015, en línea con dirección URL: http://cmas.siu.buap.mx/portal_pprd/work/sites/fdcs/resources/PDFContent/1378/Libro%20DIG%20-%20Temas%20actuales%20de%20los%20derechos%20humanos.pdf

GOMEZ, de Agreda Ángel, El ciberespacio como escenario del conflicto. Identificación de las amenazas, 2012, en línea con dirección URL: https://dialnet.unirioja.es/servlet/articulo?codigo=4540391 consultado 30/10/18.

GRANADOS Delgado María Lourdes, Articulo, Delitos informáticos delitos electrónicos, en línea con dirección URL: http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf

MARTINEZ, Julio Cesar, El blanqueo de capitales, en línea con dirección URL: https://eprints.ucm.es/41080/1/T38338.pdf

NUÑEZ, Palacios Susana, Derechos Humanos en línea con dirección URL: file:///C:/Users/maby_/Downloads/5118-4517-1-PB.pdf

Naciones Unidas, Derechos Humanos, Oficina del Alto Comisionado, en línea con direcciónURL: https://www.hchr.org.mx/index.php?option=com_content&view=article&id=448&Itemid=249

Oficina del Alto Comisionado de Naciones Unida, Manual para Parlamentarios N 26 en línea con dirección URL: https://www.refworld.org.es/pdfid/5b72fb824.pdf

RAMIREZ Sánchez Jesús, Estudio descriptivo del malware en una dependencia académica de una institución pública de educación superior, en línea con dirección URL: https://www.uv.mx/iiesca/files/2016/11/06CA201601.pdf

ROMERO Flores Rodolfo, El robo de usurpación de identidad por medios informáticos o telemáticos: su tratamiento jurídico penal. en línea con dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/6/2958/20.pdf

RUIZ, Cassou Jorge Esteban, Delitos informáticos en México, 2009 Ciudad de México en línea con dirección URL: https://revistascolaboracion.juridicas.unam.mx/index.php/judicatura/article/view/32260/29257 consultado 14-03-2021.

S/A EcuRed, Características del Ciberespacio, en línea con dirección URL: https://www.ecured.cu/Ciberespacio consultado 30/10/18

SANTOS Villareal, Mario, la Corte Penal Internacional, servicios de investigación y análisis, en línea con dirección URL: http://www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-10-10.pdf

TELLEZ Valdés Julio, Derecho Informático, 1991, UNAM, México Porrúa en línea con dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/1/313/1.pdf

Touré Hamadoun, La Búsqueda de la Paz en el Ciberespacio, Unión Internacional de Telecomunicaciones en línea con dirección URL: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-S.pdf

TRIANA Lodoño Verónica, Representaciones del cuerpo y la mente de Neuromancer imaginado por William Gibson, en línea con dirección URL: https://repositorio.uniandes.edu.co/bitstream/handle/1992/14224/u240977.pdf?sequence=1 consultado 17-03-18

VELASCO De la Fuente, Homo criminals, en línea con dirección URL: https://criminal-mente.es/

FUENTES DE CONSULTA ELECTRÓNICAS:

Coronado Contreras Laura Verónica, “la libertad de expresión en el ciberespacio, en línea con dirección URL: http://eprints.ucm.es/33067/1/T36374.pdf [12-02-17]

Écija Bernal Álvaro, El ciberespacio, un mundo sin ley. Internet: la revolución que calmo las reglas del juego, en línea con dirección URL:https://revistascolaboracion.juridicas.unam.mx/index.php/revderechoprivado/article/view/20265/18192

HOWELL O´neill Patrick, MIT TECNOLOGY REVIEW, en línea con dirección URL: https://www.technologyreview.es//s/13405/la-gravedad-del-ransomware-sigue-creciendo-ante-la-inaccion-de-rusia consultado 29-06-2021.

Martínez Echeverría, Informática y Derechos Humanos en línea con dirección URL: Instituto de Investigaciones Jurídicas UNAM, en línea con dirección URL: https://revistascolaboracion.juridicas.unam.mx/index.php/revderechoprivado/article/view/20265/18192 consultado 16-06-19.

http://www.agendasanluis.com/alianza-interinstitucional-contra-delitos-ciberneticos/

Manual para Parlamentarios n0 26 en línea con dirección URL: https://www.ohchr.org/Documents/Publications/HandbookParliamentarians_SP.pdf consultado 6-06-19..

OFICINA DE SEGURIDAD INTERNAUTA, en línea con dirección URL: https://www.osi.es/es/actualidad/blog/2019/08/07/sabias-que-las-criptomonedas-estan-involucradas-en-algunos-ciberdelitos consultado 29-06-2021.

¿Qué son los Derechos Humanos? https://revistas.juridicas.unam.mx/index.php/cuestionesconstitucionales/article/view/5965/7906 consultado 1-06-19.

¿Qué nos enseña el caso Anonymous sobre los derechos civiles en Internet? En línea con dirección URL: https://m.eldiario.es

Carta de Derechos Humanos y Principios para Internet en línea con dirección URL: https://derechoseninternet.com/docs/IRPC_Carta_Derechos_Humanos_Internet.pdf

Carpizo Jorge, Los Derechos Humanos: Naturaleza, Denominación y Características, en línea con dirección URL: http://www.scielo.org.mx/pdf/cconst/n25/n25a1.pdf

Colisión de Principios básicos de Internet, en línea con dirección URL: https://internetrightsandprinciples.org/wpcharter/
Consejos para prevenir la intervención del malware, en línea con dirección URL: https://www.redeszone.net/tutoriales/seguridad/consejos-proteger-equipos-entrada-malware/

Diferencias entre Darknet y Deep web, en línea con dirección URL: https://www.xataka.com/basics/que-dark-web-que-se-diferencia-deep-web-como-puedesnavegarella#:~:text=Si%20la%20Deep%20Web%20es,0%2C1%25%20de%20ella.&text=La%20Dark%20Web%20es%20el,a%20Freenet%2C%20I2P%20o%20ZeroNet

ECOSOC 2007/20 Resolución sobre la cooperación internacional en la prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados, http://www./ecosoc/docs/2007/Resolution 202007. Pdf.
Estructura de la UIT en línea con dirección URL https://www.itu.int/es/about/Pages/default.aspx
Fernández García Jessica. Más Allá del Rosa-Ley Olimpia con Olimpia Coral. Youtube. https://www.youtube.com/watch?v=__0p-o7g71Q
Foro de Seguridad, Tipos de Delitos cibernéticos en línea con dirección URL: http://www.forodeseguridad.com/artic/discipl/disc_4016.htm consulta 26-09-16
GLOBAL VOICES, Noticias en línea con dirección URL: https://es.globalvoices.org/2019/07/04/defensores-de-derechos-digitales-y-sector-de-tecnologia-de-australia-buscan-revertir-ley-que-socava-encriptado/

Internet Society, Foro de Gobernanza de Internet, en línea con dirección URL: https://www.internetsociety.org/es/events/igf/2017/

La importancia de la Unión Internacional de Telecomunicaciones en línea con dirección URL: https://www.itu.int/es/about/Pages/default.aspx consultado 20-11-2019

Made for maid, noticias en línea con dirección URL: https://www.dw.com/es/la-industria-de-alemania-ante-la-amenaza-de-los-hackers/a-47001762

S/A Concepto de ciberespacio, en línea con dirección URL: https://www.uv.es/cefd/5/lima.html

S/A EcuRed, Áreas del ciberespacio, en línea con dirección URL: https://www.ecured.cu/Ciberespacio consultado 30/10/18

S/A los Derechos y Principios de Internet en línea con dirección URL: http://especiales.laprensagrafica.com/2011/internet/2011/04/10-derechos-y-principios-de-internet/ consultado 02-10-2020

Secretaria de Desarrollo Económico, el acceso a Internet como derecho humano, en línea con dirección URL: https://qroo.gob.mx/iqit/el-acceso-internet-un-derecho-humano#:~:text=El%20Consejo%20de%20Derechos%20Humanos,de%20todos%20los%20seres%20humanos

Sobre la Unión Internacional de Telecomunicaciones en línea con dirección URL: https://www.itu.int/es/about/Pages/default.aspx

S/A, Ética y Ciberespacio en línea con dirección URL: https://www.bbvaopenmind.com/articulos/etica-e-internet/

OFICINA DE SEGURIDAD INTERNAUTA, en línea con dirección URL: https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen

Resolución del ECOSOC 2004/26 Cooperación internacional en la prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados, http://www.un.org/ecosoc/docs/2004/Resolution%202004.-26pdf

Termino Crimipedia: web profunda, darknet y Tor, en línea con dirección URL: https://es.scribd.com/document/429101002/df

UIT, Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica en línea con dirección URL: https://www.itu.int/en/ITUD/Cybersecurity/Documents/Cybercrime2014_S.pdf

Universidad Abierta y a Distancia de México, en línea con dirección URL: https://gaceta.unadmexico.mx/historico-anual/66-2022/marzo-abril-2022/genero/112-de-que-trata-laleyolimpia#:~:text=Es%20un%20conjunto%20de%20reformas,de%20medios%20digitales%20(ciberviolencia)

ARTICULOS

ANNAN, Kofi: Informe a la Asamblea del milenio de las Naciones Unidas (2000) en línea con dirección URL: http://www.un.org/spanish/milenio/sg/report/full.htm. Consultado 10-08-2018.

MIRONOW Nicolas, Sistema jurídico de Rusia en línea con dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/7/3376/27.pdf consultado 29-06-2021

SLAUGHTER, Ana Marie, The chessboard, the web" en línea con dirección URL: http://www.extradigital.es/las-relaciones-internacionales-e-internet-por-mercedes-gracia/

Curso IV *Fundamentos teóricos de los derechos humanos*. Características y principio, en línea con dirección URL: https://cdhcm.org.mx/serv_prof/pdf/fundamentosteoricosdelosderechos.pdf

En la Biblioteca Digital de la Comisión Nacional de los Derechos Humanos, los principios de universalidad, interdependencia indivisibilidad de los derechos humanos en línea con dirección URL: https://www.cndh.org.mx/sites/all/doc/cartillas/20152016/34Principiosuniversalidad.pdf

S/A, Capítulo I, *Conceptos y Características de los Derechos Humanos*, en línea con dirección URL: www.derechos.org.mx

REVISTA, CYBERINTERNATIONALAFFAIRS, en línea con dirección URL: https://berenicefn.wordpress.com/2017/12/15/internet-y-su-efecto-sobre-los-derechos-humanos/

Corte Interamericana de los Derechos Humanos en línea con dirección URL: http://www.corteidh.or.cr/historia.cfm

Historia de la OEA en línea con dirección URL: http://www.oas.org/es/acerca/nuestra_historia.asp

NACIONES UNIDAS, La Corte Penal Internacional, en línea con dirección URL: http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/NacionesUnidas/Paginas/CortePenalInternacional.aspx

SERVICIO DE INFORMATICA, Universidad de Jaén, en línea con dirección URL: https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%201.%20SPAM.pdf

Lista de 8 maneras de hacer phishing en línea con dirección URL: https://www.osi.es/es/actualidad/blog/2014/03/04/las-8-falsas-ofertas-de-empleo-mas-utilizadas-por-ciberdelincuentes-en-in

FUNDACION EN MOVIMIENTO en línea con dirección URL: http://www.fundacionenmovimiento.org.mx/dvsexting?gclid=EAIaIQobChMI5rqtgZrb4AIVBNvACh0dAwpcEAAYAiAAEgJFTPD_BwE

S/a, Revista sobre delitos ciberneticos en linea con direccion URL: https://revistaenterate.mx/index.php/legisladores-home/12010-propone-tipificar-al-sexting-y-grooming-como-delito

Ley Especial sobre los Delitos informáticos de Venezuela de 2001, texto completo http://www.tsj.gov.ve/lrgislacion/ledi.htm

Centeno Dayna, México y el Convenio de Budapest, edición Marianne Diaz, junio 2018, en línea con dirección URL: https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf

Consejo de Europa y derechos humanos, en línea https://www.coe.int/en/web/conventions/fulllist//conventions/treaty/185/signatures?p_auth=hZgYFWIA consultado 28-02-2020.

UIT, Comprensión del ciberdelito: fenómenos, dificultades y respuesta jurídica en línea con dirección URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf