UNIVERSIDAD DE EL SALVADOR
FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES
ESCUELA DE RELACIONES INTERNACIONALES

VULNERABILIDAD JURÍDICA DE LA INFORMACIÓN DIGITAL DE LOS HABITANTES DEL ESTADO SALVADOREÑO FRENTE A LOS CIBERDELITOS POR AGENTES FUERA DE LA JURISDICCIÓN SALVADOREÑA

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE LICENCIADO EN RELACIONES INTERNACIONALES

PRESENTADO POR:

ELMER ARTURO BONILLA RUIZ
JAVIER ARNOLDO CHÁVEZ MURRILLO
JOSÉ EDUARDO GODOY ZALDAÑA

DOCENTE ASESOR:

LICENCIADO DANNY OBED PORTILLO AGUILAR

CIUDAD UNIVERSITARIA, SAN SALVADOR, MARZO DE 2022

TRIBUNAL CALIFICADOR

LICENCIADA KARLA GABRIELA LEÓN DE PÉREZ

PRESIDENTA

LICENCIADO MIGUEL ÁNGEL FLORES

SECRETARIO

LICENCIADO DANNY OBED PORTILLO AGUILAR

VOCAL

UNIVERSIDAD DE EL SALVADOR

MSC. Roger Armando Arias Alvarado
RECTOR

Dr. Raúl Ernesto Azcúnaga López
VICERECTOR ACADÉMICO

Ing. Juan Rosa Quintanilla Quintanilla
VICERECTOR ADMINISTRATIVO

Ing. Francisco Antonio Alarcón Sandoval
SECRETARIO GENERAL

Licdo. Rafael Humberto Peña Marín
FISCAL GENERAL

Licdo. Luis Antonio Mejía Lipe
DEFENSOR DE LOS DERECHOS UNIVERSITARIOS

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

Dra. Evelyn Beatriz Farfán Mata
DECANA

Dr. Edgardo Herrera Medrano Pacheco
VICEDECANO

Msc. Digna Reina Contreras de Cornejo
SECRETARIA

MFE. Nelson Ernesto Rivera Díaz
DIRECTOR DE ESCUELA DE RELACIONES INTERNACIONALES

Msc. Diana del Carmen Merino de Sorto
DIRECTORA GENERAL DE PROCESOS DE GRADUACIÓN

Licda. Santos del Carmen Flores Umaña
COORDINADORA DE PROCESO DE GRADUACIÓN DE LA ESCUELA DE RELACIONES INTERNACIONALES

Dedicatoria

A Dios todo poderoso por su infinita gracia y bondad, a mi familia por su amor y apoyo incondicional, a mis amigos por su amistad, al Alma Mater de la Universidad de El Salvador que a través sus docentes, personal administrativo y de servicio por todo el conocimiento, experiencia y sabiduría brindada en cada momento en las aulas y los pasillos, y sin faltar, mis agradecimientos al fútbol y al arbitraje los cuales crearon en mí, además de orden y disciplina, la necesidad y deseo por superarme a través de la preparación y estudio académico. También, una mención especial al Licenciado Danny Obed Portillo Aguilar, nuestro asesor quien ha dado un aporte muy valioso para el desarrollo de este informe, pero sobre todo por su calidad humana y profesional.

“Hacia la libertad por la cultura”

Elmer Arturo Bonilla Ruiz

Dedicatoria

Primeramente, agradezco a Dios por su amor y gracia, a mi familia por amarme incondicionalmente y apoyarme desmedidamente, a mis amigos que estuvieron pendientes de mí en toda mi formación de manera incondicional, a las personas que fueron mis compañeros de estudio en cada ciclo, a todas las personas que conforman la Facultad de Jurisprudencia y Ciencias Sociales, en específico a las personas que conformaron la Escuela de Relaciones Internacionales en el transcurso de mi formación, desde el personal administrativo hasta cada uno de los docentes que dieron su máximo esfuerzo por compartir sus conocimientos de la mejor manera posible. Hago una mención especial a mi Madre por motivarme en los momentos más difíciles, por ella he logrado alcanzar muchas de las metas que me he propuesto, también agradezco a mis compañeros Elmer Bonilla y Eduardo Godoy por dar su máximo esfuerzo para culminar el presente trabajo de investigación. Por último, hago una mención especial al Licenciado Danny Obed Portillo Aguilar, por su profesionalismo como asesor, demostrando un compromiso invaluable por brindar todos los aportes necesarios para el desarrollo del presente trabajo de investigación.

“Hacia la libertad por la cultura”

Javier Arnoldo Chávez Murillo

Dedicatoria

El primer agradecimiento a Dios por su infinita misericordia aun en momentos muy difíciles y que a pesar de cualquier circunstancia siempre está ahí, a mi madre quien ha sido la persona que me ha apoyado desde mi primer día de vida y a quien le debo todo y la persona quien soy en todos los aspectos, a mi hermano que es para mí lo más valioso que tengo y ha tenido la valentía de salir adelante y sobrevivir pese a cualquier adversidad, mi familia que son por quienes me esfuerzo cada día por ser un mejor ser humano y profesional y a quienes me debo completamente y han estado conmigo en cada etapa de mi vida, a la sociedad salvadoreña ya que con sus contribuciones hacen posible que algunos salvadoreños tengamos esa posibilidad de poder obtener estudios superiores. A todos mis amigos, compañeros, maestros, empleados en general y todas las maravillosas personas sin exclusión alguna que tuve el gusto y honor de conocer durante toda mi etapa de estudio, sin duda cada experiencia compartida ha forjado en mi lo que ahora soy. Una mención especial a nuestro asesor el licenciado Danny Obed Portillo Aguilar quien ha puesto toda su experiencia y esmero en nuestro proyecto para llevarlo a buen término. A todos ustedes quienes utilizarán este documento para su formación, crecimiento y conocimiento.

“Hacia la libertad por la cultura”

José Eduardo Godoy Zaldaña

ÍNDICE DE CONTENIDOS

RESUMEN

La globalización y el desarrollo tecnológico ha llevado a la aldea global a la era digital o transformación digital a pasos acelerados, junto a este fenómeno van los riesgos que esto genera y por eso surge la necesidad de analizar la situación jurídica de la información digital de los habitantes del Estado salvadoreño frente a ciberdelitos por agentes fuera de la jurisdicción.

Es por lo anterior que se realiza una investigación de carácter académica descriptiva con el fin de acreditar el conocimiento del tema en investigación, he ahí la presentación desde un enfoque descriptivo y sintético. La investigación es de tipo exploratoria-descriptiva por el hecho que no es tan riguroso, pero si busca recabar información que permita reconocer el fenómeno y materia en estudio. En cuanto al método que se utilizó es analítico-inductivo porque se buscó descomponer en partes el todo, yendo de lo particular a lo general y luego agrupar cada parte para realizar un análisis estructurado.

El informe consta de tres aspectos principales en sus tres capítulos respectivamente, que giran en torno a la protección de la información personal digital. Primero, la evolución del derecho en materia de ciberespacio; Segundo, el marco jurídico salvadoreño en esta materia; Tercero, los retos y perspectivas en torno a la seguridad jurídica y la existencia o no de una política pública en materia de ciberseguridad y protección de la información personal digital. Finalmente, se encuentras las conclusiones y recomendaciones como resultado del análisis y estudio en la materia.

Palabras claves: Información personal digital, ciberseguridad, ciberdelitos, ciberderecho, seguridad jurídica, gobernanza regional, gobernanza global.

LISTA DE SIGLAS Y ABREVIATURAS

DARPA	Defense Advance Research Projects Agency o Agencia de Proyectos de Investigación Avanzada de Defensa en español
ARPANET	Adanced Research Projects Agency Network o Red de Agencias de Proyectos de Investigación Avanzada en español.
NPL	National Physical Laboratory o Laboratorio Nacional de Física en español.
IMP	Interface Message Processor o Procesadores de Mensajes de Interfaz (PMI) en español.
UCLA	Universidad de California en Los Ángeles.
NWG	Network Working Group o Red de Grupo de Trabajo en español.
PCR	Protocolo de control de red.
CFAA	Computer Fraud and Abuse Act o Ley de Abuso y Fraude Informático en español.
TIC	Tecnologías de la Información Comunicación.
FBI	Federal Bureau of Investigation u Oficina Federal de Investigaciones en español.
OEA	Organización de Estados Americanos.
Cyber4Dev	Cyber Resilience for Development o Ciber Resiliencia para el Desarrollo en español.

ONU	Organización de las Naciones Unidas.
ITU	International Telecommunication Union o Union de Telecomunicaciones Internacionales, UTI en español.
ESCA	Estrategia de Seguridad Centroamericana.
BCIE	Banco Centroamericano de Integración Económica.
PARLACEN	Parlamento Centroamericano.
UE	Unión Europea.
OTAN	Organización del Tratado del Atlántico Norte.
NIS	Network Information Service o Sistema de Información de las Redes en español.
OMC	Organización Mundial del Comercio.
OMPI	Organización Mundial de la Propiedad Intelectual.
ISP	Internet Service Providers o Proveedor de Servicios de Internet en español.
OCDE	Organización para la Cooperación y el Desarrollo Económicos.

INTRODUCCIÓN

En este informe final de investigación se desarrolla la temática: “vulnerabilidad jurídica de la información digital de los habitantes del Estado salvadoreño frente a los ciberdelitos por agentes fuera de la jurisdicción salvadoreña”, tema que surge ante el fenómeno de la globalización y el desarrollo del Internet, las TIC y la transformación digital de la sociedad, lo cual como todo proceso social conlleva cambios en el desarrollo de actividades económicas, comerciales, teletrabajo, transacciones digitales financieras y otras actividades remotas. Este cambio lleva a un mayor grado de vulneración y exposición de bienes como la información persona digital frente a otros agentes, ciberdelincuentes, en un entorno digital transfronterizo, los cuales actúan fuera de la jurisdicción del territorio de El Salvador, lo que lleva a la necesidad de estudiar el marco jurídico nacional en materia de ciberseguridad y ciberderecho, la agenda de seguridad nacional, aún más si existe una política pública en esta materia. La importancia de un marco jurídico, agenda y política pública en materia de ciberseguridad son importantes para la búsqueda de alianzas en el ámbito internacional con una perspectiva multilateral desde lo regional a lo global.

La situación de la información digital conlleva un mayor grado de vulneración de la información por ciberdelincuentes y otros agentes dentro del ciberespacio, así como la evolución de la materia relacionada al ciberespacio y ciberderecho que permite entender la necesidad de la creación de un marco jurídico, instituciones e instrumentos que aborden esta materia para el tema de gobernanza y cooperación en la materia. Ahora bien, por su naturaleza, es importante la definición del marco jurídico institucional en materia para el caso de El Salvador. Por eso el hecho de identificar las normativas nacionales que se emplean en el marco de la protección de la información personal digital ayudará a determinar de

manera detallada el marco jurídico en materia de información digital que se posee en El Salvador, así se podrá elaborar realizar observaciones pertinentes a lo que el contexto tecnológico actual demanda en materia técnica y jurídica, así como determinar los retos y perspectivas en torno a la materia y elementos establecidos, por parte de El Salvador. Ahora bien, por eso surge la necesidad de determinar a través de la investigación y análisis crítico del contexto nacional e internacional, como academia para dar una respuesta y alternativa al fenómeno de la transformación digital y la protección de la información digital sin vulnerar el derecho a la privacidad de cada ciudadano.

Un elemento fundamental de esta investigación, lo posee el análisis de la situación jurídica de la información digital de los habitantes del Estado salvadoreño frente a ciberdelitos por agentes fuera de la jurisdicción; desde luego, es importante identificar la evolución del derecho internacional en materia de ciberespacio y ciberderecho con relación a la protección de los datos personales, por lo que el examinar el marco jurídico e institucional en esta materia en El Salvador es fundamental y bajo estos elementos poder determinar los retos y perspectivas que existen para El Salvador en relación a la protección de la información personal digital frente a la ciberdelincuencia.

El informe se aborda a través de una investigación académica descriptiva la cual tiene como finalidad principal acreditar de manera satisfactoria el conocimiento del tema investigado, por lo que se presenta de manera descriptiva y sintética. El tipo de estudio realizado es el exploratorio-descriptivo, ya que el método descriptivo no busca aportar información rigurosa e interpretada según los criterios establecidos por cada disciplina científica, se buscó obtener toda la información necesaria sobre el fenómeno investigado. Ahora en cuanto al método a utilizado fue el analítico-inductivo, ya que se hizo una descomposición del todo en sus

partes pasando de lo particular a lo general, para luego agrupar sus partes y estructurar el análisis.

En el presente informe se divide en las partes generales como resumen, lista de abreviaturas, índice y respectiva introducción, luego se presentan los tres capítulos de la investigación. El capítulo I: La evolución del derecho internacional en materia de ciberespacio y ciberderecho en relación con la protección de los datos personales**.** En este capítulo se busca exponer los elementos generales que constituyen la referencia teórica e histórica de un nuevo interés social por atender: las relaciones en el ciberespacio. Se desarrolla los aspectos sobre la evolución del Internet y las consecuencias en sus diferentes dimensiones como las industriales, económicas y colectivas en general, así como las vulnerabilidades que conlleva para la sociedad por los comportamientos sociales y la necesidad de nuevas formas jurídicas a considerar para su regulación y aquí la importancia del Estado.

Además, se abordan tres temáticas vinculantes en esta materia como lo son los crímenes cibernéticos y sus diferentes informes, la agenda de ciberseguridad de los Estados de forma general y la gobernanza del Internet y del ciberespacio.

Ahora bien, luego se desarrollan los siguientes dos capítulos. El capítulo II: Marco jurídico e institucional salvadoreño en torno a la protección de la información personal digital, dentro del contexto del internet, globalización, ciberespacio. En este apartado se establece el desarrollo de la normativa en relación a la protección de la información personal digital desde la LEDIC, Ley de delitos informáticos y conexos, bajo el entorno de crecimiento del internet y el surgimiento de diferentes acciones que podrían lesionar la dignidad de las personas y otros bienes jurídicos. Además, se plantea la naturaleza del ciberdelito de tipo privado y sus implicaciones y el marco jurídico de rango constitucional y su realidad y perspectiva en cuanto a los tratados internacionales. Otro aspecto que se desarrolla es el del

modelo de gobernanza, ya que la complejidad en la determinación del bien jurídico atiende a la supranacionalidad que tiene el internet

Finalmente, en el capítulo II: Los retos y perspectivas en torno a la seguridad jurídica en la protección de la información personal digital en El Salvador y política pública de ciberseguridad. Se desarrolla la perspectiva de la doctrina jurídica de la privacidad y la privacidad como derecho humano frente a la doctrina jurídica de la vigilancia estatal como mecanismo de prevención social, es hablar de derechos humanos no como derechos absolutos y para lo cual se toma en cuenta los marcos jurídicos nacionales frente a los internacionales como tratados, convenciones y principios. Además, se presenta una perspectiva de las políticas públicas en materia de ciberseguridad en la región centroamericana hasta llegar a abordar de manera particular la situación de la ciberseguridad en El Salvador. Además, se encuentran las conclusiones y recomendaciones como resultado del análisis y estudio en la materia

CAPÍTULO I: LA EVOLUCIÓN DEL DERECHO INTERNACIONAL EN MATERIA DE CIBERESPACIO Y CIBERDERECHO EN RELACIÓN CON LA PROTECCIÓN DE LOS DATOS PERSONALES

Introducción capitular

Este capítulo expone argumentos que permiten concretar lo planteado en el objetivo “analizar la evolución del Derecho Internacional en materia de ciberespacio y ciberderecho en relación con la protección de los datos personales.” En ese sentido se desarrollan los elementos generales que constituyen la referencia teórica e histórica de un nuevo interés social por atender: las relaciones en el ciberespacio. Es así, como se exploran los aspectos sobre la evolución del Internet y las consecuencias en sus diferentes dimensiones como las industriales, económicas y colectivas en general, además de las vulnerabilidades que conlleva para la sociedad por los comportamientos sociales y la necesidad de nuevas formas e instituciones jurídicas a considerar para su regulación, radicando ahí la importancia del papel del Estado en esas acciones específicas. Es así como surge la importancia de identificar las implicaciones conceptuales en esta materia desde el concepto global de ciberespacio hasta lo específico en relación a la información personal digital y que es en este último aspecto donde se desenvuelve los aspectos medulares: la privacidad y seguridad individual frente a los ordenamientos jurídicos. Además, se abordan tres temáticas fundamentales: los crímenes cibernéticos y sus diferentes informes, la agenda de ciberseguridad de los Estados de forma general y la gobernanza del Internet y del ciberespacio.

1.1 Evolución de la relación derecho e internet

Internet es sin duda un ejemplo de cómo el ordenamiento jurídico se ubica por detrás del cambio de las demás formas sociales y de las relaciones que de esta se derivan. El Internet que se utiliza en la actualidad encuentra sus inicios en 1973 con el descubrimiento de los protocolos de comunicación, aunque como red entró en funcionamiento a inicio del año 1983; en estas primeras décadas de su existencia se restringió a una élite académica y de investigación.[1]

En la década de 1990, el internet comenzó a filtrarse en la sociedad y en la actualidad es ampliamente considerada como una tecnología de propósito general, sin la cual la sociedad moderna no podría funcionar. Es decir, en un período relativamente corto, la tecnología pasó de ser una herramienta exclusiva e inusual, a tener una utilidad esencial, análoga situación a lo ocurrido con el desarrollo de la red eléctrica.[2]

Hoy en día, la sociedad se encuentra en una situación de dependencia de un sistema tecnológico, que es a la vez muy disruptivo y esto trae consigo consecuencias en las dimensiones industriales, económicas y colectivas en general, expuestas en una ola de "destrucción creativa" desatada por el cambio tecnológico resultante, luchando por adaptarse a un rápido ritmo de desarrollo.[3]

El Internet, expone serias vulnerabilidades para la sociedad, que configuradas en nuevos comportamientos sociales sugieren la existencia de nuevas figuras e instituciones jurídicas a considerarse como objeto de regulación. Estos nuevos comportamientos que exponen vacíos jurídicos,

[1] Rubén Cañedo Andalia. “Aproximaciones para una historia de Internet”. ACIMED, n.1 (2004). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000100005

[2] Nickolas Pisciottano, "The Impact of the Internet on Social Capital: Broadband Access and Influences on Voting Turnout" (Thesis, Hopkins University, 2019), https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/61851/Pisciottano,%20Nickolas.pdf?sequence=1

[3] Andrew Keen. Internet no es la respuesta. (España: Catedral Editorial, 2016).

y algunos de estos, potencialmente peligrosos requieren de una rápida actuación por parte del sistema jurídico de un Estado, y presentan el desafío de diseñar normas jurídicas e instituciones reguladoras que sean aptas para el propósito de la nueva era digital.[4]

Los primeros estudios establecidos acerca de las intercomunicaciones generales fueron realizados a través de una serie de artículos elaborados por Licklider en 1962, tal como lo describe Tavosanis,[5] quien indica, que en la época habían múltiples puntos de vistas hacia la definición de "Red Espacial", proyectándose como un vinculado de ordenadores conexos a nivel mundial a través del cual se podía adherirse ágilmente a datos y trasmisiones desde cualquier sitio, básicamente el espíritu de lo que, en hoy en día, conocemos como Internet.

De acuerdo a Bay,[6] el científico Leonard Kleinrock, elaboró una teoría de la conmutación de paquetes, y en ella, el autor se dedicó a convencer a otros científicos sobre la posibilidad especulativa de comunicarse por medio de las líneas telefónicas, empleando paquetes en lugar de circuitos, lo cual generó un gran paso dentro del avance de los computadores en redes.

Luego, en 1965 se llevó a cabo otro paso clave, el hacer que las computadoras se comunicaran de manera conjunta. Tal como indica Villanueva,[7] Thomas Merrill y Robert McGhee conectaron la computadora TX-2 en Massachusetts al Q-32 en California utilizando una línea telefónica

[4] Ana Isabel Meraz Espinoza. "Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales". *Revista IUS*, n.41 (2018), http://www.scielo.org.mx/pdf/rius/v12n41/1870-2147-rius-12-41-293.pdf.
[5] Mirko LA Tavosanis, "Libraries, Linguistics and Artificial Intelligence. Jcr Licklider and the Libraries of the Future". *Rivista italiana di biblioteconomia, archivistica e scienza dell'informazione,* n. 3 (2017). https://dialnet.unirioja.es/servlet/articulo?codigo=6119085
[6] Morten Bay, "Conversation with a pioneer: Leonard Kleinrock on the early days of networking, the arpanet… and winning in Las Vegas". *Internet Histories*, n. 1-2 (2018): 140-152, https://doi.org/10.1080/24701475.2018.1446239.
[7] J Villanueva et al., "Aplicación de la transformada de Hilbert-Huang en el análisis de señales de comunicación satelital", *Revista Iberoamericana de Automática e Informática industrial*, n. 2 (2020), https://doi.org/10.4995/riai.2019.10878.

de discado de poca velocidad, de esta manera se fue instaurando la primera pequeña red de computadoras de área amplia en la historia.

La consecuencia de esta experimentación fue la sagacidad con la que operaban las computadoras, instituyendo programas y recobrando datos según fuera necesario en el aparato remoto, aunque en aquel momento el medio telefónico de circuitos conmutados era completamente inoportuno para la labor.

A finales de 1966, McGhee desarrolló en DARPA (*Agencia de Proyectos de Investigación Avanzada de Defensa*) el concepto de red informática, y rápidamente en 1967, elaboró su plan para “ARPANET” (*Red de Agencias de Proyectos de Investigación Avanzada*).

Dichas investigaciones fueron presentadas a diversos científicos, y en ellas se abordó una nueva conceptualización de red de paquetes, elaboradas por Donald Davies y Roger Scantlebury de NPL (Laboratorio Nacional de Física). En 1964, este grupo de científicos elaboraron un artículo sobre la implementación de redes de cambios para el ejército; pero, durante el proceso, diversos trabajos similares de MIT (Instituto de Tecnología de Massachusetts) y NPL, se estaban trabajando de manera paralela, sin que ninguno de los investigadores supiera sobre el trabajo del otro; por lo que decidieron compartir sus experiencias en la investigaciones, y bautizar la expresión "paquete", siendo aplicada por primera vez en un artículo de NPL.

En 1968, la colectividad desarrollada por DARPA redefinió la distribución ordinaria y las descripciones de ARPANET, esto generó que DARPA llevara a cabo un presupuesto especial para el desarrollo de los Procesadores de Mensajes de Interfaz (PMI); el cual fue abordado por un equipo de

investigación conformado por Bolt Beranek y Newman, denominados BBN [8] *Three Kinds of Demand Pull for the Arpanet into the Internet*.

El desarrollo de la Teoría de Conmutación de Kleinrock basó su perspectiva en la observación, esquema y cotejo, por consiguiente, se llevó a cabo el primer nodo de ARPANET, en el Centro de Medición de Redes en UCLA (Universidad de California), al mismo tiempo se instaló el primer IMP en UCLA, creado por BBN, dando inicio al incipiente monitor del host.[9]

Lo acontecido motivo a Doug Engelbart a elaborar un artículo sobre el "Aumento del intelecto humano", el cual fue propicio para un segundo nodo, este último se circunscribió a la redistribución de los nombres de host a direcciones.[10]

Luego de esta propuesta, se llevó a cabo el primer mensaje entre interconectores de Host, lo que incluyó comunicación entre el Laboratorio de Kleinrock y la Universidad de Stanford; luego se procedió a instalar dos nodos más entre las entidades académicas de la Universidad de Santa Bárbara y Utah, estos últimos unieron propósitos para la visualización de aplicaciones, manipulando pantallas de almacenamiento para atender el problema de modernización en la red.[11]

A finales de 1969, cuatro computadoras anfitrionas se conectaron al ARPANET, y el naciente internet despegó. Incluso en esa etapa inicial, se tomó en cuenta las investigaciones sobre redes y se incorporó la labor de red subyacente; esta tradición continúa hasta el día de hoy.

---

[8] Noel Packard, "Three Kinds of Demand Pull for the Arpanet into the Internet". *Cogent Social Sciences*, n. 1 (2020), https://doi.org/10.1080/23311886.2020.1720565.
[9] Eugenio Muttio, Salvador Botello y Maximino Tapia, "Modelado Paramétrico mediante Programación Visual en el diseño y análisis estructural de edificios", *Revista Mexicana de Métodos Numéricos*, n.1 (2017), https://www.scipedia.com/public/Muttio_et_al_2017a.
[10] Bin Dai et al. "Enabling network innovation in data center networks with software defined networking: a survey", *Journal of Network and Computer Applications*, no. 94 (2017): 33-49. https://doi.org/10.1016/j.jnca.2017.07.004.
[11] Fenwick McKelvey y Kevin Driscoll. "Arpanet and its boundary devices: modems, imps, and the inter-structuralism of infrastructures". *Internet Histories*, n.1 (2019), https://doi.org/10.1080/24701475.2018.1548138.

Sin embargo, lo que llevó a que las computadoras se anexaran ágilmente a ARPANET durante los años subsiguientes, fue la continuidad en la mejora en la comunicación de host a host, hasta lograr que fuese completamente funcional junto a otros softwares de red.

En 1970, el Network Working Group (NWG) finalizó el registro preliminar de ARPANET Host-to-Host, denominado Protocolo de control de red (PCR); esto se debió a que los sitios de ARPANET terminaron de implementar NCP y los beneficiarios de la red posteriormente lograron evolucionar las aplicaciones.

En 1972, se llevó a cabo una demostración oficial sobre el manejo de esta nueva tecnología de red al público. En ese mismo periodo, se creó la aplicación naciente del correo electrónico, para ello, el grupo BBN propuso elaborar un software elemental de envío y lectura de recados de correo electrónico, originado por la insuficiencia de desarrolladores de ARPANET al no contar con un componente de conexión sencilla.

No obstante, Pooley,[12] enfatiza que McGhee amplió su interés elaborando el primer programa para utilizar el correo electrónico, en ella contenía las instrucciones de enumerar, leer, archivar, reenviar y responder recados de manera selectiva. Este proceso, permitió que el correo electrónico se convirtiera en una de las aplicaciones de red más grande.

La regulación de Internet es ya una realidad jurídica, existen diversos instrumentos internacionales que regulan esta actividad a nivel nacional e internacional en diversas manifestaciones, desde el ámbito constitucional hasta el plano internacional en el que se busca la protección de los derechos de propiedad intelectual en materia de nombres de dominio, regulación de sitios web, comercio electrónico, libertad de expresión,

[12] Jefferson Pooley, "The Post-Program Era: The Rise of Internet & Society Centers - and a New Interdiscipline". *Culture Digitaly* (Blog), 5 de marzo de 2018, https://culturedigitally.org/2018/03/the-post-program-era-the-rise-of-internet-society-centers-and-a-new-interdiscipline/.

protección a la intimidad, del documento electrónico y firma digital, y también sobre los delitos penales.

El Internet, ha construido una nueva comunidad jurídica, en el que el respeto y la convivencia civilizada de los cibernautas, a partir de los principios de transparencia, cooperación, buena fe, seguridad y responsabilidad, han dado nacimiento a nuevas formas de ejercer los derechos y a nuevas obligaciones que deben ser garantizadas por los Estados y la sociedad, procurando de forma efectiva los derechos humanos de todas las personas.

La regulación del internet se ha desarrollado como consecuencia de actos delictivos que no estaban regulados en el derecho, valiéndose del ciberespacio, o bien, debido a que delitos ya existentes iniciaron a hacer uso de internet y otros medios digitales para concretarse. Pero, la consideración de internet como un derecho se debe a su valoración como derecho humano, y debe estudiarse desde dos vertientes, por un lado, la provisión del acceso como un medio que activa el ejercicio y disfrute del internet, que por su aporte a la sociedad del conocimiento se ha considerado un derecho humano y, por otro lado, como derecho humano que habilita una nueva gobernanza que implica nuevos bienes jurídicos a tutelar, así como políticas públicas orientadas a asegurar un acceso universal de este recurso a los ciudadanos. La valoración del internet como derecho humano se explora más adelante en la presente investigación, y en ese apartado se denota la relación entre ambos.

1.2 Implicaciones conceptuales: ciberespacio, ciberdelincuentes, ciberseguridad, ciberderecho, ciberdelitos y cibercrimen

1.2.1. Ciberespacio

Se define como el uso de la electrónica y el espectro electromagnético para acumular, cambiar y mercantilizar datos a través de métodos en red y

fundamentos mecánicos asociadas. De acuerdo con de Souza,[13] el ciberespacio se puede considerar como la interconexión de los seres humanos a través de las computadoras y las telecomunicaciones, sin tener en cuenta la geografía física, ya que todas las interacciones, intercambio de información, entre otros, se realizan en un entorno virtual, o sea, espacios inmateriales sin fronteras y limites, en el cual se utiliza el internet y dispositivos electrónicos para tal fin.

1.2.2. Ciberdelincuentes

Son personas o equipos de personas que utilizan la tecnología para realizar actividades maliciosas en sistemas o redes digitales con la intención de robar información confidencial de la empresa o datos personales y generar ganancias. Tal como señala Barrio,[14] estos acceden a los mercados clandestinos que se encuentran en la web profunda para intercambiar bienes y servicios maliciosos, como herramientas de piratería digital[15] y datos robados.

Las leyes relacionadas con el delito cibernético continúan evolucionando en varios países del mundo. Esto hace que los organismos encargados de hacer cumplir la ley también enfrentan desafíos continuos cuando se trata de encontrar, arrestar, acusar y probar delitos cibernéticos.

De acuerdo con Arroyo, la piratería no cuenta necesariamente como un delito cibernético; ya que, no todos los piratas informáticos son ciberdelincuentes, esto, porque el ciberdelincuente se dedica a infiltrar los

[13] Rodrigo de Souza, "De las redes hacia el ciberespacio", *Revista Digital Universitaria*, n. 2 (2018), http://doi.org/10.22201/codeic.16076079e.2018.v19n1.a2.
[14] Moisés Barrio Andrés, "Ciberdelitos: Amenazas Criminales Del Ciberespacio".
[15] Pirata digital, según Magazine Caser, "…es aquel que vive al margen de la ley y apropiándose de lo que no es suyo. En una asociación de ideas, un pirata digital es aquel que descarga, copia, vende o reproduce productos utilizando Internet y sin contar con el permiso expreso de sus propietarios." y "La piratería en Internet, o piratería digital, supone acceder a contenidos digitales sin pagar a sus autores o propietarios, atentando contra la propiedad intelectual. Un acto que no solo perjudica a la industria, sino también a la economía del país e incluso al propio ciudadano que hace descargas digitales ilícitas, que puede poner sus datos personales en peligro o instalarse un virus en sus equipos."

sistemas informáticos con intenciones maliciosas, mientras que los piratas informáticos solo buscan formas nuevas e innovadoras de utilizar un sistema, ya sea para bien o para mal.[16]

Por otro lado, los ciberdelincuentes son personas que llevan a cabo ataques dirigidos, y que persiguen y comprometen activamente la infraestructura de una entidad objetivo. Por lo que es poco probable que los ciberdelincuentes se centren en una sola entidad, debido a que realizan operaciones a grandes masas poblaciones definidas solo por tipos de plataformas similares, comportamiento en línea o programas utilizados.

1.2.3. Ciberseguridad

Es la habilidad de proteger computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de embates maliciosos, reconociéndose como la seguridad de las ciencias aplicadas de la información electrónica. El término se emplea en una diversidad de argumentos, desde las transacciones hasta la sistematización móvil, y se puede fraccionar en algunas categorías frecuentes.[17]

Una de ellas, es la seguridad, la cual se dedica a proteger una red informática de intrusos,[18] ya sean atacantes dirigidos o malware. Por otro lado, las aplicaciones se aglutinan en conservar el software y conectores libres de inminencias;[19] generando, una seguridad exitosa en la etapa de diseño, mucho antes de que se efectúe un programa.

---

[16] Sergio Cámara Arroyo, "La cibercriminología y el perfil del ciberdelincuente", *Derecho y Cambio Social*, no. 60 (2020), https://dialnet.unirioja.es/servlet/articulo?codigo=7524987.

[17] Luis Joyanes Aguilar, "Ciberseguridad: la colaboración público-privada en la era de la Cuarta Revolución Industrial (Industria 4.0 Versus Ciberseguridad 4.0)", *Cuadernos de estrategia*, no. 185 (2017), https://dialnet.unirioja.es/servlet/articulo?codigo=6115620.

[18] Se entiende por intruso a los hackers, crackers, sniffers, phreakers, spammers, entre otros los cuales buscan atacar las redes informáticas. *Véase:* Álvaro Gómez Vieites en "Tipos de ataques e intrusos en las redes informáticas", https://carolinacols.files.wordpress.com/2011/11/ataquesinformaticos.pdf

[19] Según la Real Academia de la Lengua Española, se entiende por Inminencia "la cualidad de inminente, especialmente tratándose de un riesgo." *Véase:* Real Academia de la Lengua Española RAE, *"inminencia"* https://dle.rae.es/inminencia

No obstante, la seguridad de la información se encarga de proteger la rectitud y secreto de los datos, mientras la seguridad operativa contiene los métodos y arbitrajes para manipular y resguardar los datos activos, esto comprende, las autorizaciones que poseen los usuarios cuando acceden a una red y los ordenamientos establecen cómo y dónde se pueden acumular los datos que contiene dicho marco.

Sin embargo, la enseñanza del usuario resulta clave para abordar un componente de seguridad cibernética más predecible: las personas debido a que cualquiera puede alojar fortuitamente un virus en un procedimiento que de otro modo sería indudable si no se persiguen las buenas destrezas de seguridad.

1.2.4. Ciberderecho

Es la rama del derecho que surgió desde la aparición del internet, ciberespacio y sus respectivas cuestiones legales. El derecho cibernético cubre un área bastante amplia, que abarca varios subtemas que va desde la libertad de expresión, acceso a internet y privacidad en línea. [20] Genéricamente, la ley cibernética se conoce como la Ley de Internet.

[20] La libertad de expresión, el acceso a internet y privacidad en línea se enmarcan dentro de la propuesta doctrinaria de Moisés Barrio Andrés, aquí el principio de libertad de expresión cibernética el cual tiene como base el derecho humano de poder manifestar de forma libre las ideas contenidas en el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP). Principio y derecho que se debe incluir como parte del acceso libre y universal al ciberespacio de todos los usuarios y a la vez se enmarca dentro del derecho fundamental de acceso al Internet. "Artículo 19.- 1. Nadie podrá ser molestado a causa de sus opiniones. 2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. 3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para: a) Asegurar el respeto a los derechos o a la reputación de los demás; b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas." *Véase*: "Pacto Internacional de Derechos Civiles y Políticos". Oficina del Alto Comisionado de Derechos Humanos de Naciones Unidas.
https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

La primera ley cibernética en el mundo, tal como señala, Bernal,[21] fue la Ley de Abuso y Fraude Informático, promulgada en 1986, en Estados Unidos y es conocida como CFAA, esta ley se encarga de prohibir el acceso no autorizado a las computadoras e incluye detalles sobre los niveles de castigo por infringir la misma.[22] Ahora bien, en cuanto a El Salvador respecta, en el año 2006, se promulgó una Ley Especial Contra los Actos de Terrorismo, en el artículo 12 se abordan los Delitos informativos donde esta establecen penas de entre 10 a 15 años a todo aquel ciudadano que utiliza de manera inadecuadas las redes informáticas.

1.2.5. Ciberdelito

Se define como un delito en el que una computadora es el objeto o se utiliza como herramienta para cometerlo. El ciberdelito es cualquier tipo de actividad ilegal que se realice a través de medios digitales. Esto se debe a que el robo de datos es, uno de los tipos más comunes de delito cibernético, pero este incluye una amplia gama de actividades maliciosas, como el acoso cibernético o la instalación de virus.[23]

Sin embargo, esta conceptualización tiende a dividirse en dos categorías distintas: los que causan daños intencionales y los que causan daños no intencionales. En la mayoría de los casos, el daño es económico, pero no siempre; un ejemplo, es el ciberacoso, el cual es ilegal cuando constituye una amenaza para la seguridad física de una persona, implica coerción, muestra odio o prejuicio contra determinadas poblaciones protegidas. En ese caso, el daño no es económico, pero sigue siendo un delito. Los daños no intencionales pueden incluir, por ejemplo, que un empleado propague

[21] Álvaro Écija Bernal, "Ciberespacio, Ciberderecho Y Ciberabogados", *Noticias Jurídicas*, 8 de marzo de 2017, https://noticias.juridicas.com/conocimiento/articulos-doctrinales/11733-ciberespacio-ciberderecho-y-ciberabogados/.
[22] Ibid.
[23] Vicente Pons Gamón, "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad". *Revista Latinoamericana de Estudios de Seguridad*, n. 20 (2017), https://doi.org/10.17141/urvio.20.2017.2563.

un virus "inofensivo" que interrumpa el negocio de cualquier manera. Si bien es posible que no cause el mismo daño financiero inmediato que el robo de información privada o financiera, aún causa daños financieros colaterales, debido tanto a la pérdida de tiempo de los empleados como al dinero que la empresa tiene que gastar para solucionar el problema.[24]

1.2.6. Cibercrimen

Es un término general para muchos tipos diferentes de delitos que tienen lugar en línea o donde la tecnología es un medio y/o un objetivo para el ataque. Tal como indica Barrera,[25] es una de las actividades delictivas de más rápido crecimiento en todo el mundo y puede afectar tanto a personas como a empresas.

Los delitos cibernéticos pueden afectar a las personas de múltiples maneras y en la mayoría de los casos se tratan como delitos del mundo real y son procesados como tales. De acuerdo con las definiciones adoptadas, los ataques a sistemas informáticos para interrumpir la infraestructura de TIC (Tecnología de la Información Comunicación)[26] y robo de datos a través de una red utilizando malware, parten de los delitos ciberdependientes.[27] Este tipo de delito se transforma continuamente debido al crecimiento de Internet, lo que dificultad su persecución debido al

[24] Robert Moore. Cybercrime: investigating high-technology computer crime. (New York: Routledge, 2010).
[25] Silvia Barrera-Ibáñez. "Ciberpol. Metodología Para La Investigación Del Cibercrimen". Universidad La Rioja UNIR (2019). https://reunir.unir.net/bitstream/handle/123456789/10060/Barrera%20Ib%C3%A1%C3%B1ez%2C%20Silvia.pdf?sequence=1&isAllowed=y
[26] De manera general, puede entenderse que las TIC son las nuevas tecnologías de la información y comunicación que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; y que se relacionan de manera interactiva e interconexionadas, lo que permite conseguir nuevas realidades comunicativas. *Véase:* Consuelo Belloch. “Tecnologías de la Información y Comunicación en el aprendizaje”, Universidad de Valencia (s.f.) https://www.uv.es/bellochc/pedagogia/EVA1.pdf
[27] David Camacho. "Aidacyber: contribuciones en ciberseguridad y cibercrimen". Universidad Politécnica de Madrid, 8 de julio de 2020, http://aida.etsisi.upm.es/wp-content/uploads/2020/07/AIDA_Cyber_2020.pdf.

necesario formalismo que requiere el sistema jurídico para crear instrumentos eficaces para combatirlos.

Según Piccirillo, los delitos cibernéticos cuestan a las empresas e individuos miles de millones de dólares al año, debido en gran medida a la evolución y accesibilidad de la tecnología inteligente, que a la vez representa múltiples puntos de acceso dentro de los hogares para que los piratas informáticos los exploten. [28]

1.3 Información personal digital

El almacenamiento de información personal se está alejando gradualmente de un enfoque que estrictamente se ubica del lado del cliente utilizando aplicaciones de software hacia servicios de almacenamiento basados en la web ofrecidos por empresas privadas como Google y Flickr.[29] Estos dispositivos contienen acceso a la información personal lo cual a largo plazo ponen en peligro la capacidad de un individuo para conservar su propia información personal.

Google actualmente da a cada cuenta 15 GB de espacio de almacenamiento, compartido entre Gmail, Google Drive y Google Fotos. Flickr ha sido una red social de almacenamiento para el manejo y uso de fotografía en el mundo, pero en la actualidad este ha puesto trabajas para que los usuarios puedan descargar sus propias fotos lo que pone en peligro los datos de los usuarios alojados en la nube.[30]

---

[28] Dario Piccirilli, "Protocolos a aplicar en la Forensia Informática en el marco de las Nuevas Tecnologías (Pericia–Forensia y Cibercrimen)". (tesis doctoral, Universidad Nacional de La Plata, 2016), https://doi.org/10.35537/10915/52212.

[29] José Luis Gómez Barroso, "Uso y valor de la información personal: un escenario en evolución". *El profesional de la información (EPI)* no. 1 (2018), https://doi.org/10.3145/epi.2018.ene.01.

[30] Ramón Peco. “Por qué es peligroso guardar nuestros datos solo en la nube y qué alternativas hay”, La Vanguardia, 9 de noviembre de 2018, https://www.lavanguardia.com/tecnologia/20181109/452801751726/peligroso-guardar-datos-nube-que-alternativas-hay.html

La adquisición de información personal digital se convierte en un proceso de selección en el que hay que considerar dos elementos, primero el contenido en sí mismo que otorga el usuario, y luego el uso que le brindan las plataformas de almacenamiento a esta información. El primer elemento cuenta con el consentimiento del individuo, no así el segundo, y ello trastoca los márgenes del ordenamiento jurídico, o al menos la esfera jurídica del individuo, quien no otorga su consentimiento para la comercialización de sus datos.[31]

De acuerdo a Roca, al estudiar la información personal y sus diferentes aristas, se hace necesario atender dos conceptos estrechamente relacionados; por un lado, la privacidad, que hace referencia principalmente a la protección personal de la información en línea, y a la seguridad que está más relacionada con la propia conciencia de las acciones y el comportamiento en línea del usuario en el ciberespacio.[32] En esencia, este planteamiento hace alusión a la necesaria precaución que el usuario ha de tener al momento de brindar información en una compra, o tan solo por solicitar información sobre algún producto o servicio, pero además de acuerdo al planteamiento de Roca, la seguridad pasa por la valoración de la seguridad tecnológica con la que cuenta un determinado sitio, lo que significa que la protección de la información personal recae en primer lugar en el individuo.

Ambas conceptualizaciones, privacidad y seguridad, abarcan competencias sobre la gestión adecuada de la información personal compartida en línea o el manejo de la seguridad (por ejemplo, el uso de filtros de navegación, contraseñas, software antivirus y cortafuegos), desde el plano individual. Este planteamiento atribuye una responsabilidad

[31] Francisco R Cortes Martinez et al. "Después de presionar el botón enviar, se pierde el control sobre la información personal y la privacidad: un caso de estudio en México", *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação*, no. 21 (2017), https://dialnet.unirioja.es/servlet/articulo?codigo=6671446.

[32] Andoni POLO ROCA, "Sociedad de la información, sociedad digital, sociedad de control". *Inguruak*, no. 68 (2020), http://dx.doi.org/10.18543/inguruak-68-2020-art05.

inherente al individuo que por “voluntad propia” decide convertirse en un ciudadano digital, algo que implícitamente sugiere que el individuo es lo suficientemente consciente de los riesgos asumidos por sus actos, y esto parece poner en tela de duda la capacidad de ejercicio otorgada al sujeto por parte del ordenamiento jurídico, esto, dado que las responsabilidades implícitas o explícitamente asumidas por el ciudadano digital se materializan en individuos incapaces de obrar ante los ojos de la ley, y ello hace necesario y justifica la intervención del ordenamiento jurídico.

Sin embargo, el ordenamiento jurídico también enfrenta el hecho de que, en la concepción de la aldea global, el acceso a internet se considera un derecho, que fomenta otros derechos, como el derecho a la educación.[33] En este sentido, la protección de la información personal ha de concebirse en un contexto más amplio que el simple acto de restringir el acceso a internet, ya de por medio se encuentra la valoración del acto como un derecho humano.

Los ciudadanos digitales tienen derechos específicos con respecto a sus datos personales (por ejemplo, acceso, corrección, denegación, consentimiento, eliminación de la lista, borrado) y que pueden ejercer estos derechos, o hacer que se ejerzan en su nombre, y en ello juega un papel importante el rol del Estado para la protección del individuo en esferas no tradicionales.[34]

Martínez, indica que tratar con la protección de la información personal en línea implica comprender que la protección de la privacidad trata de la protección de la vida privada en un espacio público, en este caso el Internet. [35] Esto abre el estudio de diversos conceptos, a ratos poco precisos y de compleja configuración para el ordenamiento jurídico, como la protección

[33] Véase la nota 3.
[34] Teresa González Ramírez y Ángela López Gracia, "La Identidad Digital De Los Adolescentes: Usos Y Riesgos De Las Tecnologías De La Información Y La Comunicación", *RELATEC*, vol. 17 no. 2 (2018), https://doi.org/10.17398/1695-288X.17.2.73.
[35] Andrew Keen, Internet no es la respuesta.

de datos,[36] y la seguridad digital.[37] Ambos conceptos tienen alcance transfronterizo, e incluso implican la configuración de otras unidades de análisis aún más complejas, como, por ejemplo, la criminalización de las personas jurídicas, que además en internet adquiere mayor complejidad, dado que varias "partes" de una ciber empresa pueden ubicarse en contextos geográficos distintos al sujeto violentado en sus derechos, por lo que por la determinación del hecho delictivo[38] puede permitir fácilmente al delincuente escapar al alcance de la ley.[39]

1.4 Explosión de los crímenes cibernéticos

Los cibercrímenes son acciones con características particulares por lo que, en tales casos, corresponde considerar la acción como tal, el sujeto, el resultado y su imputación. Este tipo de acciones muestra que la teoría del delito necesita ser replanteada en algunos de sus aspectos, para así lograr explicar estos nuevos fenómenos jurídicos, mismos que ocurren en espacios no tradicionales en los que fácilmente se encuentran lagunas jurídicas que apuntan a la impunidad en algunos Estados con debilidad normativa sobre esta materia, y en la que cada vez más hay una intervención menos directa del ser humano.

Solamente en América Latina se considera que los crímenes cibernéticos se han incrementado entre un 30% y un 40% en los últimos años, y es esta

[36] La protección de datos, según las Naciones Unidas, es derecho fundamental que tiene como finalidad proteger la dignidad y el honor de una persona a través de "Habeas Data".
[37] La seguridad de datos, de acuerdo Nathalie Hernández a se refiere a medidas de protección de la privacidad digital que se aplican para evitar el acceso no autorizado a los datos, los cuales pueden encontrarse en ordenadores, bases de datos, sitios web, etc.
[38] Hecho delictivo, de acuerdo al Manual Único de Investigación de El Salvador, de forma práctica es la relación de los hechos que permiten establecer la existencia del delito y la participación del imputado en los hechos; y desde un enfoque jurídico constituye el encuadramiento jurídico de los hechos dentro las disposiciones legales tanto sustantivas como procedimentales.
[39] Cristian Borghello y Marcelo Gabriel Ignacio Temperini, "Suplantación de identidad digital como delito informático en Argentina" (Simposio, Sociedad Argentina de Informática SADIO, 27 al 31 de agosto de 2012), http://sedici.unlp.edu.ar/handle/10915/124395.

una de las zonas del mundo que mayor actividad ha registrado en este sentido, en gran medida por su debilidad jurídica e institucional.

Los últimos informes en la región sitúan a México, como el principal objetivo, de tal manera calculándose que en los últimos cuatro años 30.000 reportes telefónicos relacionados con delitos cibernéticos.

La compañía de ciberseguridad Kaspersky Lab identifico cerca de 400 millones de intentos de ataques de virus que tenían como objetivo países de América Latina, esto son datos de únicamente el año 2015. En cuanto a este tipo de ataques (por virus), Brasil se ubica en el principio de la lista de países que han sido atacados en la región, con 27,6 millones de intentos de infección, y es a la vez el número 18 en la escala mundial, seguido de México, Colombia, Perú, Venezuela, y Chile.[40]

Los expertos apuntan a que la región es continuamente foco de ataques en principio por la falta de reportes que acostumbra a realizar el usuario, el desarrollo económico e industrial y la falta de infraestructura para dar seguimiento al rastro delictivo en la red. El principal foco de interés son las empresas, teniendo como origen el uso de troyanos (software malicioso),[41] con énfasis en cuanto al robo de datos financieros, que representa el 30% de los ataques.

Las modalidades para lograr el robo de datos financieros varían, por ejemplo, en Colombia los ciberdelincuentes acostumbran el uso de correos electrónicos para simular una comunicación de la oficina de impuestos conocida como DIAN (Dirección de Impuestos y Aduanas Nacionales de

[40] Hernan Diazgranados. “Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021”, Kaperskey daily, 31 de agosto de 2021, https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/#:~:text=El%20Panorama%20de%20Amenazas%20en,el%20mismo%20periodo%20en%202020.

[41] Un caballo de Troya o troyano es un tipo de malware que a menudo se disfraza de software legítimo. Una vez activados, los troyanos permiten a los cibercriminales espiarte, robar tu información confidencial y obtener acceso de puerta trasera a tu sistema. Kaspersky LATAM, (s.f.) https://latam.kaspersky.com/resource-center/threats/trojans

Colombia), haciendo un señalamiento explícito de evasión fiscal, y así dirigirlos a la apertura de un documento anexo que contiene un virus.[42] Sin embargo, en el caso de México, la técnica del engaño varía sutilmente, enfocándose en el envío de correos falsos de una supuesta institución bancaria.

Recientemente, en el año 2019 investigadores de la firma de ciberseguridad Kaspersky Lab dicen que ASUS,[43] uno de los fabricantes de computadoras más grandes del mundo, "*delincuentes informáticos introdujeron un software malicioso en miles de computadoras de la marca ASUS, a través del servicio de actualización en línea y abrir una puerta trasera maliciosa,*"[44] esto sucedió el año pasado después de que los atacantes, comprometieran un servidor para la herramienta de actualización de software en vivo de la compañía. El archivo malicioso se firmó con certificados digitales legítimos de ASUS para que parezca una auténtica actualización de software de la empresa.

Los investigadores estiman que medio millón de máquinas con Windows recibieron la puerta trasera maliciosa a través del servidor de actualización de ASUS, aunque los atacantes parecen haber estado apuntando solo a unos 600 de esos sistemas. El malware buscó sistemas específicos a través de sus direcciones MAC únicas. Una vez en un sistema, si encontraba una de estas direcciones específicas, el malware se comunicaba con un servidor de comando y control que operaban los atacantes, que luego instalaba malware adicional en esas máquinas. Kaspersky Lab dijo que descubrió el ataque en enero después de agregar una nueva tecnología de detección de la cadena de suministro a su

[42] Patrick Bell, "Cyber Threat Report 04 April 2019", (2019).
[43] *ASUS* es uno de los tres fabricantes de PC portátiles de consumo líder a nivel global y creador de las motherboards más vendidas y premiadas mundialmente. Véase: https://www.asus.com/us/
[44]"Kaspersky Lab advirtió que un virus infectó a miles de ordenadores de ASUS", CiberSeguridad Latam, 2021, https://www.ciberseguridadlatam.com/2019/03/28/kaspersky-lab-advirtio-que-un-virus-infecto-a-miles-de-ordenadores-asus/

herramienta de escaneo para detectar fragmentos de código anómalos ocultos en código legítimo o código de captura que está secuestrando las operaciones normales de una máquina.

La compañía planea publicar un documento técnico completo y una presentación sobre el ataque de ASUS, al que ha denominado Shadow Hammer, el próximo mes de noviembre del 2021 en su Cumbre de Analistas de Seguridad en Singapur. Mientras tanto, Kaspersky ha publicado algunos de los detalles técnicos en su sitio web.

En el año 2019, un juez otorgó a Microsoft la orden judicial que les permitía interrumpir una red de sitios web operados por un grupo de piratas informáticos vinculados a Irán. Microsoft dijo que a partir de esta orden ha eliminado 99 sitios web pertenecientes a un grupo de piratería vinculado al Estado iraní al que llama "Phosphorus", también conocido como APT35.

Según documentos judiciales, Microsoft recibió una orden judicial que les permitía tomar el control de los sitios web que el grupo de piratería había utilizado para ejecutar ataques de phishing con advertencias de seguridad falsas de Microsoft.

Microsoft había estado rastreando Phosphorus desde el año 2013 y había visto al grupo lanzar ataques en todo el mundo, aunque su actividad más reciente parecía apuntar a empresas y agencias gubernamentales.

El grupo de piratas informáticos iraní en diciembre pasado fue descubierto por investigadores de Cerfta, organización de ciberseguridad con base en London, al intentar piratear cuentas de correo electrónico de miembros del Tesoro de EE. UU, científicos atómicos árabes, figuras de la sociedad civil iraní, y ejecutores del acuerdo nuclear entre Estados Unidos e Irán. Sobre esta misma línea la organización sin fines de lucros que busca Hacer del internet un lugar seguro reduciendo el ciber riesgo, Global Cyber Alliance dice que el uso del poder legal por parte de Microsoft para alterar al grupo es el mejor de los casos.

Representantes de la empresa SiteLock, compañía seguridad y monitoreo de sitios web, asegura que la operación de Phosphorus presenta una advertencia para otras empresas, porque esta es la segunda vez que Microsoft tiene un enfrentamiento con los ciberdelincuentes estatales y demuestra que incluso una de las empresas de tecnología más grandes y sofisticadas del mundo no puede prevenir este tipo de ataques.

Desde 2013, informes de ciberseguridad han identificado operaciones de un grupo que hasta esa fecha ya había robado más de 1.200 millones de dólares. Eso incluye la venta de 15 millones de registros de tarjetas de crédito y débito robados de al menos 100 empresas en 47 Estados de los Estados Unidos, así como de Australia, Francia y el Reino Unido. Entre las empresas afectadas por el grupo FIN7 se encuentran Chipotle Mexican Grill, Arby's y Saks Fifth Avenue de Hudson's Bay Brands.

Se trata del grupo de delitos cibernéticos FIN7, que tiene como sus principales objetivos las cuentas financieras de las cadenas hoteleras, restaurantes y firmas financieras. El grupo, también conocido como Cobalt Group y Carbanak Group, estaba formado por decenas de miembros, y tuvo un gran éxito robando datos de más de 6.500 terminales de puntos de venta individuales en al menos 3.600 ubicaciones comerciales separadas, según el Departamento de Justicia.[45]

El Departamento de Justicia de EE. UU en el año 2019 describió la modalidad ransomware como un nuevo modelo comercial para el delito cibernético. Se trata de un malware que infecta computadoras y restringe su acceso a archivos, a menudo lo hace de forma permanente, a menos que se pague un rescate. Esta modalidad es actualmente el delito cibernético de más rápido crecimiento, de manera que aproximadamente cada 40 segundos, una empresa es víctima de un ataque de ransomware.

[45] Virendra Soni. "Multifunctional malware becoming extensive in 2018, finds Kaspersky Lab Report". Daily Host News, 4 de septiembre de 2018, https://www.dailyhostnews.com/multifunctional-malware-becoming-extensive.

Mientras que la empresa Cybersecurity Ventures estimó que la frecuencia se elevaría a cada 14 segundos para 2019.

De acuerdo a datos provistos por el FBI, la cantidad total de pagos de rescate se acerca a los mil millones de dólares anuales, y se prevé que los costos globales de daños por ransomware se incrementen más de 15 veces. El ransomware cambia las reglas del juego en el mundo del ciberdelito porque permite la universalidad de la singularidad, permitiendo a los delincuentes automatizar completamente sus ataques.

El gran volumen de ciberataques y eventos de seguridad evaluado diariamente por los centros de operaciones de seguridad continúa en incremento, por lo que es casi imposible para los humanos mantener el ritmo.

La seguridad es un problema manifiesto en personas, se están cometiendo crímenes cibernéticos. Y aunque evidentemente se hace uso de computadoras, se hace necesario de personas calificadas para perseguir y atrapar a los perpetradores.

La tecnología es un elemento fundamental, pero sin un suficiente ejército de agentes White hat[46] (hackers del lado de la ley), para enfrentarse el creciente ejército de black hat[47] (sombreros negros), la reducción de la tasa de delito informático será difícil de conseguir.

[46] White hat: Hacking ético, para Sandra Castro de la Universidad Piloto de Colombia, "consiste en una auditoría, que es realizada por profesionales del área de seguridad de la información, estas personas utilizan sus habilidades y conocimientos, para identificar las brechas de seguridad en una entidad y son llamados como pentester. La actividad que ellos realizan se conoce con el nombre de hacking ético o pruebas de penetración". Véase: Sandra Milena Castro Cubillos, White Hat: Hacking Ético, (s.f.) https://core.ac.uk/download/pdf/226165937.pdf

[47] Black hat: se refiere a un pirata informático que irrumpe en un sistema informático o una red con intenciones maliciosas. Un hacker de sombrero negro puede aprovechar las vulnerabilidades de seguridad para obtener beneficios económicos; robar o destruir datos privados; o para alterar, interrumpir o cerrar sitios web y redes. El hacker de sombrero negro también puede vender estas hazañas a otras organizaciones criminales. *Véase: Katie Terrell Hanna y Taina Teravainen.* "Black hat hacker", noviembre de 2021, https://searchsecurity.techtarget.com/definition/black-hat

La mayor amenaza virtual actual es la seguridad de la información, para lo cual existe una escasez de mano de obra calificada en ciberseguridad, lo que aumentará la demanda de profesionales en este campo, según lo han afirmado algunos expertos de la industria citados por el centro de investigación de Palo Alto.

1.5 Agenda de ciberseguridad de los Estados

La ciberseguridad no debe limitarse únicamente al contexto de la tecnología de la información, esto implica una mayor comprensión de los desafíos e impactos impuestos por el ciberespacio como plataforma donde la relación entre Estados y ciudadanos se presenta cada vez más de forma fluida.

Una política de ciberseguridad es un instrumento desarrollado por Estados para comunicar y expresar aquellos aspectos que un Estado quiere proteger en el ciberespacio. Se trata de una declaración que encarna la postura de un gobierno para regular ciertas conductas de sus ciudadanos, sus derechos y deberes; a partir del reconocimiento de una realidad generalizada en la sociedad, en el que la información digital, el desplazamiento y las redes sociales son la norma de su funcionamiento.

En este contexto, las variables económicas relacionadas con los movimientos de capital e inversión se ven afectados, ya que los bancos son más flexibles y promueven dicha interacción con servicios electrónicos cada vez más personalizados, fomentando el flujo en línea de activos financieros diversos. Estas condiciones requieren protección permanente, y prácticas seguras en la relación entre los clientes y el banco.

Por otro lado, existen implicaciones psicológicas importantes a considerar en estas nuevas interacciones de los ciudadanos en el ciberespacio; en el que las motivaciones, orientaciones y acciones se presentan de acuerdo con las tendencias y patrones que se definen por realidades emergentes basadas en las relaciones informáticas, cuestión que puede inducir

comportamientos positivos, negativos o neutrales que manifiestan una conciencia supranacional inmerso en el tejido social.

La conciencia supranacional se evidencia dado que esta nueva realidad de interacción virtual y real moviliza comunidades y relaciones fuera del dominio y límites de un país, los comportamientos y expresiones sociales exigen un orden completamente diferente al tradicional. En este sentido, las ciencias jurídicas encuentran un nuevo desafío de regulación, en un escenario que es incierto e impredecible, para intentar conceptualizar y proponer soluciones frente a las situaciones categorizadas como conductas reprobables, que, articulados con la tecnología de la información, se vuelven más volátil frente a posibles formas de castigo y control.

Esta realidad del ciberespacio requiere una renovada comprensión de las relaciones entre personas y Estados. Por los antecedentes dentro del ciberespacio, la ciberseguridad atendida en una política estatal formaliza la declaración que un Estado realiza al delimitar el territorio digital en que pretende tener cobertura jurídica, y donde igualmente ejercerá soberanía, sabiendo que el espacio virtual se comparte con otros Estados y es por ello necesario operar en base al principio de sinergia, principio de la teoría general de Teoría General de Sistemas que describe cómo la cooperación de dos causas distintas contribuya a generar el mismo resultado.[48]

La ciberseguridad es una temática sin duda critica para la prosperidad y seguridad en general. Las actividades maliciosas en el ámbito cibernético significan una seria amenaza a la economía y el funcionamiento de las

[48] Sinergia se define como la acción de dos o más causas que generan un efecto superior al que se conseguiría con la suma de ambos en forma individual. ala sinergia se le considera como como la integración de partes o sistemas que conforman un nuevo elemento u objeto. dos elementos que se unen y forman una sinergia ofrecen un resultado que amplía las cualidades de cada uno y se destacan en varios campos laborales como el marketing y la economía ya que suelen mostrar y resaltar las cualidades del trabajo en equipo para realizar o conseguir un mismo objetivo. Véase: Ingeniería de Sistemas, “2.1.4 Sinergia”, (s.f.)
https://sites.google.com/site/ingenieriadesistemasegfl/2-propiedades-y-caracteristicas-de-los-sistemas/2-1-propiedades-de-los-sistemas/2-1-4-sinergia

débiles democracias en la región, así como las libertades y valores conexos.

En la Cumbre Mundial sobre la Sociedad de la Información, los líderes gubernamentales reconocieron la realidad y riesgos significativos planteados por la ciberdelincuencia, y así surge en el año 2007, la agenda de Ciberseguridad como marco de cooperación internacional orientada a proponer estrategias de soluciones para mejorar la confianza y la seguridad en la sociedad de la información.

Esta agenda se basa en cinco aspectos claves: Medidas legales, medidas técnicas y de procedimiento (centradas en acciones claves para abordar las vulnerabilidades de software), estructuras organizativas (para la prevención, detección, respuesta y gestión de crisis de ciberataques), desarrollo de capacidades (estrategias para crear conciencia, transferir conocimientos e impulsar la ciberseguridad en la agenda política nacional), y finalmente, cooperación internacional (desarrollar una estrategia de cooperación, diálogo y coordinación internacional en el tratamiento de ciberamenazas).[49]

1.6 Gobernanza del internet y del ciberespacio

La gobernanza de Internet se concibe a menudo como una cuestión de diseño o fortalecimiento de marcos institucionales dentro de los cuales se facilitarán diversas actividades. La necesaria comprensión de internet implica que, comprender cómo se manifiestan las acciones de los usuarios de Internet, para lo que es necesario estudiar más allá del texto de las normas jurídicas, se trata de saber sobre lo hacen los usuarios a diario.

[49] "La Agenda sobre Ciberseguridad Global", Unión Internacional de Telecomunicaciones (UIT), 2007, https://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18#:~:text=La%20Agenda%20sobre%20Ciberseguridad%20Global%20%28GCA%29%20de%20la,la%20confianza%20en%20la%20sociedad%20de%20la%20informaci%C3%B3n

Al referirse a la gobernanza, es necesario tener en cuenta que en diversas publicaciones académicas y políticas existen diversos usos sobre este término. Sin embargo, gran parte de lo que muchos autores quieren decir proviene del trabajo de Wiener 1948 y Deutsch 1963. A partir de ahí la gobernanza como concepto hace referencia a determinadas acciones, que a la vez implican el uso de recursos para conseguir un objetivo, el que básicamente es lograr que alguien haga o no algo.

La gobernanza de las relaciones internacionales, también referida como “gobernanza global” implica una relación entre varios actores que siguen el enfoque de influir en las acciones de los demás, de lo contrario no tendría sentido hacer referencia a la gobernanza. Estas acciones pueden ser realizadas por personas físicas o colectivos y la determinación de estos agentes es de mucha importancia porque su reacción ante las acciones de gobernanza está en dependencia del peso que estos tengan en el escenario internacional, es decir, su actuación dependerá de que tan permeables sean a la influencia de otro actor y del equilibrio de poder entre ellos.

La gobernanza de internet, un fenómeno relativamente reciente, y en gran medida se debe a su concepción como herramienta global, incluso a la consideración que el acceso a esta ha tenido como derecho humano. Por lo tanto, la gobernanza del internet debe considerar la premisa de que como herramienta global no puede y no debe ser controlado ni regulado por una sola entidad o gobierno. De no ser así, internet dejaría de considerarse un espacio pluralista y democrático de discusión en el que múltiples actores tanto a nivel nacional como internacional se reúnen a fin de exponer diversos criterios de interés de alcance nacional o global.

Antes de los años 80, a los Estados se les atribuía exclusivamente la responsabilidad del desarrollo social y económico de sus ciudadanos. Sin embargo, con la entrada de la tecnología y los procesos de globalización, la sociedad civil ha asumido un rol más beligerante en las decisiones que

toma el Estado, interviniendo de manera más directa en los asuntos relacionados a la libertad y la reivindicación de los derechos ciudadanos.

Considerando lo anterior, la gobernanza requiere de un equilibrio entre el Estado y la sociedad civil como agente de importante interacción en la economía, la política, y aspectos sociales como los derechos humanos relacionados a asuntos ambientales y tecnológicos.

La gobernanza propende por un equilibrio entre el Estado y la sociedad civil en su interacción en la economía y la política, y en aspectos sociales como los derechos humanos asociados a asuntos ambientales y tecnológicos. La idea principal es, ante las falencias de la actividad gubernativa, ampliar la capacidad del Estado con enfoques que vengan de la ciudadanía, y particularmente de actores sociales que son quienes viven y conocen las problemáticas sociales para que este llegue a ser legítimo, competente y eficaz.[50]

Una gobernanza logra sus fines en la medida en las instituciones y los procesos dentro de estas tienen transparencia, y además promueven la participación, el pluralismo y la equidad. El internet, como red, genera un importante intercambio de información entre las personas, y ello hace necesario que se administre y proteja, sobre todo considerando una importante pluralidad de agentes que intervienen en la red, por lo que vale destacar que la gobernanza ha sido el medio para desarrollar reglas entre los gobiernos, el sector privado y la sociedad, a fin de regular su uso y evolución teniendo la vista su importancia para el desarrollo de la sociedad y de los derechos que esta exige, como el acceso a la información, la educación y la libre opinión.

En este sentido, la gobernanza en internet persigue desarrollar la participación colectiva de las personas en los procesos de comunicación y

[50] Marcela Palacio Puerta y Karen Isabel Cabrera Peña, "La gobernanza de internet como plataforma para impulsar políticas en la educación con TIC. El caso de Colombia", *Revista Opera*, no. 21 (2017), https://doi.org/10.18601/16578651.n21.02.

acceso a la información, cumpliendo con ello su aporte formativo y cultural. Sin embargo, su misma importancia como medio de divulgación del conocimiento y acceso a la información obliga a su gestión descentralizada.

De otra manera, podría provocarse la limitación a los derechos antes comentados, pues su carácter descentralizado no solamente evita la apropiación del medio por una institución específica, sino que además permite que los contenidos y la información que se transmite pueda ser recibida y enviada –de forma interactiva– por cualquier persona en cualquier lugar del mundo.

Es en este punto donde puede manifestarse la complejidad de gestionar jurídicamente las relaciones derivadas del internet, los ciudadanos y el gobierno, ya que su descentralización obliga a considerar consecuencias transfronterizas del fenómeno, y al reconocimiento de instituciones e instrumentos de carácter supra nacional, provocan así un interesante análisis jurídico, mismo que trastoca el ordenamiento jurídico en distintas escalas.

Ahora bien, aunque el internet ha permitido posicionar al conocimiento y la cultura como un recurso esencial por encima de los factores tradicionales de producción, también es un espacio disponible para realizar una diversidad de transacciones e intercambios que, si bien expresan una faceta de la nueva economía mundial, implican una serie de relaciones que escapan a la protección estatal.

En este sentido, la gobernanza es vital para permitir la conectividad de los ciudadanos evitando la fragmentación de internet y salvaguardando los derechos de los usuarios, definiendo las responsabilidades de los diferentes actores que intervienen en la red, procurando principalmente la protección de la información individual que el usuario cede en la red, y sancionando el mal uso de esta sin lesionar la privacidad de las personas.

Acentuando el carácter descentralizado de internet, es importante resaltar que las decisiones administrativas o jurídicas que valoran la gestión de la red y la protección de los usuarios se encuentran en constante evolución e implican a sectores muy diversos en la esfera pública o privada, además de la presencia de variadas problemáticas.

En consecuencia, la gobernanza tiene el reto de promover políticas públicas y leyes que posibiliten a las poblaciones expresarse libremente en línea, acceder a cualquier tipo de restricción social o político, pero a la vez generar medidas de protección para que garanticen la privacidad del ciudadano, por lo que la gobernanza puede llegar a ser un medio en el que las partes interesadas participan activamente.

A través de un corresponsal especial, Economic and Political Weekly (2005) identifica las siguientes corporaciones como las responsables de la "gobernanza" en internet: Internet Corporation for Assigned Names and Number (ICANN), que tiene un manejo centralizado de los Domain Name System (DNS). Adicionalmente, juegan un importante papel las empresas que manejan los servidores raíz y los llamados dominios tops .com y .net, como Microsoft y Google las cuales han sido acusadas de tener ventajas comerciales desleales bajo el temor de que puedan ser usadas por el gobierno norteamericano con fines estratégicos.[51]

Conclusión capitular

Por el desarrollo del Internet y como consecuencia de esto el crecimiento del riesgo a que las personas, instituciones públicas y privadas, así como países en cuanto a la información digital personal e institucional, es un tema que va más allá de la responsabilidad individual. Actualmente es necesario un ordenamiento jurídico para la protección de datos y seguridad digital de carácter transfronterizo, ya que la globalización ha logrado el desarrollo de la tecnología y las infraestructuras digitales, esto ha ayudado a que exista

[51] Economic & Political weekly, n.10 (2005). https://www.epw.in/journal/2005/10

comunicación y mayor acceso al ciberespacio, creciendo de forma exponencial el riesgo para los países y personas por medio de la ciberdelincuencia, es por lo anterior que las leyes relacionadas con el delito cibernético continúan evolucionando en varios países del mundo, es por eso que se debe trabajar en materia de cooperación internacional desde una perspectiva del multilateralismo, ya que los organismos internacionales de forma continua enfrentan desafíos cuando se trata de encontrar arrestar acusar y probar delitos cibernéticos. Por eso la evolución del derecho internacional en materia de ciberespacio debe seguir su curso de manera acelerada en relación con la protección de los datos personales digitales.

CAPÍTULO II: MARCO JURÍDICO E INSTITUCIONAL SALVADOREÑO EN TORNO A LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL DIGITAL, DENTRO DEL CONTEXTO DEL INTERNET, GLOBALIZACIÓN, CIBERESPACIO

Introducción capitular

El objetivo de este capítulo busca “examinar el marco jurídico e institucional en materia de protección de la información personal digital en El Salvador”. En ese sentido en este apartado se establece el desarrollo de la normativa en relación a la protección de la información personal digital desde la LEDIC, Ley de delitos informáticos y conexos, bajo el entorno de crecimiento del internet y el surgimiento de diferentes acciones que podrían lesionar la dignidad de las personas y otros bienes jurídicos. La LEDIC se presenta como propuesta del marco jurídico en respuesta a sucesos en 2002 en relación a la vulneración de un sitio web estatal y el alto porcentaje de casos, 70%, en la Fiscalía General de la Republica de tipo penal y su bajo porcentaje de materialización en una acción penal. Se presenta una perspectiva de estudio de la LEDIC en cuanto a su alcance y limitaciones o áreas de oportunidad a mejorar, así como una perspectiva de relación interinstitucional la cual debe fortalecerse para mayor alcance. También, en el capítulo se estudia parte del alcance que presenta la legislación del país con relación a los delitos informáticos y conexos, enfocándonos en aquellos que son más conocidos y que debido a su impacto social forman parte de la motivación jurídica para la regulación del ciberdelito en el país.

En el apartado correspondiente a estos alcances, puede observarse la interrelación entre los diferentes instrumentos jurídicos que intentan proteger a los mismos sujetos desde perspectivas distintas. Además, se

plantea la naturaleza del ciberdelito de tipo privado y sus implicaciones y el marco jurídico de rango constitucional y su realidad y perspectiva en cuanto a los tratados internacionales. Otro aspecto que se desarrolla es el del modelo de gobernanza, ya que la complejidad en la determinación del bien jurídico atiende a la supranacionalidad que tiene el internet como espacio que atraviesa fronteras y su alcance en otros ordenamientos jurídicos dentro de las actividades derivadas de este medio de alcance mundial, se busca discutir las diferentes formas en que la gobernanza digital se presenta, específicamente con respecto a Internet.

2.1 Normativa para la protección de información personal digital en El Salvador

A pesar del crecimiento del acceso a internet de parte de la población salvadoreña , y por ende el surgimiento de diferentes acciones que podrían lesionar la dignidad de las personas y otros bienes jurídicos protegidos, fue hasta el año 2016 que en el país la comisión de seguridad pública de la Asamblea Legislativa, acordó proponer un marco normativo para combatir comportamientos delictivos valiéndose del internet y otros dispositivos electrónicos, lo que finalmente se configuró como la ciberdelincuencia.

Parte de la motivación de esta iniciativa fue el ataque cibernético que en el año 2002 se presentó en contra del órgano legislativo, mostrando la vulnerabilidad de su página web, aunque, como se desarrolla en párrafos anteriores, ya existían conductas lesivas a la dignidad de las personas y bienes jurídicos inmateriales valiéndose de las redes sociales. Estos esfuerzos en materia de combate al ciberdelito por parte de El Salvador no son aislados, sino que se enmarcan dentro de un contexto regional, lo que tiene gran sentido por el carácter transfronterizo de esta actividad.

Frente a este panorama la situación en El Salvador exhibe un escenario propio en el que el ciberdelito no es una causa frecuente en el actuar de los tribunales, a pesar de que las estadísticas de la Fiscalía General de la

República, FGR, apuntan a que entre el año 2016 a febrero del 2018 se habían registrado un total de 568 casos, de los que el 70% de los mismos se tramitaron como tipos penales calificados como: revelación de datos o información, hurto de identidad, utilización de datos personales, acoso a través de TIC y comportamientos relativos a la pornografía [52]. Estos tipos penales se enmarcan dentro de los delitos relacionados con la intimidad individual. Sin embargo, no hay estadísticas relacionadas a filtraciones sin consentimiento a sistemas informáticos, esto, a pesar de que la compañía de seguridad ESET para el año 2015 informó que en El Salvador un 34% de las empresas encuestadas habían sido objeto de ataques por medio de malware.

Pueden existir diversas razones que no permiten evidenciar los delitos vinculados a los accesos no autorizados, y parte de las razones es que las propias empresas perjudicadas no revelan esta información por no hacer notar su vulnerabilidad ante sus clientes, lo que disminuiría significativamente su confianza, e incluso podría generarles cierta responsabilidad jurídica, a esto se le suma la falta de confianza en el actuar policial sobre este tipo de delitos de naturaleza informática.[53]

De acuerdo con Ayala, solamente un aproximado del 10% de las denuncias vinculadas a ciberdelito se materializaran en una acción penal, presentándose requerimiento, y de estos, según el autor apenas la mitad va a llegar a la etapa de presentación de Dictamen de Acusación, con unas escasas posibilidades de lograr una condena, en gran medida por que la delincuencia informática presenta sus propias dificultades probatorias y de

[52] Oswaldo Feusier, “Aplicación y contenido de la Ley Especial contra la Delincuencia Informática y Conexos”. Consejo Nacional de la Judicatura El Salvador (2020), https://www.academia.edu/41596209/APLICACI%C3%93N_Y_CONTENIDO_DE_LA_LEY_ESPECIAL_CONTRA_LA_DELINCUENCIA_INFORM%C3%81TICA_Y_CONEXOS_CONCURSO_DE_INVESTIGACI%C3%93N_CNJ_Fomentando_la_investigaci%C3%B3n_para_mejorar_la_Administraci%C3%B3n_de_Justicia_

[53] “Estudio comprensivo de cibercrimen”. Oficina de Naciones Unidas contra la Droga y el Delito UNODC (2013), https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf.

cooperación que no se requieren necesariamente en la mayoría de delitos comunes como por ejemplo, la transnacionalidad, horizontalidad y peritaje de redes sociales, lo que impide y atrasa los requerimientos del fiscal.[54]

Por último, es oportuno considerar que se trata de comportamientos delictivos que apenas empiezan a incorporarse en las estadísticas del sistema penal salvadoreño, esto, a partir del 2016 con la Ley Especial de Delitos Informáticos y Conexos (LEDIC), que, a pesar de sus muchas tipificaciones, aun logra muy poco impacto, al menos en cuanto a condenas se refiere.

En este instrumento jurídico a como antes se ha comentado la definición de delito informático se caracteriza por su amplitud y por la necesidad de que exista un dispositivo de por medio que permite el acto delictivo, que a la vez se vale de la tecnología de la información, lo que puede involucrar diversos bienes jurídicos de forma directa o indirecta con la finalidad de obtener, manipular cierta información.

De tal manera que, en la LEDIC, el bien tutelado suele considerarse como la integridad, confidencialidad y manejo de los datos en los sistemas informáticos, lo que genera sus propias dificultades justificando así el tratamiento de estos delitos en un cuerpo legal especial y aislado, con alcance en lo punitivo, no así en lo investigativo y preventivo, etapas que se desecharon en el proceso de consulta por la ambigüedad práctica que requerían.[55]

Si bien a nivel internacional se presentan muchos criterios de clasificación de los delitos informáticos, el criterio utilizado en la LEDIC puede considerarse ambiguo en muchos casos. Es una clasificación cargada de imprecisiones y ambigüedades, lo que podría estar afectando sus propios

[54] Marcela Palacio Puerta y Karen Isabel Cabrera Peña, "La gobernanza de internet como plataforma para impulsar políticas en la educación con TIC. El caso de Colombia".
[55] César Eduardo Vásquez Mata, José Mauricio Regalado González, y Ricardo Salvador Guadrón Gutiérrez, "Cibercrimen E Informática Forense: Introducción y Análisis en El Salvador", *Revista Tecnológica*, *no. 10* (2017). http://hdl.handle.net/10972/3029

resultados, que continúan siendo bajos a pesar de las variadas tipificaciones que presenta la ley.

Los principales problemas que actualmente enfrenta la LEDIC para los especialistas en la materia resultan ser de carácter procedimental, en lo que respecta a la ejecución y cumplimiento de la investigación delictiva. A lo que se le suma el anonimato propio de este tipo de delitos, y la compleja carga de la prueba por la presencia de múltiples operadores privados, que a la vez buscan preservar su imagen de custodios de datos informáticos, lo que bloquea las órdenes judiciales de entrega de datos informáticos, lo que resta operatividad a este instrumento jurídico.

Por lo tanto, la cooperación entre las autoridades y las instituciones privadas que son las predominantemente afectadas es básicamente nula, y con reducidas perspectivas de mejora, igual ocurre con respecto al ejercicio de la cooperación internacional para la persecución de un delito, lo que hasta el momento no ha sido necesario requerir.

Sin embargo, es importante analizar otras dimensiones de los delitos apoyados por medio cibernéticos, en los que sí se hace necesaria y evidente la relación entra instituciones estatales, lo que predominantemente ocurre con respecta los delitos que afectan a las niñez, y que requieren la atención por ejemplo, del Consejo Nacional de la Niñez y de la Adolescencia -CONNA- que es la máxima autoridad de lo que se conoce como el Sistema Nacional de Protección Integral de la Niñez y de la Adolescencia, cuyas funciones se concentran en la defensa efectiva de los derechos de las niñas, niños y adolescentes (Art.134 y 135 ambos de la Ley de Protección Integral de la Niñez y Adolescencia) Muchos de los delitos en contra de la niñez en El Salvador se expresan bajo la figura bajo la figura del ciberbullying caracterizado como un tipo de violencia por medio de un dispositivo móvil, medio por el cual se desarrollan una persecución

física y psicológica con repetidos ataques a la víctima.[56] Esta práctica también puede desarrollarse por medio de mensajes de texto redes sociales, chat entre otros medios, lo que muestra un claro vínculo entre un delito típico y lo que se considera como ciberdelito.

La Constitución de la República, enfatiza en su artículo 34, que: “Todo menor tiene derecho a vivir en condiciones familiares y ambientales que le permitan su desarrollo integral, para lo cual, tendrá la protección del Estado”.

La Ley de Protección Integral de la Niñez y Adolescencia LEPINA de forma particular, coadyuva al cumplimiento de este artículo para garantizar el ejercicio y disfrute pleno de los derechos y deberes de toda niña, niño y adolescente en El Salvador (art. 1). Pero esta normativa no puede dar protección complete a los sujetos protegidos, por lo que se apoya en la Ley Especial en contra de los Delitos Informática y Conexos, que castiga el ciberacoso en los artículos 27 y 32.

El artículo 32 está especialmente pensado para la niñez, y el mismo se considera como perjuicio cualquier acción que afecte la personalidad y amenace la estabilidad psicológica de niños, niñas y adolescentes. Considerando como agravante el abuso sexual.

El artículo 27, se enfoca en los adultos principalmente en lo relacionado con lo sexual. También existen otras formas de castigar el ciberacoso, cuando este se refiere a la utilización de datos personales y a la divulgación indebida de estos, lo que se concibe en los artículos 24 y 26.

Es en la dimensión de protección a la niñez y adolescencia ante situaciones de ciberbullying en donde mejor se expresa la relación inter institucional en El Salvador, aunque vale apuntar que debido a la misma protección de la información que el Estado debe garantizar con respecto a los menores de

[56] Carlos de la Cuba, "La interpretación de la norma jurídica", *Derecho y Cambio Social*, no. 2 (2004), https://dialnet.unirioja.es/servlet/articulo?codigo=5512186.

edad, este tipo de casos son escasamente divulgados, por lo que tampoco se hace fácil darle un seguimiento a la acción resultante.

A manera de conclusión en este apartado, es importante subrayar que la propia naturaleza del ciberdelito –en el que el bien lesionado es predominantemente de tipo privado- dificulta su conocimiento por parte de las entidades correspondientes. Al tratarse de empresas afectadas, es lógico pensar que estas resguardarán todo lo relacionado al ciberataque del que han sido víctimas, lo que responde a una lógica económica de protección sobre sus acciones, y al aseguramiento de la confianza ganada a través de muchos años ante sus clientes. Esta situación no distingue entre empresa nacional o extranjera, porque la filosofía proteccionista de sus activos no distingue tal condición geográfica.

Si bien la ciberdelincuencia tiene efectos negativos en diferentes dimensiones de la vida socio económica y política, la acción para la persecución del hecho delictivo requiere en gran medida que el afectado se arriesgue a la exposición de su información privada, lo que, en caso de menores de edad afectados, requiere la decisión de los padres de iniciar una acción penal que también puede exponer información privada de sus hijos o hijas.

En El Salvador, el marco jurídico existente, bien sean normas jurídicas de rango constitucional, tratados internacionales suscritos o reglamentarias y aprobados por el órgano legislativo presentan importantes garantías y adecuación a los estándares internacionales que se han definido en materia de derechos humanos y su aplicabilidad en situaciones de intervención en contextos de vigilancia por medio de las telecomunicaciones. Sin embargo, la débil institucionalidad pone en tela de duda la efectividad de la norma jurídica que brinde protección a la información personal, esto, independientemente del matiz que tome la concepción del término “información personal”.

Por otra parte, la discusión sobre las nuevas tecnologías de la información y la comunicación es aún incipiente, y desde luego es materia de interés predominante en el sector empresarial, que naturalmente lo concibe como una actividad prioritaria, cuestión que no ocurre desde la óptica pública. A pesar de la aprobación y entrada en vigor de la Ley de Intervención a las Comunicaciones, queda pendiente debatir sobre la protección a la información personal utilizada por el sector público y sector privado.

El entorno socio político caracterizado tradicionalmente por difundir una cultura de secretismo y arbitrariedad bastante arraigada en la gestión institucional no fomenta la discusión con respecto a la materia que interesa en el presente estudio, la atención a este asunto implica el fortalecimiento mismo de la democracia, la que a vez se ve fracturada desde el momento en que al individuo se le violenta su derecho a la privacidad de sus datos, a la protección de su información personal que ha consentido compartir con un propósito definido claramente, y no más allá de este, y a partir de este momento cualquier otro uso ha de requerir la autorización del individuo propietario único de la información individual, situación que no está sucediendo en el plano practico.

En El Salvador, al igual que en otros países la expansión de internet también ha llevado al desarrollo de nuevos modos de operación delictivo que implican pornografía, amenazas, estafas, robo de identidades y violaciones a la honra y dignidad de la persona. Las víctimas de esto delitos no distinguen edades ni estrato social.

En la legislación penal de El Salvador vigente desde el año 1998, de forma indirecta ya se hacía referencia al del delito por medio de medios tecnológicos que facilitan la información y la comunicación. Algunos términos como “a través de medios electrónicos”, encontrados en los artículos 172 y 346 del Código Penal, marcaban la pauta para la incorporación del ciberdelito en una expresión más específica.

Por lo tanto, puede afirmarse que ya en esta época la regulación de los actos delictivos basados en medios informáticos se presentaba de forma desconectada con el resto de normas jurídicas que forman parte del sistema jurídico nacional, lo que se conoce comúnmente como regulación asistemática.[57]

Por la casi inexistente regulación sistémica de los delitos informáticos que atentan contra la integridad de los datos informáticos y otros bienes jurídicos relacionados a los activos digitales, es que por medio del Decreto Legislativo No. 260 de fecha 26 de febrero de 2016, publicado en el Diario Oficial No. 40, Tomo No. 410, de fecha 26 de febrero de 2016, se aprobó la Ley Especial contra Delitos Informáticos y Conexos (en adelante LEDIC). Esta normativa entró en vigencia apenas 8 días después de su publicación en el Diario Oficial, provocando la necesidad de actualizar algunos elementos necesarios para la administración de la justicia penal.

Sin embargo, esta necesaria actualización pasa por la compleja identificación del bien jurídico protegido en los delitos informáticos. Al respecto, la doctrina internacional y las legislaciones de distintos países encuentran planteamientos distintos, ello en gran medida por las características que presenta el campo informático en sus diferentes facetas, y la relación de esta actividad con diversas aristas de la vida en la sociedad, bien sea la banca, el comercio, la educación, el almacenamiento de la información y el procesamiento de esta. Además, la complejidad en la determinación del bien jurídico protegido ha de atender a la supranacionalidad que tiene internet como espacio que atraviesa fronteras, y como resultado no solo se trastocan diferentes ordenamientos jurídicos, sino que además se presenta la posibilidad de anonimia en las actividades derivadas del uso de este medio de alcance mundial.

[57] Marcelo Temperini, "Delitos informáticos en Latinoamérica: un estudio de Derecho Comparado. 1ra. Parte". *Simposio Argentino de Informática y Derecho*, no. 14 (2013), https://www.academia.edu/33134232/Delitos_Informaticos_en_Latinoamerica.

En tal sentido, como bien asegura Tejero, en tanto no existe un bien jurídico común afectado, o se presentan en exceso y de forma distinta, los bienes jurídicos susceptibles de afectación a través de medios electrónicos, los delitos de esta naturaleza aparecerán vinculados a otros tipos delictivos en los que el legislador haya considerado el uso de las redes digitales o medios electrónicos como idóneos y suficientemente para determinar la lesión de algún bien penalmente protegido a priori.[58]

Por otro lado, ha de considerarse que los delitos informáticos requieren comprender el necesario desarrollo tecnológicos en la sociedad, desarrollo que cada vez es necesario en las relaciones socio económicas entre personas naturales y jurídicas, provocando el interés tutelar del Estado en la protección de la información y demás dimensiones del fenómeno.

Aun con la compleja determinación del bien jurídico protegido, parece no haber duda en que la información debe ser objeto de una tutela orientada a comprender que el contenido de dicha información no tiene que limitarse a la dimensión personal del individuo, es decir, a su intimidad, -que ha de subrayarse-, ya se encuentra regulada en mayor o menor grado por los códigos penales de cada país.

La protección de los datos debe considerar la preservación integral de los sistemas que hacen uso de tecnología de la información y las comunicaciones (TIC), cuya protección evita la lesión a bienes jurídicos de distinta naturaleza.

En cuanto a la consideración de bien jurídico protegido el art. 3 letra b de la LEDIC apuesta por una interpretación según la cual el bien jurídico tutelado puede ir más allá de una consideración taxativa, esto al incorporar la consideración de “entre otros”

[58] Emilio Luis Tejero. "Dificultades jurídicas ante las conductas delictivas contra y a través de medios informáticos y electrónicos", *Revista de Pensamiento Estratégico y Seguridad CISDE*, no. 2 (2019), http://www.uajournals.com/ojs/index.php/cisdejournal/article/view/474.

Art. 3.- Para los efectos de la presente Ley, se entenderá por: (…)

b) Bien Jurídico Protegido: es la información que garantice y proteja el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros";

En el orden planteado el legislador parece brindarle primacía a la información como objeto de tutela, esto ya que subraya en que se trata de "*la información que garantice y proteja el ejercicio de (…)*. Adicionalmente, en el mismo artículo 3 una vez que se define el delito informático vuelve a subrayarse "la información" como objeto de protección sobre una conducta antijurídica.

Art. 3.- Para los efectos de la presente Ley, se entenderá por:

a) Delito Informático: se considerará la comisión de este delito, cuando se haga uso de las Tecnologías de la Información y la Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información; [59]

Ayala considera que no todos los tipos penales que se encuentran en la LCEDIC, hacen una referencia hacia otros bienes jurídicos individuales o colectivos que pudieran ser protegidos, a como ocurre con la intrusión en los sistemas informáticos sin autorización o con abuso, pero sin intencionalidad de ejecutar algún daño, ya que de otra manera se daría vida al art. 7 del referido cuerpo normativo, este precepto aborda los "Daños a Sistemas Informáticos".[60]

[59] Ley de Acceso a la Información Pública. (El Salvador: Asamblea Legislativa de El Salvador, 2011) https://www.fiscalia.gob.sv/wp-content/uploads/portal-transparencia/Ley-de-Acceso-a-la-Informacion-Publica.pdf

[60] Víctor Rodríguez, "Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del Título Segundo de la Ley Especial contra los Delitos Informáticos y Conexos". Oficina de Naciones Unidas contra la Droga y el Delito UNODC (2018) https://escuela.fgr.gob.sv/wp-content/uploads/leyes-nuevas/analisis-juridico-de-la-ley-especial-contra-los-delitos-informaticos-y-conexos-COMPLETO-CAP-I-II-III-V.pdf.

En cuanto delitos inicialmente tipificados por la norma penal y luego retomados por LEDIC, puede considerarse, por ejemplo, la estafa, que una vez en congruencia con los componentes digitales pasaría a considerarse una estafa informática, que como tal recoge elementos constituyentes del delito de estafa, como el ánimo de lucro y la transferencia patrimonial no consentida, pero carente del engaño y error típico de la estafa común, lo que le daría un carácter autónomo a la estafa informática. Esto, a partir de lo indicado de forma específica en el artículo 10, LEDIC.

Estafa Informática

Art. 10.- El que manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro, será sancionado con prisión de dos a cinco años…"[61]

El texto resaltado claramente indica la ausencia del engaño y error antes comentados, y plantea la materialización de la estafa por medio de una habilidad técnica que a un individuo especifico le brindó acceso al sistema tecnológico, al que luego alteró para un beneficio patrimonial. Es decir, para la ejecución de la conducta descrita, el sujeto activo deberá valerse del uso de datos falsos, el uso indebido de su conocimiento de programación, y hacer uso de un "artificio" tecnológico.

El hecho de que la no incorporación de la transferencia no consentida de activos patrimoniales en la tipificación del delito de Estafa Informática en el

[61] Ley de Acceso a la Información Pública. (El Salvador: Asamblea Legislativa de El Salvador, 2011) https://www.fiscalia.gob.sv/wp-content/uploads/portal-transparencia/Ley-de-Acceso-a-la-Informacion-Publica.pdf

texto de la LEDIC, también es objeto de discusión en cuanto a si con ello realmente hay una sustitución del engaño característico de la estafa común, porque “la operación informática o artificio tecnológico”, parece buscar la sustitución del engaño, bajo la premisa de que la máquina efectúa la operación, aunque en efecto lo hace a voluntad del estafador, y dado que el sujeto pasivo no está en condición de aprobar el traspaso patrimonial, el perpetrador lo hace por medio de la manipulación informática, a partir de la obtención fraudulenta del acceso al sistema, lo que lo equivaldría a la presencia de un engaño.[62]

El fraude informático contemplado en el art. 11 LEDIC, también presenta la relación concursal indicada para el delito de estafa informática, por lo cual ahí remitimos.

Otro delito de importante impacto es el espionaje informático, consistente en la obtención de toda clase de información no autorizada, bien sea por motivo de lucro o curiosidad. En la LEDIC este delito se encuentra tipificado en el artículo 12 expuesto a continuación.

Espionaje informático

Art. 12.- El que con fines indebidos obtenga datos, información reservada o confidencial contenidas en un sistema que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, será sancionado con prisión de cinco a ocho años.

Si alguna de las conductas descritas en el inciso anterior se cometiere con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas, resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de la información de carácter

[62] Marcelo Temperini, "Delitos informáticos en Latinoamérica: un estudio de Derecho Comparado. 1ra. Parte".

reservada, confidencial o sujeta a secreto bancario, la sanción será de seis a diez años de prisión".

En la práctica comercial este es un delito de gran importancia, y tradicionalmente busca la protección de los secretos empresariales. Por otro lado, de acuerdo al inciso segundo del art. 12, al referirse a "la seguridad del Estado", pareciera que el bien jurídico protegido tiene mayor amplitud, y por ello la pena es superior ya que se protege la inviolabilidad del secreto, los datos personales, los empresariales y, en mayor medida los estatales.

En un análisis sistémico también se hace necesario valorar que se entiende por datos, información reservada o confidencial, a la que alude el articulo 12 LEDIC.

Esto en buena medida puede solventarse por los artículos 19 y 24 de la Ley de Acceso a la Información Pública (LAIP).

Art. 19.- Es información reservada:

1. Los planes militares secretos y las negociaciones políticas a que se refiere el artículo 168 ordinal 7º de la Constitución.

2. La que perjudique o ponga en riesgo la defensa nacional y la seguridad pública.

a). La que menoscabe las relaciones internacionales o la conducción de negociaciones diplomáticas del país.

b). La que ponga en peligro evidente la vida, la seguridad o la salud de cualquier persona.

c). La que contenga opiniones o recomendaciones que formen parte del proceso deliberativo de los servidores públicos, en tanto no sea adoptada la decisión definitiva.

d). La que causare un serio perjuicio en la prevención, investigación o persecución de actos ilícitos, en la administración de justicia o en la verificación del cumplimiento de las leyes.

e). La que comprometiere las estrategias y funciones estatales en procedimientos judiciales o administrativos en curso.

f). La que pueda generar una ventaja indebida a una persona en perjuicio de un tercero.

No podrá invocarse el carácter de reservado cuando se trate de la investigación de violaciones graves de derechos fundamentales o delitos de trascendencia internacional.

Art. 24. Es información confidencial:

a). La referente al derecho a la intimidad personal y familiar, al honor y a la propia imagen, así como archivos médicos cuya divulgación constituiría una invasión a la privacidad de la persona.

b). La entregada con tal carácter por los particulares a los entes obligados, siempre que por la naturaleza de la información tengan el derecho a restringir su divulgación.

c). Los datos personales que requieran el consentimiento de los individuos para su difusión.

d). Los secretos profesional, comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal.

Por su parte la ley de bancos al referirse al secreto Bancario señala:

Art. 232.- Los depósitos y captaciones que reciben los bancos están sujetas a secreto y podrá proporcionarse informaciones sobre esas operaciones sólo a su titular, a la persona que lo represente legalmente y a la Dirección General de Impuestos Internos cuando lo requiera en procesos de fiscalización.

Las demás operaciones quedan sujetas a reserva y sólo podrán darse a conocer a las autoridades a que se refiere el artículo 201 de esta Ley, y a quien demuestre un interés legítimo, previa autorización de la Superintendencia, salvo cuando sea solicitada por la Dirección General de Impuestos Internos cuando lo requiera en procesos de fiscalización.

Lo establecido en este artículo es sin perjuicio de la información que debe solicitar la Superintendencia para cumplir con lo dispuesto en el Artículo 61 de esta Ley, y con la información detallada que debe dar a conocer al público en virtud del literal f) del Artículo 21 de su Ley Orgánica, así como la que solicite la Dirección General de Impuestos Internos cuando lo requiera en procesos de fiscalización.

El secreto bancario no será obstáculo para esclarecer delitos, para la fiscalización, determinación de impuestos o cobro de obligaciones tributarias, ni para impedir el embargo sobre bienes.[63]

A partir de lo anterior, puede asegurarse que la información reservada o confidencial, como bien jurídico tutelado es un concepto más amplio que la definición sobre estas categorías, en cuyo caso el bien tutelado es el secreto.

Por otro lado, una de las regulaciones expuestas por LEDIC hace referencia a una categoría de análisis de mucho interés en cuanto la regulación de abusos en sistemas ajenos. El delito se presenta en el momento de que una persona paraliza la operación regular de un determinado servicio o recurso vinculado de forma indispensable y necesaria con las TIC, a como sucedería en la paralización de gestiones bancarias o tramites públicos que pudieran realizarse por medio de la web, restringiendo el derecho de uso al servicio.

[63] Ley de Acceso a la Información Pública. (El Salvador: Asamblea Legislativa de El Salvador, 2011) https://www.fiscalia.gob.sv/wp-content/uploads/portal-transparencia/Ley-de-Acceso-a-la-Informacion-Publica.pdf

La denegación de servicio como tipo penal está regulado en el art. 14 de la LEDIC de la siguiente manera:

Técnicas de Denegación de Servicio

Art. 14.- El que, de manera intencionada, utilizando las técnicas de la denegación de servicio o prácticas equivalentes, que afectaren a los usuarios que tienen pertenencia en el sistema o red afectada, imposibilite obtener el servicio, será sancionado con prisión de tres a cinco años.[64]

En este tipo de ataques puede provocar la denegación de un servicio incluso sin que el usuario del equipo pueda enterarse, se trata de software malicioso de intrusión no detectada fácilmente, conocidos como Botnet que invaden un equipo informático y permiten que los cibercriminales los controlen de forma remota, pudiendo ejecutarse actividades ilegales, como, por ejemplo, el hurto de información y la denegación de servicio.

2.2 Modelo de gobernanza con interrelación de lo nacional hacia lo internacional

Por ser internet ese espacio pluralista y democrático en el que discuten múltiples actores a nivel nacional como internacional para establecer criterios de interés de alcance nacional y global es que debe verse como ese espacio en el que la gobernanza sea según las características de este espacio y que no exista una sola institución que regule este entorno.

2.2.1 El principio de corresponsabilidad

La gobernanza del internet ha evolucionado de forma ad hoc, dando lugar a un entorno normativo descentralizado que se ha configurado por una extensa combinación de organizaciones públicas y privadas, actualmente a través del lente de la ciberseguridad el tema se discute en las Naciones

[64] Ley Especial contra Delitos Informáticos y Conexos. (El Salvador: Asamblea Legislativa de El Salvador, 2016) https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2010-2019/2016/02/B6B74.PDF

Unidas, Organización de Estados Americanos, otros foros de servicio del sector privado como el Foro Económico Mundial y en espacios de múltiples actores compuestos por Estados, sociedad civil y academia.

Como antes se comentó, la naturaleza descentralizada de la gobernanza con respecto del internet se encuentra bajo fuertes cuestionamientos, en gran medida por sus problemas de seguridad y privacidad naturalmente vinculados a la gestión de internet, lo que ha suscitado dudas en principio por la naturaleza laxa de la regulación, y en segundo lugar por las dudas acerca de la capacidad normativa que los Estados presentan para regular las prácticas socio económicas relacionadas al uso de internet, que notablemente presentan una dinámica superior a la de la gran mayoría de sistemas jurídicos en el mundo.

El cuestionamiento a la gobernanza del internet en su carácter descentralizado va mucho más allá de lo estrictamente técnico; el trasfondo es sobre quien controla o debería controlar el internet, planteamiento que evidentemente valora la naturaleza descentralizada, a la vez que reconoce el riesgo que esto implica, esto, una multiplicidad de agentes gubernamentales, organizaciones privadas y organismos internacionales. De tal manera que el debate se concentra en la sustitución de un modelo de gobernanza descentralizado con múltiples partes interesadas hacia un modelo centralizado y multilateral.

La tendencia en cuanto a este cambio de modelo de gestión se examina tomando en cuenta los esfuerzos de algunos Estados miembros de la Unión Internacional de Telecomunicaciones, cuyo objetivo es reforzar el papel de los gobiernos en la regulación de Internet.

El modelo de gobernanza mundial de Internet, que ha estado basado en la presencia de múltiples partes interesadas, ha sido el enfoque dominante. La protección de este modelo de gobernanza mundial por medio de internet ha sido valorada como "esencial" para el futuro de Internet.

La convergencia de actores del sector público y privado, además de la sociedad civil, es considerado como un modelo de organización valido, sobre todo para la atención a cuestiones supra estatales. Sin embargo, como consecuencia de la búsqueda de reparto de poder, es necesario abordar las cuestiones de legitimidad y responsabilidad en lo que respecta a la responsabilidad e identificación de los agentes formuladores de las normas.

2.2.2 Labor de los organismos internacionales para prevenir conflictos internacionales

En Centroamérica en general, se reconocen importantes esfuerzos para la promoción del desarrollo de las tecnologías de la información, lo que al igual que en El Salvador incrementa el riesgo a los ciberataques. Algunos de los principales ataques en la región se expresan por medio de las siguientes modalidades: el Phishing (22%), el Malware (20%), los ataques cibernéticos para interrumpir operaciones (13%), así como aquellos que buscan robar dinero (12%) y los fraudes (10%).[65]

El phishing, el robo de datos a través de mensajes SMS o llamadas telefónicas y el fraude amigable son los tres tipos de crímenes cibernéticos de mayor presencia en Centroamérica, cuestión que pudo verse incrementada a raíz del aumento en los servicios digitales los cuales se presentaron como resultado de la pandemia de Covid-19.

Desde el año 2007 fue aprobada la ESCA (Estrategia de Seguridad Centroamericana) como instrumento básico para, desde una perspectiva integral, orientar acciones coordinadas en materia de ciberseguridad

[65] "Tendencias De Seguridad Cibernética En América Latina y El Caribe". Organización de los Estados Americanos OEA, (2013) http://sedici.unlp.edu.ar/bitstream/handle/10915/44143/OEA-_Tendencias_en_la_seguridad_cibern%C3%A9tica_en_Am%C3%A9rica_Latina_y_el_Caribe_y_respuestas_de_los_gobiernos__33_p._.pdf?sequence=19&isAllowed=y .

adopten los países de la región, enmarcadas en sus respectivos ordenamientos jurídicos. El objetivo principal es establecer los componentes y actividades necesarias para fortalecer la seguridad de las personas en la región centroamericana, pero no se contempla la seguridad en su dimensión digital, solamente en su valoración física.

En el año 2019 en Guatemala se realizó un Foro Regional sobre Ciberdelincuencia con destacada participación de Rusia. Este evento se realizó con el propósito de compartir conocimientos prácticos sobre medidas de protección de las instituciones públicas. El Banco Centroamericano de Integración Económica (BCIE) también ha patrocinado seminarios sobre Ciberseguridad en diversos países de la región centroamericana. En estos eventos se discuten temas como, por ejemplo, el funcionamiento de las agencias nacionales de ciberseguridad existentes en otros países; las últimas tendencias en ciberseguridad; las tecnologías aplicadas por el sector privado; y la propuesta de creación de redes de cooperación en materia de ciberseguridad.

El Parlamento Centroamericano (PARLACEN) también ha organizado eventos para estudiar el tema de ciberseguridad bajo el enfoque de Conversatorio Regional sobre Ciberdelincuencia y Seguridad Internacional de la Información, en el que los principales exponentes han sido expertos rusos. Estos eventos han contado con la participación de representantes de Belice, Guatemala, Honduras, República Dominicana, Costa Rica, Nicaragua, Panamá y El Salvador. En Guatemala se ha avanzado en la creación de documentos enfocados en la definición de estrategias sobre sistemas de seguridad digital, por ejemplo, el informe sobre la situación actual de ciberseguridad en Guatemala elaborado en el año 2016.

Desde que ocurrió la filtración histórica de los Panamá Papers (en la que se divulgaron datos privados que mostraban escándalos de corrupción mundial), la región volcó su interés por la mejora de legislaciones encaminadas a la transparencia y la protección de datos.

De acuerdo con Microsoft para Centroamérica y el Caribe los ataques de ransomware han disminuido 67% en Centroamérica y el Caribe, pero la tasa del uso de malwares para robar criptomonedas es 40% más alta en esta región que el resto del mundo. La tasa de ataques por malware para otros fines disminuyó 35%, sin embargo, República Dominicana preserva altos niveles de amenazas. ESET Security Report Latinoamérica indicaba que, en el año 2015, en México, Honduras, Nicaragua, Panamá, Ecuador, Perú, Chile y Uruguay, más del 50% de las empresas encuestadas reportaron "accesos externos no autorizados, lo que supone un alto riesgo de sustracción de información confidencial para todas estas empresas [66].

El Salvador ha suscrito y ratificado una variedad de convenciones internacionales, cuyo objetivo de creación es velar por los derechos de los menores de edad, los cuales, son incapaces de hacerlos valer por ellos mismos. Dichas convenciones ahora forman parte del ordenamiento jurídico del Estado salvadoreño, así mismo, lo que se busca con estas legislaciones internacionales es que se genere la regulación necesaria para prevenir el delito del acoso a niños, niñas, adolescentes y personas con discapacidad.

2.2.3 Vinculación de los organismos nacionales e internacionales

En materia de regulación del ciberdelito, al momento de elaborar la legislación nacional también ha de considerarse la compatibilidad con las leyes de otras naciones. De esta manera se facilitaría la cooperación internacional, porque este tipo delitos es inherentemente de naturaleza internacional y transfronteriza. Acompañado a lo anterior, se necesitan mecanismos internacionales que también faciliten la cooperación internacional en el marco del respeto al derecho soberano de los Estados, y así lograr la asistencia judicial recíproca de forma exitosa.

[66] "ESET Security Report 2015: el estado de la seguridad corporativa en Latinoamérica", ESET Latinoamérica (2015), https://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf.

En resumen, como punto de partida es importante considerar que los delitos y los aspectos procesales deben ser compatibles con los marcos jurídicos de otros Estados. Además, los Estados tienen la responsabilidad de reconocer la importancia de normar este fenómeno jurídico, de tal manera que, las medidas que se consideren en el contexto ciberdelincuencia, han de contar con carácter específico y sentido global a la vez, lo que obliga a una visión conjunta de los problemas.

Con relación a lo anterior, es claro que la dimensión *supranacional* [67] juega un rol de gran importancia en la tipificación y persecución de los delitos informáticos, cuestión que obliga imperativamente a la ejecución de políticas estatales y regionales conjuntas, y que integren a todos los actores afectados o en riesgo de afectación en la sociedad.

Se considera que no basta con establecer una correcta política de cooperación, en lo que el referente son los tratados bilaterales, si no que se requiere de *convenios multilaterales,* [68] porque estos involucran a un mayor número de países.

El multilateralismo permitiría armonizar, al menos, las políticas regionales en materia de cibercrímenes, disminuyendo la contradicción en mayor medida. Para ello, las relaciones entre los Estados deben enmarcarse dentro de un plano de igualdad, equidad, reciprocidad, cooperación y respeto y autodeterminación de los pueblos.

La cooperación internacional en materia de ciberseguridad y ciberdelito

[67] Adjetivo que sobrepasa los límites de lo nacional: autoridad supranacional; las ONG son organizaciones supranacionales. sistema político en el cual determinados Estados ceden parte de sus atribuciones de gobierno. *Véase:* Oxford Languages, (s.f.), acceso el http://www.oxforddictionaries.com/es/definicion/espanol/supranacional.

[68] Los tratados y los acuerdos, tanto bilaterales como multilaterales, entre países son unas de las herramientas más importantes en la diplomacia internacional y la resolución de conflictos. Ambos permiten que los estados se unan y superen desafíos a través de principios jurídicos. Con su larga trayectoria de cooperación, la OEA ayuda a sus Estados miembros a enfrentar los retos de manera colectiva, y por medio de asistencia técnica y jurídica. *Véase:* "Tratados y Acuerdos". Organización de Estados Americanos OEA (s.f.), https://www.oas.org/es/temas/tratados_acuerdos.asp

debe encontrar su fundamento en los instrumentos internacionales aplicables a la materia, así como en una legislación basada en el principio de reciprocidad, esto en aras a agilizar las investigaciones y los procedimientos vinculados a estos delitos transfronterizos como ocurriría, por ejemplo, para la obtención de las pruebas electrónicas de la actividad delictiva.

Ahora bien, es importante resaltar que la cooperación internacional entre los Estados en materia penal ya encuentra fuertes antecedentes, y esta se rige a partir de los acuerdos bilaterales o multilaterales suscritos sobre temáticas específicas, y por uno o varios países, encontrando su fundamento en los principios de voluntariedad y reciprocidad.

Si bien la investigación de la delincuencia informática es una tarea posiblemente más compleja que la actividad delictiva típica, también puede apoyarse en esta estructura de acuerdo para la persecución del acto criminal, no reinterpretando la norma existente, sino aprovechando la cooperación ya existente en diferencias agencias internacionales.

La investigación y el posterior enjuiciamiento de delincuentes informáticos subraya la importancia de la Cooperación internacional en la materia. A como antes se ha subrayado. La posibilidad de lesionar bienes jurídicos en jurisdicciones distintas provoca una pronunciada brecha al momento de llevar ante la justicia a delincuentes informáticos, por lo que establecer un frente común como el propuesto por el Convenio de Budapest en el artículo *23*[69] y siguientes, parece ser la única manera de combatir estas nuevas

[69] Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos. Principios generales relativos a la cooperación internacional. *Véase:* Convenio sobre la Ciberdelincuencia. (Consejo Europeo, Budapest, 2011), artículo 23. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

tipologías delictivas, y con ello su carácter transgresor de fronteras jurídicas y políticas.

En términos prácticos la cooperación internacional en materia de ciberseguridad se presenta predominantemente en torno a algunas organizaciones internacionales como la Unión Europea (UE), la Organización del Tratado del Atlántico Norte (OTAN) o la ONU, entre otras. Con relación a la UE, debe destacarse que, aunque la Comisión Europea comenzó a interesarse en el tema de la ciberseguridad desde el año 2001, fue hasta en el año 2013 cuando se adoptó la primera Estrategia de Ciberseguridad en la que se identifican las prioridades que deben de servir como guía para la política de ciberseguridad en la UE y en el contexto internacional.

Estas prioridades se han enfocado en reducir de forma drástica el cibercrimen, adoptando la Directiva 2013/40/EU), buscando desarrollar una política de ciber defensa regional, y finalmente, definir una política internacional sobre el ciberespacio.

El hecho que más resalta en esta estrategia ha sido la Directiva 2016/1148/UE sobre seguridad de las redes y sistemas de información, también referida como directiva NIS. En esta se han establecido obligaciones aplicables tanto para los Estados miembros como a los operadores de infraestructuras consideradas críticas y relacionadas a los servicios de información, en lo que se incluyen las plataformas de redes sociales, servicios de almacenamiento en la nube y motores de búsqueda.

Por medio de estos instrumentos la UE dejó atrás el enfoque voluntario y se inclina a un enfoque prescriptivo, según el cual impone a los operadores privados la obligatoriedad de adoptar medidas de seguridad, y a la vez la obligación de compartir información con las autoridades con respecto a incidentes de riesgo identificados.

El enfoque prescriptivo marca claramente el rumbo de las estrategias nacionales en materia de ciberseguridad en el plano global. Respecto de la OTAN, debe decirse que esta organización destacar como la primera organización internacional en reaccionar ante las amenazas relacionadas al ciberespacio.

La actividad de la ONU también ha sido muy importante de destacar en cuanto a la ciberseguridad, y en el marco de la Primera Comisión de la Asamblea General en 1998, Rusia comenzó la promoción de resoluciones sobre la seguridad en el ámbito de las telecomunicaciones y la información.

Rusia, China y otros Estados presentaron en 2011 en la asamblea general un Código de Conducta Internacional para la Seguridad de la Información, esto mediante un tratado para la regulación de Internet, propuesta a la que Estados Unidos se opuso de forma concreta. Es en el año 2013 cuando ya se plantea el reconocimiento de la aplicabilidad del Derecho internacional y de la Carta de la ONU al ámbito de las tecnologías de la información y la comunicación (TIC), además de las normas sobre derechos humanos y responsabilidad internacional de los Estados, lo que se ha matizado principalmente con respecto del principio de la diligencia debida, así como respecto de los principios propios del Derecho internacional humanitario.

2.3 Normas de Derecho Internacional y de Derechos Humanos

El 23 de noviembre de 2001 la Unión Europea junto con Estados Unidos, Canadá, Japón y Sudáfrica, firmaron el Convenio de Budapest. Este instrumento jurídico internacional busca intensificar la cooperación entre los Estados firmantes en la persecución de la actividad criminal y en la protección de las actividades relacionadas al uso de las TIC.

En términos generales se busca ofrecer respuestas eficaces, expeditas y coordinadas en la investigación y persecución de esta tipología delictual.

Por lo anterior, se asume el compromiso de adoptar medidas en principio enfocadas en la prevención de lesiones a los derechos de propiedad intelectual, la intimidad, acceso no autorizado y sabotaje. Adicionalmente, se establecieron las condiciones, garantías y lineamientos de cooperación internacional los cuales dirigirán sus acciones.

El convenio agrupa los delitos informáticos en cuatro grupos:

1. Aquellos delitos contra la confidencialidad, integridad, y manejo de datos.
2. Delitos penales que se divulgan por medio electrónicos, como la pornografía infantil y la xenofobia.
3. Delitos conexos relacionados con la informática para alterar sus características originales, como la falsificación y el fraude.
4. Delitos vinculados con los derechos de propiedad.

La Unión Europea, basada en el Convenio de Budapest, en el año 2009 propuso la creación de un tribunal de delitos informáticos, que en un inicio se enfocaría en delitos de fraudes telemáticos y usurpación de identidades. La Convención Sobre Delitos Informáticos o Convenio de Budapest está considerada como el instrumento jurídico internacional más completo, incluyendo un marco global que abarca diversas dimensiones de la ciberdelincuencia. Este es el primer tratado internacional sobre delitos cometidos a través de Internet y otras tipologías de redes informáticas, considerando de forma particular las infracciones a los derechos de autor, la pornografía infantil, el fraude informático y las violaciones de seguridad en la red. Pero, también brinda pautas para identificar una serie de competencias y procedimientos para la persecución de estos delitos.

El Convenio de Budapest se enfoca en enumerar nueve categorías de ofensas, promoviendo la adopción de medidas legislativas o de otra naturaleza, que sean necesarias para hacer converger la infracción penal contempladas en el tratado con su derecho interno.

De tal manera que su principal objetivo, es lograr la aplicación de una política penal común en dirección a la protección contra el cibercrimen, especialmente considerando el fomento de la cooperación internacional.

El instrumento presenta nueve categorías, que se refieren a ocho delitos: acceso ilícito, interceptación ilícita, atentados contra la integridad de datos, infracciones relativas a la pornografía infantil, falsedad informática, atentados contra la integridad del sistema, abuso de equipos e instrumentos técnicos, estafa informática.

A manera de resumen los objetivos fundamentales de la convención son los siguientes:

a) Armonizar las leyes penales de derecho sustantivo que deban ser aplicables a las conductas delictivas que se producen en el entorno informático.
b) Establecer principios de cooperación internacional efectivos, que a la vez puedan adaptarse a la dinámica misma de esta tipología delictiva.

La estructura normativa de este instrumento jurídico de alcance internacional consta de 4 capítulos:

El capítulo I contiene conceptos básicos relacionados a delimitar algunos términos como: datos informáticos, proveedores de servicios de interconexión o almacenamiento de datos informáticos e intercambio electrónico de datos.

En el capítulo II se establecen las medidas recomendadas a los Estados parte para la homologación de su legislación penal sustantiva y adjetiva. Por último, el capítulo III recoge los principios generales de cooperación

internacional, en los que se incluyen elementos medulares como la extradición, asistencia legal mutua e intercambio de información.[70]

En su contenido, el Convenio de Budapest resalta los delitos relacionados con la violación de los Derechos de Autor, lo que obliga a la necesidad de actualización de los acuerdos ya existentes sobre la materia, como la Convención de Berna para la Protección de Trabajos Literarios y Artísticos, el Acuerdo de la OMC sobre Aspectos de Comercio Relacionados con la Propiedad Intelectual, y el Tratado sobre Derechos de Autor de la OMPI.

De igual forma es importante tener en cuenta que el artículo 12 de la Convención remarca en la competencia de los Estados signatarios para adoptar medidas legislativas que aseguren la responsabilidad de las personas jurídicas como actores de actividades delictivas establecidas de conformidad al texto del instrumento.[71]

Adicionalmente, el instrumento también contempla algunas medidas judiciales concretas, tomar en cuenta, como la preservación de la integridad y custodia de datos informáticos; órdenes de búsqueda y allanamiento de datos informáticos, y órdenes para la interceptación de datos informáticos en tiempo real.[72] Estas medidas emitidas por autoridad competente, de conformidad con las disposiciones normativas internas de cada Estado, podrán ser aplicables tanto a individuos como a proveedores de servicios de interconexión informática (ISP, Internet Service Providers), siempre que

[70] La asistencia judicial recíproca en asuntos penales es un proceso por el cual los Estados procuran y prestan asistencia en la reunión de pruebas que se utilizarán en una causa penal. La extradición es el proceso formal por el cual un Estado solicita el regreso forzoso de una persona acusada de un delito o condenada por este a fin de someterla a juicio o que cumpla la condena en el Estado requirente. *Véase:* Manual de asistencia judicial recíproca y extradición de la UNODC (2012).
https://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_S.pdf

[71] Convenio sobre la Ciberdelincuencia, (Consejo Europeo: Budapest, 2001), artículo 8,

[72] Las medidas judiciales como la cadena de custodia de la información, forman parte de los principios del peritaje y el reconocimiento de la evidencia digital de acuerdo al “Manual de Manejo de Evidencias Digitales y Entornos Informáticos” del Dr. Santiago del Pino” al cual puede accederse mediante el siguiente enlace:
https://www.oas.org/juridico/english/cyb_pan_manual.pdf

se encuentren domiciliados dentro del territorio nacional del Estado signatario.

En este contexto, queda a salvo la reserva hecha por los Estados, según la cual tendrán competencia las autoridades nacionales en cualquiera de las siguientes circunstancias: (1) Cuando el delito sea cometido dentro del territorio del Estado; (2) Cuando el delito sea cometido a bordo de un buque con la bandera del Estado; (3) Cuando el delito sea cometido a borde de una aeronave con la bandera del Estado; y (4) Cuando el delito sea cometido por alguno de sus nacionales, si éste es punible de acuerdo con las leyes del lugar en que fue cometido, o si fue perpetrado fuera de la jurisdicción territorial del Estado.

En cuanto al estudio del ciberdelito y su relación con el esquema de ordenamiento jurídico internacional destacan los apuntes de Segura – Serrano,[73] quien comenta que el análisis doctrinal acerca del ciberespacio como ámbito de aplicación de derecho internacional es una temática superada, por lo que no cabe discusión alguna en cuanto a su configuración como ámbito de aplicación al derecho internacional.

Segura – Serrano comenta que, si bien no se ha celebrado ningún tratado general sobre internet, la raíz del problema no debe ubicarse en el ámbito jurídico, sino político. Artiles,[74] también atribuye a una situación política y no jurídica, la falta de interés en la creación formal de un ordenamiento jurídico internacional de Internet, principalmente por un interés estratégico atribuible a los Estados Unidos.

[73] Antonio Segura-Serrano, "Ciberseguridad y Derecho Internacional". *Revista Española de Derecho Internacional,* n. 69 (2017), http://dx.doi.org/10.17103/redi.69.2.2017.2.02.
[74] Néstor Artiles, "Situación de la Ciberseguridad en el ámbito internacional y en la OTAN", *Cuadernos de estrategia*, no. 149 (2011), https://dialnet.unirioja.es/servlet/articulo?codigo=3837337.

Sin embargo, la falta de un único instrumento internacional en la materia no ha limitado el reconocimiento de la aplicabilidad de las normas generales de derecho internacional al ciberespacio.

La ciberseguridad será por mucho tiempo una problemática de interés que seguirá requiriendo de la cooperación internacional en materia política y judicial. Esto encuentra una clara justificación en el interés sobre la seguridad colectiva como una preocupación de primer orden que ya se encuentra atendida en el derecho internacional.

Entre los principales desafíos de regulación a nivel internacional se encuentran las modalidades de cibercrimen y en menor medida el ciberespionaje, ya que frente a las ciber amenazas, las organizaciones internacionales como la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la Unión Internacional de Telecomunicaciones (UIT), están desarrollando una modalidad de cooperación asistencial debido a que se confía más en la creación de capacidades a nivel estatal que en la cooperación de tipo jurídico internacional, situación que claramente se relaciona con la estructura de la gobernanza inicialmente expuesta en este capítulo.

En la dimensión de la responsabilidad internacional, se presentan algunas importantes problemáticas técnico – jurídico a tener en cuenta. Por un lado, debe tomarse en cuenta que la actividad cibernética puede atravesar distintas jurisdicciones nacionales o estatales y, por otro, está la problemática de la atribución de la conducta delictual en la red, misma que es básicamente caracterizada por el anonimato de actividad en la red.

De acuerdo Segura – Serrano a falta de preceptos más específicos, en la regulación del ciberespacio se aplicarían los principios del Derecho internacional general. Sin embargo, queda dilucidar si las actividades de los actores no estatales podrían o no atribuirse a los Estados. Aunque esta situación podría resolverse en el marco del criterio de la diligencia debida,

fundamentado a la vez en la obligación consuetudinaria de no permitir el uso de un territorio para causar daños en otro Estado. Bajo esta premisa, perdería relevancia la necesidad de identificar al autor individual de la actividad cibernética, quien realmente realiza una operación técnica valiéndose de la infraestructura de un Estado.

Diversos autores como José Luis Gómez Barroso, Antonio Segura-Serrano, Néstor Artiles y otros, han identificado las distintas amenazas para la seguridad nacional que emergen desde internet, las que se resumen en la ciberguerra, el ciberterrorismo, el cibercrimen y el ciberespionaje. De acuerdo a Mónica Luengo Montero, "*Vivimos ciber amenazados. Junto con el terrorismo yihadista, la amenaza online constituye el mayor riesgo para nuestra seguridad. Es el quebradero de cabeza de Gobiernos y grandes compañías. Los ciudadanos son los más vulnerables en esta batalla que se libra en Internet, convertida en la ciudad sin ley del siglo XXI."*[75]

Desde el Derecho internacional salvo en el caso de la Convención de Budapest de 2001 no se han desarrollado iniciativas normativas concretas hacer frente cada una de las amenazas antes indicadas.

La doctrina y la práctica jurídica en cada Estado han optado por interpretación extensiva o analógica de las normas convencionales que se encuentran vigentes, y consideradas por algunos autores como suficientes para atender esta problemática.

La ciberguerra es una de las temáticas de mayor atención desde la óptica doctrinal. El problema se presenta ante la posible calificación de los ciberataques como acción encuadrada en el "uso de la fuerza", condición

[75] Mónica Luengo Montero. "Cibercrimen. Ciberguerra. Ciber espionaje. Nadie está a salvo en Internet" EL PAÍS, 31 de enero de 2018, https://elpais.com/elpais/2018/01/22/eps/1516637253_754345.html

que lo equipararía al uso de la fuerza armada contra un Estado, y este punto encuentra bastante consenso en la literatura académica.[76]

El art. 2.4 de la Carta de la ONU abarca lo relacionado a los ataques que causen lesiones o pérdida de vidas humanas, destrucción de la propiedad y, también, daños a infraestructuras críticas que provoquen la normal prestación de servicios esenciales para el funcionamiento de la sociedad.

Con relación a si un ciberataque puede ser interpretado como un ataque armado debe indicarse que la mayoría de autores se inclina a esta posibilidad amparándose en el art. 51 de la Carta de la ONU que hace alusión a la legítima defensa. Sin embargo, en este caso habrá que considerar que el ataque previo tenga una cualitativamente análogos a los de un ataque armado, esto es, en cuanto a su escala y efectos resultantes. Sin embargo, este supuesto no se ha materializado, por lo que no existe antecedente al respecto.

Por lo que respecta al ciberterrorismo, existe la posibilidad de aplicar las Convenciones sectoriales de la ONU que abordan acciones relacionadas como el secuestro, la toma de rehenes, la seguridad de la navegación o la aviación, etc. Algunos actos de ciberterrorismo podrían quedar encuadrados en estos convenios, pero la mayoría quedarían fuera de su ámbito de aplicación si consideramos el enfoque funcional de los mismos, es decir, su operatividad con fines no terroristas de algunos de estos delitos.

Con relación al ciberespionaje, debe decirse que este presenta una preocupación creciente en muchos Estados de la comunidad internacional. A pesar de esto, también se tiende a conceptualizar el ciberespionaje, en términos generales, como una vulneración al principio de soberanía de los Estados, y como resultado el ciberespionaje podría ser considerar una amenaza a la paz y seguridad internacional, y no estrictamente estatal.

[76] Vicente Pons Gamón, "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad".

En principio es necesario reconocer que ya existen delitos considerados de alcance internacional, por lo que no se trata únicamente de la creación de la norma como tal, sino que se hace necesario un reforzamiento e institucional efectivo para la persecución del delito en situaciones transfronterizas. Por lo tanto, se requieren de medidas no legislativas como por ejemplo la creación de unidades especializadas con jurisdicción en diversos contextos geográficos, a como ha quedado demostrado a partir de la experiencia de la Unión Europea. Por supuesto, una de las problemáticas a enfrentar es la disponibilidad de recursos, lo que definirá la capacidad real para atender de forma efectiva la persecución de los delitos de naturaleza transfronteriza. [77]

El estudio de Gamón, también hace énfasis en que América Latina, destina cerca de 400 USD per cápita anual al desarrollo de las TIC, mientras que los países desarrollados gastan entre 2.000 y 3.000 USD anuales.

Esta brecha de inversión entre América latina en los países desarrollados marca una importante capacidad de disponibilidad de recursos y de adaptación a los en estándares de seguridad requeridos para la prevención del delito, Situación que obliga a establecer importantes vínculos de confianza entre agencias nacionales e internacionales especializadas en la persecución del delito o transfronterizo, ratificando la importancia de establecer una red de investigación que logre actividades punitivas en contra de los actores delictivos. [78]

Por lo tanto, a lo antes hecho referencia, si bien es cierto es necesario actualizar el marco jurídico existente en cada Estado y resaltar la importancia de crear equipos especializados que incluyan actores no

[77] María Eugenia Rodríguez Florez, "América Latina, ¿debe crear un sistema de normas armonizadas para el cibercrimen?", *Trabajos de Investigación en Políticas Públicas,* no. 16 (2013), https://econ.uchile.cl/uploads/publicacion/9ba7739a0ac26598402dab53c990c58e49fc259a.pdf.

[78] Vicente Pons Gamón, "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad".

policiales, que, aunque pudieran no comprender la dimensión delictiva, podrían colaborar técnicamente de forma muy eficaz. Estos Actores no policiales, no son más que especialistas vinculados al soporte técnico y creación de redes, son los antes mencionados White Hat, de quienes pueden obtenerse buenas prácticas en el adecuado uso de la web.

"La Declaración de Georgetown en el 2001, puso en evidencia el interés de América latina para lograr propuestas regulatorias con respecto a la convergencia tecnológica…"[79] principalmente con respecto al desarrollo de tecnología que abarate el costo de conectividad, que permita la ampliación de este servicio en condiciones de seguridad.

Desde luego, esto supone un reto para la región, porque el mayor alcance de la red se requerirá mayor educación para la navegación en condiciones seguras. es importante destacar que el interés de la región latinoamericana en cuanto al desarrollo del internet encuentra principalmente motivaciones de naturaleza formativa, porque en cuanto a la configuración delictiva de algunos actos derivados del uso indebido de la red, el comportamiento de la región es predominantemente reactivo enfocado principalmente en la penalización de temática sensibles como sucede con respecto a la divulgación de la pornografía infantil.

En la región, en términos generales, no cuenta con un cuerpo normativo suficiente como para hacer frente a las cambiantes tipologías de crímenes, específicamente en el ciberespacio, mucho menos para atender el carácter transfronterizo que estos tienen, lo que se agudiza con ausencia de armonización jurídica conceptual, sustantiva y procesal en el que los países de la región presentan en sus ordenamientos jurídicos.

Las respuestas reactivas ejecutadas por los países latinoamericanos se encaminan a la modificación de su ordenamiento jurídico penal, pero no a la creación de normas jurídicas el específicamente atiendan a la tipología

[79] Antonio Segura-Serrano, "Ciberseguridad y Derecho Internacional".

delictual derivada del actuar criminal en el ciberespacio. Este es el caso de países como Argentina, Costa Rica, Paraguay Guatemala, México, Bolivia, y Perú.

Los países que si han apuntado a la creación de normas jurídicas específicas son Brasil, Chile, Colombia y Venezuela. Ecuador, presenta un caso particular, en el que la ley civil y comercial ha servido para la introducción de sanciones penales, mientras que Uruguay solo prevé una ley de Protección a los Derechos de Autor.

En un importante grupo de países no se ha presentado una reforma a la ley penal, Ni se han creado de forma específicas leyes para la tipificación de los delitos relacionados al actuar criminal en el ciberespacio, en este caso este grupo de países adoptado por re interpretar las normativas establecidas.

A manera de grupos subregionales como la Comunidad Andina (CAN), el Mercosur, Centroamérica y el Caribe destacan algunos importantes esfuerzos por crear preceptos jurídicos armonizados.

La CAN ha dado importantes pasos en cuanto al uso y reconocimiento de la firma digital y la contratación electrónica como instrumento válido, el Mercosur y Centroamérica se han enfocado más en la protección a la privacidad. Estas acciones también obedecen a un compromiso asumido en la Declaración de Florianópolis del 2001, en la que los países de la región acordaron la promoción de un observatorio regional para el monitoreo del impacto de las TIC sobre la economía, lo que ha llevado al fomento de políticas de armonización a favor de desarrollar marcos normativos que provean confianza y seguridad tanto en la escala nacional como regional.

A la fecha, aunque hay muchas tareas pendientes por resolver, principalmente relacionadas a la terminología que sirva de base para presentar propuestas regionales más sólidas.

La necesidad de resolver las tareas pendientes se acrecienta a partir de los datos mostrados por el Internet Security Threat Report de Symantec [80]: en que se indica que México ocupa el lugar 16 en el mundo, como país origen de ataques, y *el 14% de los computadores zombis del mundo*, se encuentra en la región y América Latina generó 20% de todo el spam en 2019.

Los esfuerzos normativos que se han realizado en la región evidencian voluntad política para desarrollar sistemas jurídicos que respondan a los cambios tecnológicos, pero destaca también una falta de comprensión de las tecnologías que se intentan regular. El comportamiento tradicionalmente reactivo el de la región con respecto a atender nuevas tipologías de delito, específicamente en las que se desarrollan en el ciberespacio, se evidencia con la “Ley Carolina Dieckman” y la Reforma al Código penal que se presentó en Brasil en el año 2013 a partir de la violación a la privacidad y robo de datos personales, seguida de extorsión a la actriz Carolina Dieckmann, lo que detonó un en acciones legislativas para la tipificación de estas acciones.

Conclusión capitular

A partir del comportamiento reactivo de los Estados en América Latina, se debe entender que el cambiar de paradigma es necesario para poder dar respuestas eficaces, expeditas y coordinadas en la investigación y persecución de los ciberdelitos y ciberdelincuentes, es por lo tanto a través del principio de corresponsabilidad, la cooperación internacional e instrumentos internacionales con un enfoque supranacional que se puede perseguir y atacar esta problemática. Ahora bien, todo parte desde la lo regulado a nivel de cada Estado, en el caso de El Salvador podemos concluir que cuenta con un marco jurídico disperso y ambiguo el cual lo leja aún más en función de adherirse a iniciativas desde lo nacional a lo

[80] Dean Turner et al., "Symantec Global Internet Security Threat Report–Trends for July-December 07", *Symantec Enterprise Security*, n.13 (2019), https://docs.broadcom.com/doc/istr-08-april-en.

internacional, ya que el homologar delitos, aspectos procesales es indispensable. Los marcos jurídicos deben ser compatibles por los Estados para construir un modelo de gobernanza efectivo y eficaz, en El Salvador en los últimos cinco años se ha realizado esfuerzos encaminados a la protección de la información personal digital de los habitantes del Estado, a través de instrumentos como la LEDIC, sin embargo este instrumento solo tiene alcance y jurisdicción dentro del territorio salvadoreño y no tiene impacto como marco jurídico con alcance frente a aquellos agentes que delinquen más allá de las fronteras nacionales a través del ciberespacio vulnerando la información personal digital.

CAPÍTULO III: LOS RETOS Y PERSPECTIVAS EN TORNO A LA SEGURIDAD JURÍDICA EN LA PROTECCIÓN DE LA INFORMACIÓN PERSONAL DIGITAL EN EL SALVADOR Y EN POLÍTICA PÚBLICA DE CIBERSEGURIDAD

Introducción capitular

En este capítulo se estableció como objetivo: “determinar los retos y perspectivas que existen en torno a la protección de la información personal digital frente a la ciberdelincuencia.” Por eso, dentro de este capítulo se desarrolla la perspectiva de la doctrina jurídica de la privacidad y la privacidad como derecho humano frente a la doctrina jurídica de la vigilancia estatal como mecanismo de prevención social, es hablar de derechos humanos no como derechos absolutos y para lo cual se toma en cuenta los marcos jurídicos nacionales frente a los internacionales como tratados, convenciones y principios. Además, se presenta una perspectiva de las políticas públicas en materia de ciberseguridad en la región centroamericana hasta llegar a abordar de manera particular la situación de la ciberseguridad en El Salvador, tratando de encontrar los elementos que permitan identificar la existencia de una agenda de ciberseguridad en el país, aun mas allá de eso si existe una política pública en materia. Sin embargo, dado que se trata de crímenes que rebasan la frontera jurídica de un Estado, se ha tomado en cuenta considerar la situación de la ciberseguridad en el entorno geográfico inmediato al cual pertenece El Salvador, situación que implica el análisis de esta temática a nivel regional desde una perspectiva de los conflictos de la ley entro del espacio ya que tenemos frente a esto lo que es soberanía y jurisdicción, ya que la colaboración entre Estados es indispensable para contrarrestar los delitos informáticos de carácter trasnacional. Luego, se ve la perspectiva de una

regulación para generar un entorno seguro sin limitar los derechos y la evolución del derecho humano a la protección de los datos personales y la importancia de la actuación del Estado.

3.1 Retos en el derecho a la protección de los datos personales

El derecho a la privacidad es parte de la evolución del derecho individual enmarcado en los derechos humanos, y su conceptualización encuentra límites de compleja identificación. Sin embargo, la falta de una definición única no resta importancia al asunto, de hecho, al considerarse parte de los derechos humanos encuentra un importante punto de partida para estructurar su definición, por lo que no parece oportuno asegurar una ausencia absoluta de la definición del derecho a la privacidad.

En la doctrina jurídica la privacidad, como derecho humano, ha sido reconocida en los tratados internacionales de derechos humanos[81]. Sin embargo, debe recordarse que como derecho humano no puede considerarse un derecho absoluto, situación que abre la puerta a la regulación estatal en la que se imponen limites, por ejemplo, en materia de seguridad nacional, preservación del orden público, la salud, y los derechos y libertades de terceros. Aunque estas situaciones, para ser permisibles, deben haber sido previstas por el ordenamiento jurídico, y su contenido ha de ser proporcional para perseguir los fines legítimos.

Por supuesto, la doctrina jurídica hace referencia a una fértil discusión

[81] Declaración Universal de Derechos Humanos, artículo 12; Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares, artículo 14; Convención sobre los Derechos del Niño de Naciones Unidas, artículo 16; Pacto Internacional de Derechos Civiles y Políticos, artículo 17; convenciones regionales incluido artículo 10 Del Capítulo Africano Carta sobre los Derechos y el Bienestar del Niño; artículo 11 de la Convención Americana de Derechos Humanos; artículo 4 de los principios de la Unión Africana sobre la Libertad de Expresión; artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre; artículo 21 de la Declaración Derechos Humanos de la ASEAN, artículo 21 de la Carta Árabe de Derechos Humanos, y artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; Principios de Johannesburgo sobre la Seguridad Nacional, Expresión y Acceso a la Información, Principios de Camden para la Libertad de Expresión y la Igualdad Libre.

acerca de la utilidad de la vigilancia estatal como mecanismo de prevención social, lo que puede derivar en un sistema de control punitivo y discrecional sobre miembros de la sociedad de forma particular, o bien sobre la sociedad en su conjunto.

En El Salvador, la discusión respecto al debido uso de internet, ha sido fomentada por organizaciones de carácter no gubernamental, y la finalidad de los datos aportados por el consumidor por medio de las telecomunicaciones y en general por medio de las nuevas tecnologías ha sido motivada en gran medida por las necesidades e intereses del mercado, más que por interés legítimo de proteger los derechos fundamentales de la ciudadanía. Esto se debe a que los datos que voluntariamente comparte el usuario, y que involuntariamente también lo hace al navegar en determinados sitios webs pueden llegar a constituir un importante activo digital para las empresas, llegando a ser objeto de transacciones comerciales de relevante cuantía.

En este sentido, el derecho a la privacidad se encuentra regulado en normativas de distinto rango en varios países, y usualmente se regulan distintas dimensiones de este derecho, bien sea en normas primarias o en normas secundarias. De manera particular, en la región centroamericana, la norma constitucional de Nicaragua, Honduras, Guatemala y El Salvador, protegen el derecho a la privacidad de forma dispersa, expresándose en artículos relacionados explícitamente con el derecho a la intimidad, la inviolabilidad de las comunicaciones, y al domicilio, la autodeterminación informativa, la protección de datos o la garantía de *hábeas data*.

La constitución salvadoreña garantiza en su artículo 2 de forma expresa el derecho a la intimidad personal y familiar y a la propia imagen en su artículo 2, lo que permite evidenciar que el derecho a la intimidad como una de las aristas del derecho de la privacidad está expresamente

manifiesto a nivel constitucional, y, por tanto, las diferentes expresiones de este derecho se pueden encontrar en las actuaciones de los tribunales de primera y segunda instancia.

La protección a la privacidad constituye la base para la protección de la información personal en El Salvador, y es por ello que se hace alusión de forma inicial a tal derecho. En tal sentido, la protección de la información personal también encuentra sustento en la protección a la inviolabilidad de las comunicaciones.

La relación entre la información personal como derecho protegido y la inviolabilidad de las comunicaciones es evidente, dado que la esencia de este último derecho es la protección frente a injerencias arbitrarias a la vida privada de las personas, punto en el que se abraza con la protección de la información personal. La noción de la información personal es amplia, y de forma básica implica todos los datos personales que pueden identificar o llegar a identificar a una persona determinada.

En El Salvador, al igual que en otros sistemas normativos, las garantías legales que protegen a las personas frente a la interferencia de su privacidad, libertad de expresión y protección a su información personal se encuentran dispersas entre la norma constitucional, leyes y tratados internacionales. El efecto de esta protección expone el rol del Estado en la protección, la criminalización, e inclusive de acuerdo a Martínez [82], también implica la vigilancia digital de defensoras y defensores de derechos humanos. Esto se expresa en diversos instrumentos jurídicos de diferente nomenclatura en diferentes países, pero que básicamente son: Código Penal, Ley de Acceso a la Información Pública y Ley de Telecomunicaciones.

[82] Juan Carlos Martínez, "La Cuarta Ola de Derechos Humanos: Los Derechos Digitales (Fourth Wave of Human Rights: The Digital Rights)", *Revista latinoamericana de derechos humanos* 25, no. 1 (2014), https://ssrn.com/abstract=2515038.

3.2 Delitos conexos frente al derecho a la protección de los datos personales

El Código Procesal Penal salvadoreño define que cuando sea necesario intervenir las telecomunicaciones de una persona, debe existir una investigación o proceso aperturado, debiéndose cumplir con las respectivas garantías constitucionales, para que de esta manera la información recolecta pueda tener validez en un proceso judicial con carácter probatorio (Asamblea Legislativa, 2009, art. 176). Este precepto se acompaña de la Ley para la Intervención de las Comunicaciones.

En el ordenamiento jurídico de El Salvador esta intervención se ve limitada a un listado de delitos específicamente delimitados, además de los conexos a este listado, lo que brinda una facultad discrecional al órgano ejecutor de la norma, y como resultado su aplicabilidad es de amplio espectro.[83]

En todo caso, esta intervención puede recaer sobre cualquier tipo de transmisión, emisión, recepción de signos, señales escritas, imágenes, correos electrónicos, sonidos o información de cualquier naturaleza, bien sea haciendo uso de medios ópticos o cualquier otro sistema electromagnético, telefonía, radiocomunicación entre otros.

En este punto es importante destacar la amplia discrecionalidad del Estado en cuanto a la valoración de los medios que pueden ser objeto de intervención, y además es importante subrayar que al menos en el plano

[83] El art. 5 regula de manera taxativa en que delitos únicamente se podrá hacer uso de la facultad de intervención: 1) Homicidio y su forma agravada. 2) Privación de libertad, Secuestro y Atentados contra la Libertad Agravados. 3) Pornografía, Utilización de personas menores de dieciocho años e incapaces o deficientes mentales en pornografía, y Posesión de pornografía. 4) Extorsión. 5) Concusión. 6) Negociaciones Ilícitas. 7) Cohecho Propio, Impropio y Activo. 8) Agrupaciones Ilícitas. 9) Comercio de Personas, Tráfico Ilegal de Personas, Trata de Personas y su forma agravada. 10) Organizaciones Internacionales delictivas. 11) Los delitos previstos en la Ley Reguladora de las Actividades Relativas a las Drogas. 12) Los delitos previstos en la Ley Especial contra Actos de Terrorismo. 13) Los delitos previstos en la Ley contra el Lavado de Dinero y de Activos. 14) Los delitos cometidos bajo la modalidad de crimen organizado en los términos establecidos en la ley de la materia. 15) Los delitos previstos en la presente Ley. 16) Los delitos conexos con cualquiera de los anteriores.

formal, las restricciones jurídicas a la intervención del Estado suponen un límite de actuación que a la vez configura la esfera de protección jurídica a la información personal de aquellos que no han accionado el supuesto jurídico normativa que da vida a la intervención estatal. Dicho de otra manera, la intervención del Estado salvadoreño en cuanto a permear la privacidad e información personal del individuo en el marco de la ley, supone indirectamente la protección de la información personal de quienes no han infringido la norma jurídica que justifica la intervención.

3.3 Casos emblemáticos: delitos más recurrentes

La Ley Especial Contra Delitos Informáticos y Conexos vigente en El Salvador, es de los primeros intentos para poder sancionar lo que se conoce como delitos cibernéticos en el país, y en su contenido se han establecido sanciones de naturaleza penal, siendo necesario el conocimiento de las conductas consideradas ilegales en por la ley, tales como las Estafas electrónicas, el acoso, la manipulación de registros públicos o privados, accesos indebidos a sistemas informáticos, e Interferencia de sistemas informáticos, entre otras.

En el país se han presentado diversas manifestaciones de actos delictivos haciendo uso de dispositivos digitales, algunos de ellos han sido más relevantes que otros. Por ejemplo, en el año 2003 en un simulacro controlado y a 2 semanas en las elecciones presidenciales en el país, se demostró la vulnerabilidad del sistema de transmisión de resultados al lograr ingresar al mismo y alterar la información sobre los votos obtenidos por cada partido. Este ejercicio, implicó de manera ficticia la alteración de actas falsas en 6 juntas receptoras de votos. Este hecho, destaca por la facilidad con que pudo ingresarse al sistema para alterar sin dejar rastro el resultado de la voluntad popular, remarcando que tal acción fue resultado de un simulacro.

Recientemente, la Policía Nacional Civil y la Fiscalía General de la Republica ha recibido muchas denuncias sobre fraudes financieros por medio de correos electrónicos falsos enviados a usuarios de distintos bancos, dejando en condición vulnerable sus estados de cuenta.

También recientemente, el órgano policial ha recibido denuncias de parte de ciudadanos que aseguran haber sido víctimas de estafas telefónicas, lo cual implica la manifestación de llamadas haciéndose pasar por empleados públicos o uno, empleados de bancos que requieren del ciudadano información personal que los ayuda a obtener acceso a sus cuentas bancarias personales.

En otra situación reciente, la Fiscalía General de la República en conjunto con la policía informó haber detenido a cinco personas vinculadas al delito de estafa conocido como “el cuento de las maletas”, el cual se materializaba por medio de la suplantación de identidades digitales de familiares de los afectados. En este acto delictivo, se presentaba la suplantación de familiares y amigos de las víctimas valiéndose de Facebook, y posteriormente contactaban a las víctimas por medio de WhatsApp para comunicarles que había paquetes de encomienda a su nombre. Acto seguido, las víctimas recibían llamadas de supuestos empleados de reconocidas empresas de transporte de encomiendas como Fedex, quienes confirmaban la supuesta encomienda a nombre de las víctimas, con la salvedad de que debido a un sobrepeso del paquete y al contenido de este, debía de pagarse una multa para su liberación. Las víctimas realizaban la transferencia por el monto solicitado a ciertas cuentas bancarias, por lo que estos hechos se enmarcan dentro del delito de estafa por medios electrónicos, lo que en una extensión del término se consideraría una ciber estafa.

Al momento de la presente investigación, la fiscalía ha calculado aproximadamente sin cuenta estafa de este tipo, atribuyéndole el acto delictivo a diez imputados distintos, que de acuerdo las investigaciones han

estafado de manera comprobada por el orden de $30,000, monto correspondiente a diez acusaciones.

Otros casos que sobresalen tienen que ver con el robo de identidad de reconocidos presentadores en medio de comunicación con alcance nacional, entró que cuentan los comunicadores Federico Zeledón, Andrea Giselle del programa “Llévatelo”, así como Alejandra Ochoa y Celina Chanta quienes también han sido blancos de estos delitos.

3.4 Red oculta y el desafío de regulación

Los usuarios normalmente realizan búsquedas por medio de navegadores reconocidos, como Google y además revisan y comparten contenido en sus redes sociales. Sin embargo, detrás de estas acciones existe un lucrativo mercado para la comercialización de la información personal, lo que puede dar inicio a partir de la instalación de programas que el usuario voluntariamente activa en sus dispositivos[84]. Ante esto, quienes navegan por internet han buscado mecanismos para la protección de su identidades, sortear las censuras y entrar en niveles de la navegación web que le permitan la protección de sus datos, y es aquí donde surge la Deep Web también conocida muerte invisible, la que debe de diferenciarse de la Dark Web, que se define como la parte de Internet que se oculta intencionalmente a los motores de búsqueda, utiliza direcciones IP enmascaradas y solo se puede acceder a ella con un navegador web especial, aunque también es parte de la web profunda.

La Deep web presenta un reto para la regulación jurídica, precisamente porque el rastro de las actividades que aquí se realizan es técnicamente muy difícil de seguir, al menos para las instituciones de la ley. Por otro lado, los hechos delictivos que pudieran realizarse en esta modalidad de navegación pueden tener una secuencia de actos en diferentes espacios

[84] Ross Anderson et al., "Measuring the Cost of Cybercrime". Heidelberg (2013), http://dx.doi.org/10.1007/978-3-642-39498-0_12.

jurídicos, cuestión que complica aún más el seguimiento al delito, y la determinación de la jurisdicción correspondiente.[85]

Sin embargo, es necesario para que la Deep web no es solo un mercado de drogas y otros artículos ilegales; también encajan en esta modalidad las redes privadas de navegación, mismas que en su mayoría están destinadas a la protección de datos, información personal y privacidad de su propietario, y por ello, no revisten importancia jurídica. Algunos ejemplos de Deep web son los siguientes: Los sitios internos de las principales empresas, sistemas de intranet de instituciones académicas, bases de datos en línea, y sitios web protegidos con contraseña con acceso solo para miembros.

El lado oscuro de esta modalidad de navegación, ese lado que busca el anonimato para realizar actividades delictivas, se expresa en la venta de drogas, armas ilegales, sicariato y pornografía infantil, entre otras actividades a las que no puede accederse con una búsqueda regular en la web superficial, es decir, en la web de uso común y cotidiano a la que acceden los ciudadanos. La Deep Web incluso ha contado con plataformas de comercio electrónico al estilo de eBay, conocida como Silk Road, la que fue clausurada en el año 2013 como resultado de la cooperación entre diversas agencias de la ley en los Estados Unidos de América [86].

La Deep Web también incluye información oculta detrás de las medidas de seguridad con la que cuentan algunas empresas como media protección, y la violación a esta información oculta se considera una infracción legal, por violación de derechos de autor y violación de términos de uso de un sitio. Recientemente, al momento de elaborar el presente estudio la Deep Web en 2020 había sido un escenario que, debido a la pandemia de salubridad a nivel mundial, propicio diversos tipos de estafas relacionados a la venta

[85] Vicente Pons Gamón, "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad".
[86] Manual de asistencia judicial recíproca y extradición de la UNODC (2012).

de tests caseros de coronavirus, mascarillas de protección y fraudulentas vacunas del Covid-19.

La Deep web supone un reto de regulación jurídica para cualquier país, esto, debido a los recursos especializados que se requiere para operar en ella, costos de infiltración para obtener información, y coordinación entre distintos Estados para la ejecución de una operación, a lo que se agregan los conflictos jurisdiccionales propios de esta situación. Al momento de elaborar este estudio, no existen un instrumento jurídico específico para regular los actos delictivos acontecidos en este nivel de la navegación web.

3.5 Políticas públicas en materia de ciberseguridad y ciberdelitos

De manera particular los países centroamericanos han realizado algunas acciones enfocadas en materia de ciberseguridad. En el año 2016, mediante un convenio de cooperación entre Israel y Honduras, este país centroamericano estudió temas de inteligencia y ciberseguridad, para la protección de bases de datos. En el año 2020 Nicaragua aprobó su Estrategia Nacional de Ciberseguridad. Esta estrategia, se enmarca en la política de Seguridad Nacional que busca establecer condiciones jurídicas y administrativas en materia de ciberespacio, en sus líneas de acción contempla la constitución de un órgano de naturaleza consultiva en materia de ciberseguridad el cual sea integrado por instituciones públicas y privadas.

En el caso de Costa Rica, este país se ubica en la posición 48 del National Cybersecurity Index, en el que se incluyen 160 países, lo que lo ubica en la posición cinco de América, solamente antecedido por Estados Unidos, Paraguay, Chile y Canadá, lo que evidentemente significa que el país lidera la temática de seguridad informática en la región centroamericana, ya que cuenta con una estrategia Nacional de Ciberseguridad elaborada con el apoyo de la OEA y el Cyber4Dev de la Unión Europea.

Panamá por su diversidad en la banca e industria financiera, se convierte en un objetivo de gran interés para los cibercriminales, aunque los esfuerzos de ciberseguridad radican en la auto protección de las empresas privadas sin una política claramente definida desde el sector público.

En El Salvador el gobierno del presidente Nayib Bukele ha creado en el año 2020 la secretaría de Innovación, con la tarea de guiar al país en el proceso de transformación digital y creación de lo que se refiere como la gobernanza digital, entendida como una serie de actividades dirigidas a propiciar un marco legal favorable que busca facilitar la construcción de una sociedad de la información que garantice la privacidad y la seguridad en internet.

Este accionar del gobierno se sustenta en los siguientes instrumentos jurídicos: Constitución de la República, que en su artículo 86 indica que el Estado es responsable de trabajar de forma coordinada, lo que se facilitaría con la aplicación de nuevas tecnologías. Ley especial contra los delitos informáticos y conexos que en términos generales busca la prevención y sanción de los delitos relacionados al uso indebido de datos que terminen por afectar la identidad e intimidad e imagen de personas naturales o jurídicas, así como también la ley de Firma Electrónica y la ley de acceso a la Información Pública, además de la Política Nacional de Datos Abiertos.

Desde la página de la presidencia de la república la ciberseguridad se enfoca en las siguientes actividades:

1. Elaborar e implementar una Estrategia Nacional de Ciberseguridad y política de seguridad digital del Estado, para proteger la información digital en poder del Estado a través de la adopción de estándares internacionales y el trabajo articulado de las instituciones públicas.
2. Elaborar registro y plan de gestión de infraestructura crítica del Estado para identificar riesgos y mitigar amenazas a la infraestructura que soporta los servicios prioritarios nacionales.

3. Fortalecer la gestión del dominio de nivel superior (TLD por sus siglas en inglés) asignado a El Salvador (.SV) para garantizar la seguridad de los portales e impulsar el uso de dominios nacionales en nuestro país.
4. Implementar Centros de Operaciones de Seguridad (SOC) sectoriales para responder a las necesidades específicas de las diferentes áreas y servicios que administra el Estado.
5. Implementar programas de capacitación en ciberseguridad para empleados públicos para garantizar las competencias mínimas y asegurar la información en poder del Estado, para prevenir y mitigar los riesgos derivados de los delitos informáticos.
6. Fortalecer la gestión y los alcances de SalCERT de forma que el Estado pueda contar con una gobernanza claramente definida y con lineamientos actualizados de ciberseguridad.

Sin embargo, estos elementos no permiten hacer referencia a una política de ciberseguridad nacional, aunque si puede destacarse la existencia de una agenda a seguir en materia de ciberseguridad, partiendo de los 6 punto antes declarados. Por otro lado, tampoco es posible hacer referencia a una política de ciberseguridad a nivel regional, dado que los países centroamericanos trabajan sus propios ordenamientos jurídicos en esta materia con escasos vínculos entre ellos. De tal manera que Costa Rica es el único país centroamericano que cuenta con una política de ciberseguridad formalmente declarada por el ministerio de ciencia, tecnología y comunicaciones desde el año 2017.

3.6 El papel de las organizaciones nacionales e internacionales y la cooperación internacional en el combate a los ciberdelitos.

Frente a ese espacio virtual ambivalente, la reacción de los Estados ha sido el reforzamiento de la vigilancia y la protección de los sistemas de información gubernamentales y de infraestructuras vitales de

comunicación, así como también la formulación de mecanismos jurídicos encaminados a limitar los riesgos inherentes a Internet. El problema en el combate del ciberdelito radica en que, a lo interno de las organizaciones internacionales, los países han adoptado posiciones antagónicas con respecto al refuerzo de la seguridad en el ciberespacio.

Algunos países apuntan a elaborar un instrumento jurídico internacional vinculante para todos los Estados, y en el que se enmarque la acción de los Estados. Otros se inclinan a que los Estados no son los únicos afectados, y por ello debe de trabajarse en conjunto con las empresas y la sociedad civil, para así consolidar la seguridad del ciberespacio.

Con este último enfoque también se persigue disminuir el poder estatal en cuanto al riesgo de que el Estado asuma un mayor control en el ciberespacio, limitando así la libertad que caracteriza a Internet.

Otros planteamientos apuntan a considerar que el derecho internacional existente puede ser aplicable al ciberespacio, y, por lo tanto, no es necesario elaborar un nuevo marco jurídico vinculante. De acuerdo a este planteamiento procede que los Estados adopten de manera voluntaria principios de colaboración entre ellos, diseñando medidas que favorezcan la confianza entre ellos, a nivel internacional esta posición colaboracionista encuentra mayor respaldo en el bloque europeo.

Por lo anterior, puede concluirse que el papel de las organizaciones internacionales en cuanto al ciberdelito radica principalmente en la diplomacia colaboracionistas fundamentada en acuerdos de cooperación específicos entre Estados.[87]

[87] José-Luis Gómez-Barroso, Claudio Feijóo, y Dolores F Martínez, "Política antes que regulación: la protección de la información personal en la era del big data", *Economía industrial*, no. 405 (2017), https://dialnet.unirioja.es/servlet/articulo?codigo=6207519

3.7 Soberanía y jurisdicción versus Conflictos de ley en espacio: la necesidad de la colaboración judicial entre los Estados. Reflexiones sobre la extradición

En efecto, las formas sociales naturalmente evolucionan en un colectivo social, en gran medida por la influencia de los cambios en el entorno socio económico, lo que obliga a la sociedad a regular las nuevas expresiones sociales, siempre que estas tengan un interés jurídico que proteger, de esta manera se preservan los componentes del contrato social necesario para la convivencia entre los sujetos sociales. Esta convivencia, a partir de los avances tecnológicos y otros cambios de importante impacto en la sociedad ha rebasado la esfera gubernamental y política, tradicionalmente anclada a un territorio específico, esto se expresa, por ejemplo, en los intercambios comerciales, en los que necesariamente se requiere de instituciones e instrumentos supra nacionales para regular su funcionamiento, lo que también supone un reto para el ordenamiento jurídico de cada Estado. Sin embargo, es importante subrayar que la regulación de una actividad por medio de instrumentos de carácter supra nacional no se manifiesta de forma inmediata, ello porque el ordenamiento jurídico suele presentar una dinámica menor a los cambios económicos, y más cuando se trata de cambios tecnológicos y la forma en que se configuran las relaciones sociales a partir de estos cambios.

Los conflictos de ley en el ciberespacio trastocan los conceptos de soberanía y jurisdicción, esto, por la naturaleza transfronteriza de los datos y la información que implica la manifestación de los ciberdelitos. Si bien el tema no es nuevo, ha tomado relevancia en los últimos años debido a que las pruebas y evidencias que pueden ser útiles para una investigación penal, se encuentran no solamente en sistemas de cómputo utilizados por delincuentes que pueden estar ubicados en diferentes territorios, sino también albergadas en servidores y centros de datos de proveedores de servicios de almacenamiento de cómputo en la nube (cloud computing)

localizados físicamente en distintos países, lo cual complica la labor y las tareas de investigación de las autoridades investigadoras nacionales. De manera tal, que la persecución a los ciberdelitos trae consigo muchas temáticas polémicas y de compleja resolución que afectan tanto el ámbito local en su dimensión de soberanía nacional, como el derecho a la protección de datos.

La soberanía nacional distante del derecho internacional implica la vez la salvaguarda y protección de derechos fundamentales, consideración de la que gozan el derecho a la protección de datos. El complejo concepto de soberanía nacional obliga a la cooperación internacional en la persecución de los delitos cibernéticos, lo que ha de respaldarse en mecanismos de asistencia mutua desde la dimensión jurídica, procurando así el conflicto de leyes, aunque evidentemente estos mecanismos no resolverán en términos prácticos los conflictos jurisdiccionales en la persecución del ciberdelito, situación agravada por la indefinición fronteriza del ciberespacio.

Al momento en que el presente estudio es redactado, a nivel internacional no ha existido un instrumento jurídico que logre unificar las diferentes perspectivas jurídicas estatales sin rozar la soberanía estatal y el conflicto jurisdiccional. Tal problemática, no podido resolverse en sistemas jurídicos que han abordado mayor profundidad el delito en el ciberespacio, como, por ejemplo, el espacio judicial europeo.

La problemática radica en la acción espacial del delito, mismo que puede ser cometido a través del sistema informático de un Estado, pero manifestar sus efectos en uno o más Estados, generando en infinidad de ocasiones la duda con respecto a la identificación acertada del órgano competente para conocer del hecho delictivo.

La anterior situación puede vulnerar con facilidad – a juicio de los autores del presente estudio – el principio de seguridad jurídica que rige que rige el ordenamiento jurídico de El Salvador. En palabras distintas, ante la

ausencia de un instrumento internacional que defina con meridiana claridad la competencia del órgano encargado de perseguir el ciberdelito, la persecución de los actos que encajar en esta categoría delictual terminaría afectando la seguridad jurídica del Estado, esto, por medio de un evidente conflicto jurisdiccional que también puede valorarse como una lesión a la soberanía estatal. También es posible afirmar, que las normas en materia de ciberdelincuencia no cumplen con el carácter imperativo característico de la norma penal, porque no definen de manera exacta la jurisdicción de estos delitos, teniendo hacia la vista un claro vacío en cuanto al existencia de criterios que permitan subsanar la ausencia de tal carácter imperativo.

Se reconoce la complejidad de determinar la jurisdicción en materia de ciberdelito, en principio porque al hacer referencia a internet como escenario principal para la materialización de los ciberdelitos, ha de tenerse en cuenta la ausencia de un espacio físico donde en términos concretos pueda localizarse al actor de los hechos delictivos, lo que dificulta el desarrollo de la investigación criminal. Por lo tanto, puede considerarse que el fenómeno de internet, puede provocar violación del principio de territorialidad, el cual se manifiesta en los aspectos procesales y en el enjuiciamiento de la conducta delictiva.

Por otro lado, el inicio de una investigación por un presunto delito, a excepción de los casos de extradición, el acusado no va a ser entregado a otro Estado reclamante para su debido procesamiento y condena. Otra cuestión a dilucidar es el llamado principio de justicia universal, según el cual sobre ciertos delitos como por ejemplo el ciberterrorismo, cualquier juez podría conocer de la causa.

3.8 El reto de la temporalidad del derecho y la irretroactividad

Considerando que los delitos informáticos son transnacionales, cuando la acción se ejecuta en un país y el resultado en otro país, o bien cuando la transferencia de datos se da en redes informáticas internacionales,

desaparecen plenamente las tradicionales categorías de espacio y tiempo, afectando el principio de territorialidad, y por ende a la extradición, porque la comisión del delito no es discernible fácilmente en términos de territorialidad.

En cuanto el aspecto temporal de la comisión de los delitos informáticos, esto sigue los principios ordinarios, por lo que, si el acto delictivo se manifestó en El Salvador, obligadamente han de seguirse los principios de aplicación temporal del Código Penal en el momento de la comisión del hecho punible, y lo mismo hará cada Estado en razón de su competencia. Sumado a esto, se debe de aplicar el principio de la norma más favorable al imputado, como ocurre en el proceso penal ordinario, resultando en que, si durante la ejecución de la pena se dicta una ley más favorable al condenado, esta deberá beneficiar al imputado, todo de conformidad a la norma constitucional y sustantiva. Por lo que la consideración de ciberdelito no altera los principios básicos del derecho penal, y no se encuentra razón para una posición en sentido contrario.[88]

Entorno seguro sin limitación de derechos

La seguridad en el ciberespacio se trata a dos niveles: la lucha contra el uso criminal del ciberespacio y la protección de los ataques que se presentan en contra de los sistemas de información y comunicación a nivel mundial o a nivel de país. Para la creación de un entorno seguro en el ciberespacio los convenios internacionales como, por ejemplo, el Convenio sobre la Ciberdelincuencia del Consejo de Europa, firmado en Budapest en 2001, y el ordenamiento jurídico nacional busca la regulación de los delitos

[88] Jaime Parra, "Análisis de la penalización del cibercrimen en países de habla hispana". *Revista Logos, Ciencia & Tecnología* 8, no. 1 (2016), https://doi.org/10.22335/rlct.v8i1.339.

contra la confidencialidad y manejo seguro de los datos personales, así como también se penaliza la difusión electrónica de pornografía infantil.[89]

Evidentemente, la protección los sistemas de información requiere una mayor regulación del ciberespacio, pero también una mayor capacidad tecnológica de cada país, para que, de manera particular sus propios sistemas informáticos sean capaces de protegerse, es decir, es necesario la protección de las infraestructuras críticas de la información a escala nacional, en complemento de la protección que algunos sistemas informáticos proveedores de servicios en El Salvador ya posean a escala mundial.

La búsqueda de un entorno seguro en el ciberespacio busca la construcción de una dimensión en la que los derechos de los cibernautas no sean vulnerados, tampoco limitados en su ejercicio, lo que obliga al diseño de políticas públicas que propicien el acceso a internet, y garanticen la no restricción de sus derechos como ciudadano, así como también la navegación segura en estos espacios.

Internet es un motor de crecimiento económico, es también una expresión de libertad y democracia, y son estas extensas materias de derecho las que los Estados deben de proteger y garantizar su manifestación en el ciberespacio sin limitación alguna.

La vulneración de los derechos civiles y políticos de los ciudadanos en internet pueden ser restringidos por diferentes tipos de amenazas, mismas que evolucionan con gran rapidez, como ocurre con el ciberespionaje, interrupción de redes y servicios, o paralización de sistemas informáticos por medio de ataques virtuales.

A nivel país, El Salvador no cuenta con una política pública encaminada a la protección de sus infraestructuras de comunicación vitales, por lo que su

[89] Dario Piccirilli, "Protocolos a aplicar en la Forensia Informática en el marco de las Nuevas Tecnologías (Pericia–Forensia y Cibercrimen)".

economía y demás sistemas informáticos son vulnerables a un ciberataque.[90] En términos prácticos, la protección de los sistemas informáticos se encuentra en manos del sector privado, quienes proveen de seguridad a los sistemas informáticos del sector público, lo que plantea un reto pendiente que escapa al alcance del nivel nacional, porque garantizar los derechos de los ciudadanos en el ciberespacio y asegurar los sistemas informáticos y de comunicación implican un reto a escala internacional, y esto lleva implícitamente un reto diplomático que busca garantizar la seguridad y estabilidad en Internet a pesar de las pronunciadas diferencias económicas y estructurales entre los países.

3.10 Evolución del derecho humano a la protección de los datos personales

Una vez expuesta la evolución del Internet en la sociedad actual, se reconoce una nueva forma de organización social, con claras consecuencias en la economía; por lo que es necesario reconocer que el uso y acceso al internet tiene evidentes impactos en el ejercicio de los derechos humanos de los ciudadanos. Al respecto, debe considerarse que, en un mundo interdependiente y conectado, garantizar los derechos cívicos implica reconocer la conexión de estos con los procesos de desarrollo tecnológico y la valoración del internet como un derecho humano no puede eludir tal situación.

La promoción y la defensa de los derechos humanos es una condición esencial en el fortalecimiento del Estado de Derecho, y esta protección debe extenderse al plano virtual tanto en materia criminal como desde la óptica de los derechos humanos.

[90] Jefferson Pooley, "The Post-Program Era: The Rise of Internet & Society Centers - and a New Interdiscipline".

En el año 2016 el Consejo de Derechos Humanos de Naciones Unidas[91] determinó textualmente que “los derechos de las personas también deben estar protegidos en Internet”. Diversos informes de Relatores para la libertad de expresión, y de forma específica el Relator Especial para la Libertad de Expresión del Sistema Interamericano de Derechos Humanos y el Relator Especial para la Libertad de Expresión de Naciones Unidas, han reconocido los impactos que tiene Internet en el ejercicio del derecho a la libertad de expresión y en el ejercicio de otros derechos humanos. De manera conjunta, estos relatores han manifestado sus preocupaciones sobre los impactos que el Internet tiene en el ejercicio de los derechos humanos, puntualizando en que la protección de los datos y el tráfico de Internet no debe ser objeto de ningún tipo de discriminación por contenido, aplicación o tipo de dispositivo utilizado para su conexión.

En cuanto al antecedente declarativo del internet como derecho Humano, debe apuntarse que la Declaración Universal de los Derechos Humanos fue aprobada en la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948, en ella se promueven, mediante la enseñanza y la educación, el respeto a estos.

El artículo 3 determina que: “Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona.”

En el artículo anterior estipula que los derechos ahí consagrados son inalienables a las personas y que se les tiene que hacer valer, por ello, los Estados que ratificaron este convenio tienen la obligación de crear normativas jurídicas para garantizar el cumplimiento de cada uno de ellos.

---

[91] *“El Consejo de Derechos Humanos de Naciones Unidas es un organismo intergubernamental dentro del sistema de las Naciones Unidas compuesto por 47 Estados responsables de la promoción y protección de todos los derechos humanos en todo el mundo. Tiene la capacidad de debatir todas las diversas cuestiones temáticas relativas a los derechos humanos y situaciones que requieren su atención durante todo el año.”* Consejo de Derechos Humanos de Naciones Unidas (s.f.) *https://www.ohchr.org/sp/hrbodies/hrc/Pages/Home.aspx*

El artículo 5 dice “Nadie será sometido a torturas ni penas o tratos crueles, inhumanos o denigrantes.”

Es decir, que la declaración hace mención que a ninguna persona se le debe vulnerar sus derechos, ni se le tiene que realizar ningún castigo ni menosprecio, ni tratos denigrantes haciendo énfasis en las niñas niños, jóvenes y personas con discapacidad, de todo lo anterior cabe destacar que los niños, niñas y adolescentes que se convierten víctimas del ciberacoso pueden llegar al punto de ser denigrados, lo cual, puede afectar su salud emocional y psicológica.

El artículo 12 regula lo siguiente: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”

En El Salvador se reconoció el 6 de junio de 1995 la competencia de la Corte Interamericana de Derechos humanos, de conformidad con lo dispuesto en el art. 62 de la Convención Americana sobre los Derechos Humanos o Pacto de San José.[92]

Entre los artículos de esta convención se establece que el Estado está en la obligación de crear políticas encaminadas a este tema referente a los menores de edad, en el cual, se deben orientar a los padres de familia e incluso a las personas encargadas legalmente de cuidar a los niños, niñas y adolescentes ajenos a su familia ya que ellos también están en la obligación de garantizar el respeto de los valores de los menores de edad, orientándolos a conocer los mecanismos de educación y disciplina.

La convención de manera general en sus artículos establece una serie de principios en los cuales, se rigen la política de los países que lo ratificaron,

[92] Convención Americana sobre los Derechos Humanos. Organización de los Estados Americanos OEA (1969) https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm

en el Estado salvadoreño, por ejemplo, ha influenciado tanto para crear políticas públicas que beneficien y ayuden a salvaguardar la dignidad de los niños, niñas y adolescentes que son tan vulnerables en esta sociedad.

Conclusión capitular:

En El Salvador en materia de protección de la información personal digital el gran reto por parte del Estado es cambiar ese enfoque disperso por uno que garantice la protección de los datos a nivel individual sin que se vulnere el derecho a la privacidad. Dentro de este cambio de enfoque la agenda y política pública en esta materia es indispensable, ya que esto permitirá tener un enfoque trasfronterizo de tal forma que se puedan suscribir instrumentos jurídicos internacionales vinculantes, ya que actualmente se carece de una estrategia, agenda y política pública en materia de ciberseguridad y protección de la información personal digital en El Salvador desde una perspectiva nacional y aún más desde una perspectiva internacional.

CONCLUSIONES

Después de la investigación, análisis y estudio de la información digital de los habitantes del Estado salvadoreño frente ciberdelitos por agentes fuera de la jurisdicción, podemos concluir lo siguiente:

La globalización ha logrado el desarrollo de la tecnología y las infraestructuras digitales, esto ha ayudado a que exista comunicación y mayor acceso al ciberespacio, creciendo de forma exponencial el riesgo para los países y personas por medio de la ciberdelincuencia, es por lo anterior que las leyes relacionadas con el delito cibernético continúan evolucionando en varios países del mundo, es por eso que se debe trabajar en materia de cooperación internacional desde una perspectiva del multilateralismo, ya que los organismos internacionales de forma continua enfrentan desafíos cuando se trata de encontrar arrestar acusar y probar delitos cibernéticos. Por eso la evolución del derecho internacional en materia de ciberespacio debe seguir su curso de manera acelerada en relación con la protección de los datos personales digitales.

La privacidad y protección personal de la información en línea enfrentan el desafío de la seguridad de la información personal digital más allá de la conciencia de las acciones y comportamientos de usuario o individuo en el ciberespacio y el uso de herramientas como filtros de navegación, contraseñas, software antivirus y cortafuegos, es por eso necesario que cada Estado desarrolle agendas en materia de ciberseguridad, así como una política pública en esta materia para velar por los derechos y deberes de cada uno de los ciudadanos desde una perspectiva nacional a lo internacional, a través de un ordenamiento jurídico para la protección de datos personales y seguridad digital, respetando los derechos al acceso a internet y el ciberespacio bajo un entorno seguro.

Por lo anterior podemos establecer que en El Salvador en los últimos cinco años se ha realizado esfuerzos encaminados a la protección de la información personal digital de los habitantes del Estado, a través de instrumentos como la LEDIC, sin embargo este instrumento solo tiene alcance y jurisdicción dentro del territorio salvadoreño y no tiene impacto como marco jurídico con alcance frente a aquellos agentes que delinquen más allá de las fronteras nacionales a través del ciberespacio vulnerando la información personal digital.

Por parte del Estado de El Salvador la evolución del derecho en materia de ciberespacio y la protección de datos personales no ha sido de acuerdo al desarrollo de las tendencias de las TIC y los retos e implicaciones que todo esto representa. Actualmente el marco jurídico existente no es suficiente al punto que brinde protección a la información personal digital frente a las amenazas del entorno del ciberespacio y por lo tanto se tienen grandes retos para poder decir que existe seguridad jurídica en cuanto a la protección de la información personal digital, lo que presupone que hay vulnerabilidad jurídica para cada habitante dentro del territorio, ya que no hay un marco de actuación ante sucesos o amenazas. Actualmente se carece de una estrategia, agenda y política pública en materia de ciberseguridad y protección de la información personal digital en El Salvador desde una perspectiva nacional y aún más desde una perspectiva internacional.

Finalmente, la seguridad de la información personal digital y ciberseguridad debe estar basada en que debe de existir un equilibrio en el que se genere un entorno seguro, pero sin limitar derechos y hablar de derechos y capacidades para generar desarrollo sin olvidar la seguridad informática. Todo esto se debe de promover en un entorno seguro bajo las normas de derecho internacional y de derechos humanos. Por lo tanto, se debe trabajar con una estrategia nacional que se vincule a lo internacional ante

incidentes. Los marcos jurídicos se deben buscar por medio de una estrategia integral vinculante desde el área personal, institucional, nacional e internacional, teniendo como punto clave la cooperación, y aunque a nivel técnico la clave pasa por la prevención, ante delitos entra la parte jurídica como regulaciones, reglamentos, leyes y otros instrumentos en materia.

RECOMENDACIONES

Una recomendación es que de parte de la academia, docentes y estudiantes se debe iniciar a partir de este informe con la sistematización, estudio e investigación en materia de ciberespacio, partiendo de la protección de la información personal digital de cada persona desde una perspectiva jurídica y más allá de la técnica. La academia debe velar por el desarrollo de un entorno seguro en esta materia, ya que forma, investiga, desarrolla y aplica la ciencia para buscar soluciones y genera talento humano.

En El Salvador se debe crear un organismo que monitoree la actividad y riesgo con lineamientos y regulaciones como políticas, legislación, capacitación, equipos de respuesta, creación de capacidades y de respuestas a emergencias informáticas y unidades de ciberdelincuencia en todos los países. La política y estrategia nacional de ciberseguridad tanto pública como privada, deben ser desde un enfoque técnico y jurídico, ya que en general en El Salvador hay ausencia de un órgano, instrumento, convenio internacional que regule el ciberespacio, por lo tanto, hay vacíos que se vinculen desde el derecho internacional y de aplicación de este.

En cuanto al papel del Estado de El Salvador, el gobierno como autoridad debe articular el diseño de las políticas públicas de seguridad de la información personal digital y ciberseguridad, debe dar impulso y coordinar

la cooperación en el ámbito de la ciberseguridad desde una perspectiva regional y global, partiendo de lo nacional. Es por lo anterior que el Estado deben crear una agencia de inteligencia en materia de ciberespacio, tener una agenda y estrategia en ciberseguridad que incluyan trabajar con el sector privado, la academia y la sociedad civil para desarrollar una política pública en esta materia, de tal forma que se pueda llevar a cabo el ejercicio en la red y ciberespacio, y ejercer el derecho a la información y datos con seguridad y libertad a la vez.

Para una estrategia integral vinculante desde las áreas personal, institucional, nacional e internacional la cooperación es clave, en ese sentido el Estado debe trabajar en fortalecer las relaciones y mecanismos de interlocución a partir de dos puntos: uno, un grupo de composición abierta para vincularse a organismos internacionales; dos, grupo de expertos intergubernamentales donde confluyan múltiples actores como la academia, sociedad civil, empresa y otros.

En términos de planificación, agenda y política públicas se recomienda en específico para la protección a la información digital y respeto a la privacidad el papel del Estado es crucial, por eso la planificación debe prever las manifestaciones delictuales conforme a estos delitos en el futuro. Se debe de entender que la realidad de internet es cambiante y a veces mucho más rápida que el material, por eso, a través del Estado debe tomar en cuenta a profesionales de las relaciones internacionales, ciencias jurídicas, sociología y psicología estudiar el comportamiento humano en este sentido, de manera que sirva para el diseño de políticas públicas e instituciones jurídicas, acompañado de grupo de expertos en materia técnica.

FUENTES DE INFORMACIÓN

Libros

- Barrio Andrés, Moisés. "*Ciberdelitos: Amenazas Criminales Del Ciberespacio*". Ed.1. España: Editorial Reus S.A.; 2017.
- Keen, Andrew. Internet no es la respuesta. (España: Catedral Editorial, 2016).
- Moore, Robert. Cybercrime: investigating high-technology computer crime. (New York: Routledge, 2010).

Trabajos de Graduación

- Piccirilli, Darío. "Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías (pericia–forensia y cibercrimen)". Tesis doctoral, Universidad Nacional de La Plata, 2016. https://doi.org/10.35537/10915/52212.
- Pisciottano, Nickolas. "The Impact of the Internet on Social Capital: Broadband Access and Influences on Voting Turnout". Master´s Thesis, Hopkins University, 2019. https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/61851/Pisciottano,%20Nickolas.pdf?sequence=1

Jurisprudencia

- Convención Americana sobre los Derechos Humanos. San José. Costa Rica. Organización de los Estados Americanos, 1969. https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm
- Convenio sobre la Ciberdelincuencia. Consejo Europeo. Budapest, 2001. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Documentos Institucionales

- Barrera Ibáñez, Silvia. "*Ciberpol. Metodología para la Investigación del Cibercrimen*." Universidad de la Rioja UNIR (2019). https://reunir.unir.net/bitstream/handle/123456789/10060/Barrera%20Ib%C3%A1%C3%B1ez%2C%20Silvia.pdf?sequence=1&isAllowed=y
- Bell, Patrick. "*Cyber Threat Report 04 April 2019*". Army Ciber Institute at West Point (2019). https://digitalcommons.usmalibrary.org/cgi/viewcontent.cgi?article=1041&context=aci_rp
- “Estudio exhaustivo sobre el delito cibernético”. Oficina de Naciones Unidas contra la Droga y el Delito UNDOC (2013). https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf.
- “ESET Security Report 2015: el estado de la seguridad corporativa en Latinoamérica”. ESET Latinoamérica. (2015). https://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf.
- Feusier, Waldo. “Aplicación y Contenido de la Ley Especial contra la Delincuencia Informática y Conexos”. Consejo Nacional de la Judicatura El Salvador (2020). https://www.academia.edu/41596209/APLICACI%C3%93N_Y_CONTENIDO_DE_LA_LEY_ESPECIAL_CONTRA_LA_DELINCUENCIA_INFORM%C3%81TICA_Y_CONEXOS_CONCURSO_DE_INVESTIGACI%C3%93N_CNJ_Fomentando_la_investigaci%C3%B3n_para_mejorar_la_Administraci%C3%B3n_de_Justicia_Barrera-Ibáñez.
- Rodríguez Florez, María Eugenia. "América Latina, ¿debe crear un sistema de normas armonizadas para el cibercrimen?" *Trabajos de Investigación en Políticas Públicas TIPS*, no. 16 (2013).

https://econ.uchile.cl/uploads/publicacion/9ba7739a0ac26598402dab53c990c58e49fc259a.pdf.

- “Tendencias De Seguridad Cibernética En América Latina y El Caribe”. Organización de los Estados Americanos OEA (2013). http://sedici.unlp.edu.ar/bitstream/handle/10915/44143/OEA-_Tendencias_en_la_seguridad_cibern%C3%A9tica_en_Am%C3%A9rica_Latina_y_el_Caribe_y_respuestas_de_los_gobiernos__33_p._.pdf?sequence=19&isAllowed=y.
- Rodríguez. “Análisis jurídico de los delitos contenidos en los capítulos I, II, III y V del título segundo de la Ley Especial contra los Delitos Informáticos y Conexos". Oficina de Naciones Unidas contra la Droga y el Delito UNODC (2018). https://escuela.fgr.gob.sv/wp-content/uploads/leyes-nuevas/analisis-juridico-de-la-ley-especial-contra-los-delitos-informaticos-y-conexos-COMPLETO-CAP-I-II-III-V.pdf
- Turner, Dean, Marc Fossi, Eric Johnson, Trevor Mack, Josepth Blackbird, Stephen Entwisle, Mo King Low, David McKinney and Candid Wueest. "Symantec Global Internet Security Threat Report– Trends for July-December 07". *Symantec Enterprise Security* (2019). https://docs.broadcom.com/doc/istr-08-april-en

Fuentes hemerográficas

- Aguilar Joyanes, Luis. "Ciberseguridad: la colaboración público-privada en la era de la Cuarta Revolución Industrial (Industria 4.0 Versus Ciberseguridad 4.0)." *Cuadernos de estrategia*, no. 185 (2017): 19-64. https://dialnet.unirioja.es/servlet/articulo?codigo=6115620.
- Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michael J. G. Van Eeten, Michael Levi, Tyler Moore y Stefan Savage. "Measuring the cost of cybercrime”. *The Economics of Information*

Security and Privacy, (2013): 265-300. http://dx.doi.org/10.1007/978-3-642-39498-0_12

- Arroyo. "La cibercriminología y el perfil del ciberdelincuente". *Derecho y Cambio Social*, no. 60 (2020): 470-512. https://dialnet.unirioja.es/servlet/articulo?codigo=7524987.
- Ardissom de Souza, Rodrigo. "De las redes hacia el ciberespaci*o*". *Revista Digital Universitaria*, no. 2 (2020). http://doi.org/10.22201/codeic.16076079e.2018.v19n1.a2
- Bay, Morten. "Conversation with a Pioneer: Leonard Kleinrock on the Early Days of Networking, the Arpanet… and Winning in Las Vegas". *Internet Histories,* no. 1-2 (2018): 140-52. https://doi.org/10.1080/24701475.2018.1446239.
- Camacho, David. "Aidacyber: Contribuciones En Ciberseguridad Y Cibercrimen". *Information Fusion, n.*63 (2020): 1-33. http://aida.etsisi.upm.es/wp-content/uploads/2020/07/AIDA_Cyber_2020.pdf.
- Dai, Bin, Guan Xu, Bengxiong Huang, Peng Qin, and Yang Xu. "Enabling Network Innovation in Data Center Networks with Software Defined Networking: A Survey". *Journal of Network and Computer Applications, no.* 94 (2017): 33-49. https://doi.org/10.1016/j.jnca.2017.07.004.
- Écija Bernal, Álvaro. "*Ciberespacio, ciberderecho y ciberabogados.*" *Noticias Jurídicas*, 8 de marzo de 2017, https://noticias.juridicas.com/conocimiento/articulos-doctrinales/11733-ciberespacio-ciberderecho-y-ciberabogados/.
- Franco de la Cuba, Carlos Miguel. "*La Interpretación de la norma jurídica.*" *Derecho y Cambio Social*, no. 2 (2004): 14. https://dialnet.unirioja.es/servlet/articulo?codigo=5512186.
- Ganuza Artiles, Néstor. "Situación de la ciberseguridad en el ámbito internacional y en la OTAN." *Cuadernos de estrategia*, no. 149 (2011): 165-214.

https://dialnet.unirioja.es/servlet/articulo?codigo=3837337

- Gómez-Barroso, José Luis. "Uso y valor de la información personal: un escenario en evolución". *El profesional de la información (EPI),* no. 1 (2018): 5-18. https://doi.org/10.3145/epi.2018.ene.01.
- Gómez-Barroso, José Luis, Claudio Feijóo, y Dolores F. Martínez. "Política antes que regulación: la protección de la información personal en la era del big data.". *Economía industrial*, no. 405 (2017): 113-19. https://dialnet.unirioja.es/servlet/articulo?codigo=6207519.
- González Ramírez, Teresa y Angela López Gracia. "La identidad digital de los adolescentes: usos y riesgos de las tecnologías de la información y la comunicación". *RELATEC,* no. 2 (2018). https://doi.org/10.17398/1695-288X.17.2.73.
- Martinez, Candelaria, Lozano, Zúñiga, Peláez, y Michel. "Después de presionar el botón enviar, se pierde el control sobre la información personal y la privacidad: un caso de estudio en México." *Revista Ibérica de Sistemas e Tecnologias de Informação RISTI*, n. 21 (2017): 115-280. https://dialnet.unirioja.es/servlet/articulo?codigo=6671446.
- McKelvey, Fenwick and Kevin Driscoll. "Arpanet and its boundary devices: modems, imps, and the inter-structuralism of infrastructures". *Internet Histories*, n. 1 (2019): 31-50. https://doi.org/10.1080/24701475.2018.1548138.
- Meraz Espinoza, Ana Isabel. "Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales". *Revista IUS*, n. 41 (2018): 293-310. http://www.scielo.org.mx/pdf/rius/v12n41/1870-2147-rius-12-41-293.pdf.
- Muttio, Eugenio Muttio, Salvador Botello y Maximino Tapia. "Modelado paramétrico mediante programación visual en el diseño y análisis estructural de edificios". *Revista Mexicana de Métodos*

Numéricos, n.1 (2017). https://www.scipedia.com/public/Muttio_et_al_2017a.

- Palacio Puerta y Cabrera Peña. "La gobernanza de internet como plataforma para impulsar políticas en la educación con TIC. El caso de Colombia". *Revista Opera*, no. 21 (2017): 5-23. https://doi.org/10.18601/16578651.n21.02.
- Poodley, Jeff. “The post-program era: the rise of Internet & society centers—and a new interdiscipline”. *Culture Digitaly* (blog), march 5, 2018. https://culturedigitally.org/2018/03/the-post-program-era-the-rise-of-internet-society-centers-and-a-new-interdiscipline/.
- Polo Roca, Andoni. "Sociedad de la información, sociedad digital, sociedad de control". *Revista Vasca de Sociología y Ciencia Política Inguruak,* no. 68 (2020). http://dx.doi.org/10.18543/inguruak-68-2020-art05.
- Pons Gamón, Vicente. "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad”. *Revista Latinoamericana de Estudios de Seguridad URVIO*, no. 20 (2017): 80-93. https://doi.org/10.17141/urvio.20.2017.2563
- Riofrío Martínez-Villalba, Juan Carlos. "La Cuarta Ola de Derechos Humanos: Los Derechos Digitales ". *Revista latinoamericana de Derechos Humanos*, no. 1 (2014). https://ssrn.com/abstract=2515038.
- Rojas Parra, Jaime Hernán. "Análisis de la penalización del cibercrimen en países de habla hispana”. *Revista Logos, Ciencia & Tecnología* (2016): 220-31. https://doi.org/10.22335/rlct.v8i1.339
- Segura-Serrano, Antonio. "*Ciberseguridad y Derecho Internacional”. Revista Española de Derecho Internacional REDI,* n.2, *(*2017. http://www.revista-redi.es/es/articulos/ciberseguridad-y-derecho-internacional-2/
- Soni, Virendra. "Multifunctional malware becoming extensive in 2018, finds Kaspersky Lab Report”. Daily Host News DHN (2018).

https://www.dailyhostnews.com/multifunctional-malware-becoming-extensive

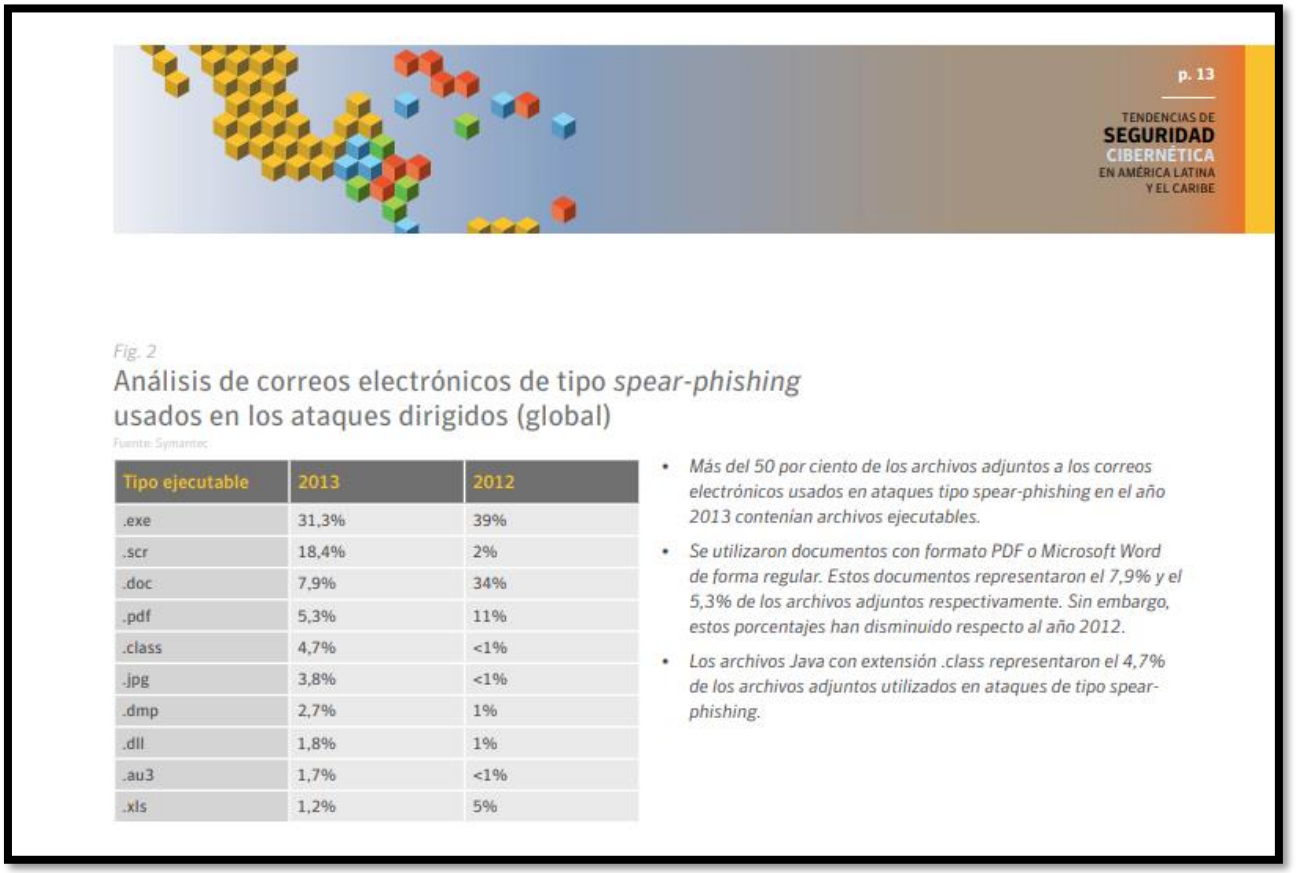
- A. Tavosanis, Mirko L. "Libraries, linguistics and artificial intelligence: Jcr Licklider and the libraries of the future". *JLIS.It,* n. 8 (2017), 137–147. https://doi.org/10.4403/jlis.it-12271
- Tejero, Emilio Luis. "Dificultades jurídicas ante las conductas delictivas contra y a través de medios informáticos y electrónicos". *Revista de Pensamiento Estratégico y Seguridad CISDE* 4, no. 2 (2019): 39-54. http://www.uajournals.com/ojs/index.php/cisdejournal/article/view/474.
- Vásquez Mata, César Eduardo, José Mauricio Regalado González, y Ricardo Salvador Guadrón Gutiérrez. "*Cibercrimen E Informática Forense: Introducción Y Análisis En El Salvador.*" *Revista Tecnológica, n. 10* (2017). http://hdl.handle.net/10972/3029.
- Villanueva, J., M. Bueno, J. Simón, M. Molinas, J. Flores, y P. E. Méndez. "Aplicación de la transformada de Hilbert-Huang en el análisis de señales de comunicación satelital". Revista Iberoamericana de Automática e Informática industrial, n. 2 (2020): 181-89. https://doi.org/10.4995/riai.2019.10878.

Otras fuentes

- Borghello, Cristian y Marcelo Temperini. "Suplantación de identidad digital como delito informático". *Simposio, Sociedad Argentina de Informática SADIO, 27 al 31 de agosto de 2012, http://sedici.unlp.edu.ar/handle/10915/124395.*
- Temperini, Marcelo. "Delitos informáticos en Latinoamérica: un estudio de Derecho Comparado. 1ra. Parte". Simposio Argentino de Informática y Derecho, no. 14 (2013), https://www.academia.edu/33134232/Delitos_Informaticos_en_Latinoamerica.

ANEXOS

Ilustración 1: Análisis de correos electrónicos de tipo spear-pishing usados en los ataques dirigidos (global)



p. 13

TENDENCIAS DE
SEGURIDAD
CIBERNÉTICA
EN AMÉRICA LATINA
Y EL CARIBE

Fig. 2

Análisis de correos electrónicos de tipo *spear-phishing* usados en los ataques dirigidos (global)

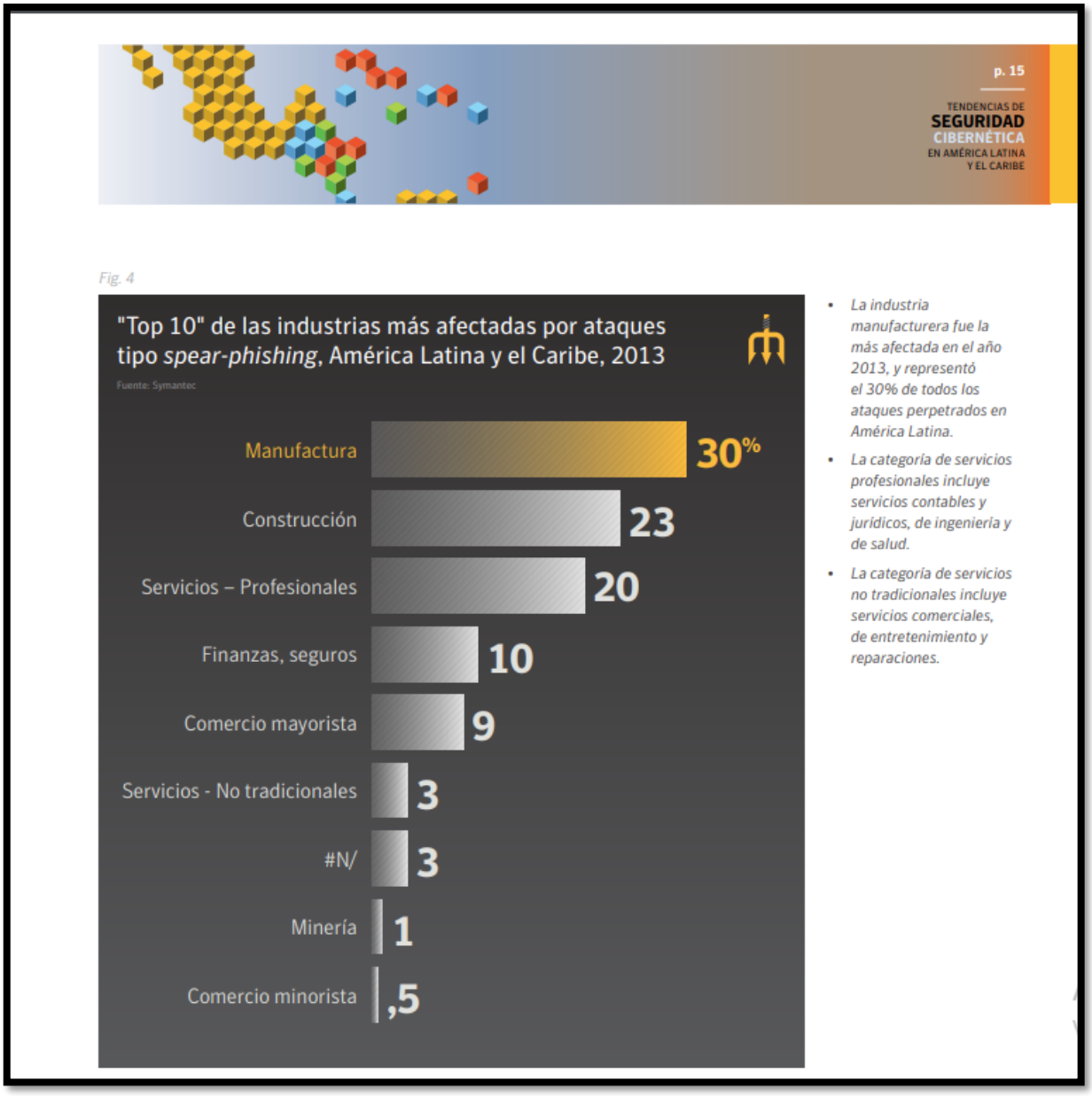
Fuente: Symantec

Tipo ejecutable	2013	2012
.exe	31,3%	39%
.scr	18,4%	2%
.doc	7,9%	34%
.pdf	5,3%	11%
.class	4,7%	<1%
.jpg	3,8%	<1%
.dmp	2,7%	1%
.dll	1,8%	1%
.au3	1,7%	<1%
.xls	1,2%	5%

- *Más del 50 por ciento de los archivos adjuntos a los correos electrónicos usados en ataques tipo spear-phishing en el año 2013 contenían archivos ejecutables.*
- *Se utilizaron documentos con formato PDF o Microsoft Word de forma regular. Estos documentos representaron el 7,9% y el 5,3% de los archivos adjuntos respectivamente. Sin embargo, estos porcentajes han disminuido respecto al año 2012.*
- *Los archivos Java con extensión .class representaron el 4,7% de los archivos adjuntos utilizados en ataques de tipo spear-phishing.*

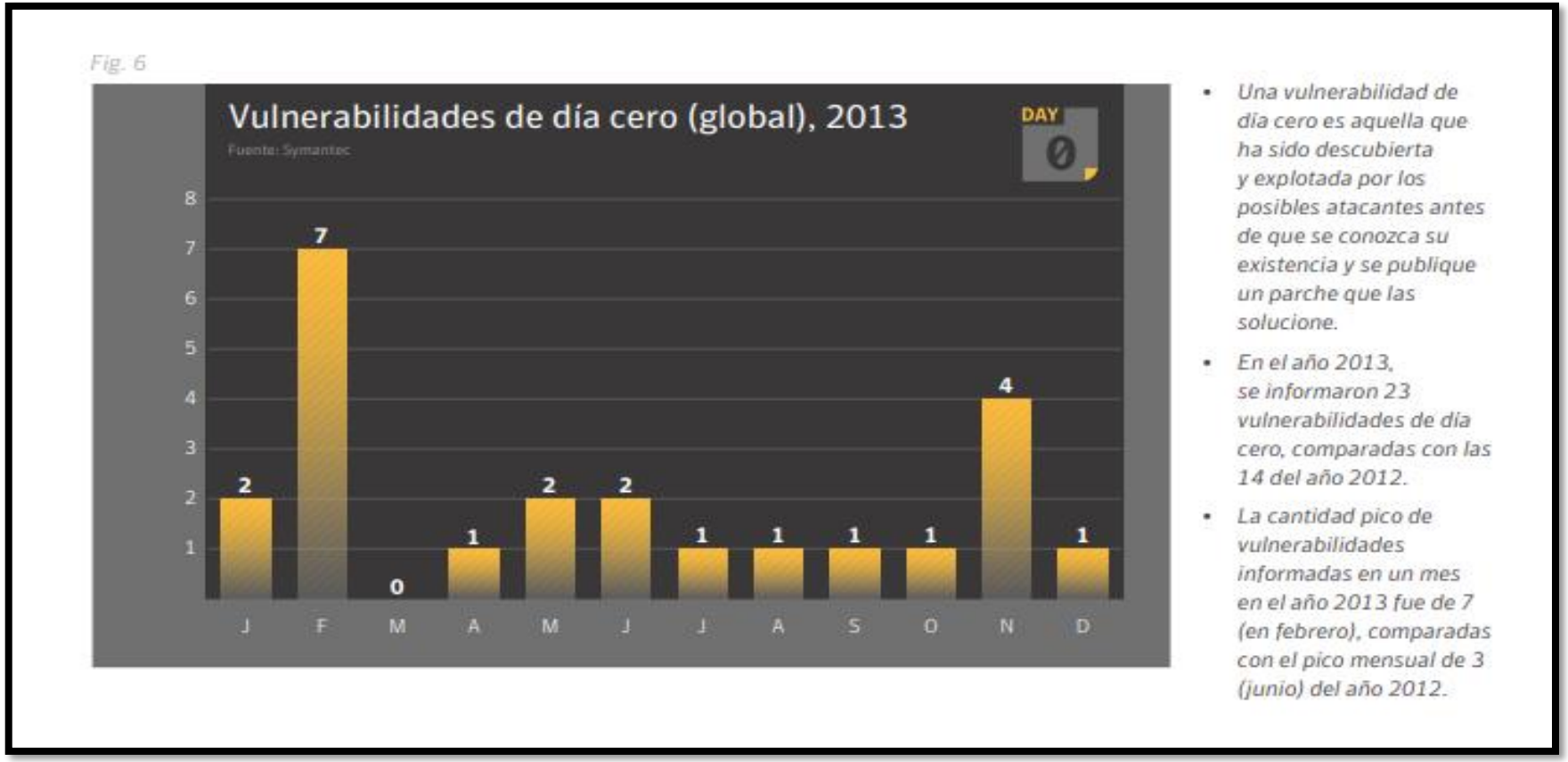
Fuente de la imagen: “Tendencias de Seguridad Cibernética en América Latina y el Caribe”. Symantec Organización de los Estados Americanos OEA (2014) https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

Ilustración 2: “Top 10” de las industrias más afectadas por ataques tipo spear-pishing, América Latina y el Caribe, 2013



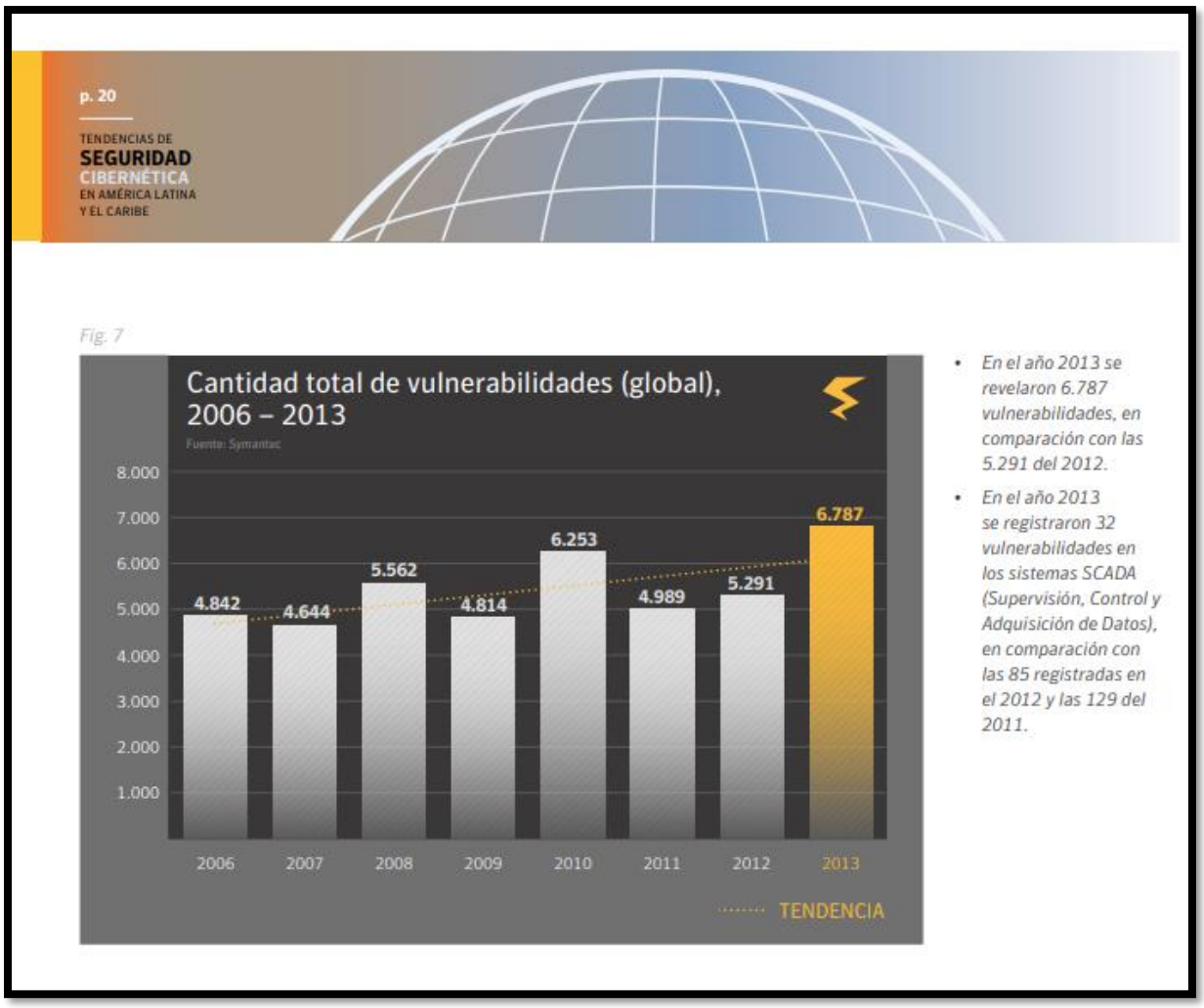
Fuente de la imagen: “Tendencias de Seguridad Cibernética en América Latina y el Caribe”. Symantec Organización de los Estados Americanos OEA (2014) https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

Ilustración 3: Vulnerabilidades de día cero (global), 2013



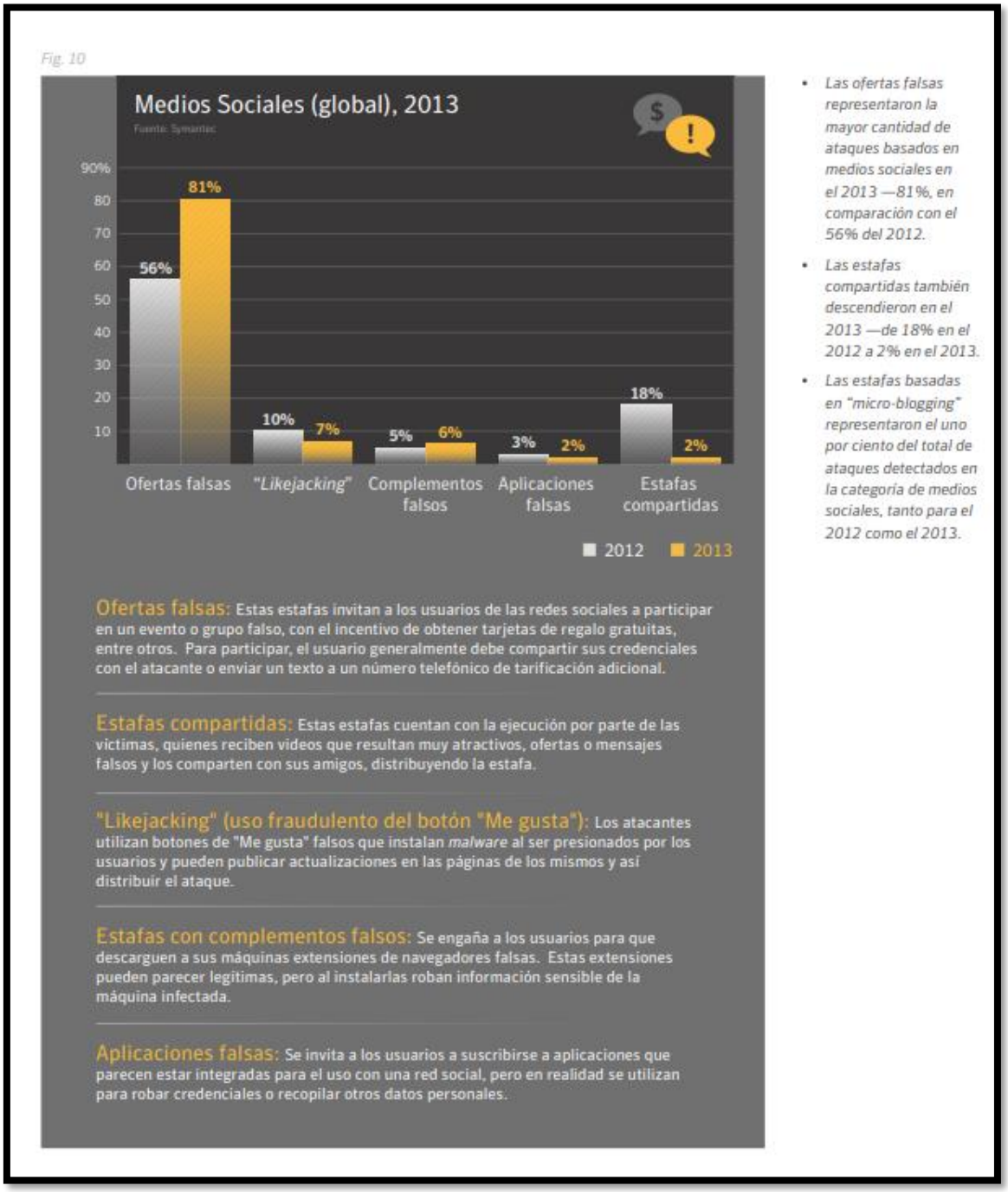
Fuente de la imagen: “Tendencias de Seguridad Cibernética en América Latina y el Caribe”. Symantec Organización de los Estados Americanos OEA (2014) https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

Ilustración 4: Cantidad total de vulnerabilidades (global) 2006-2013



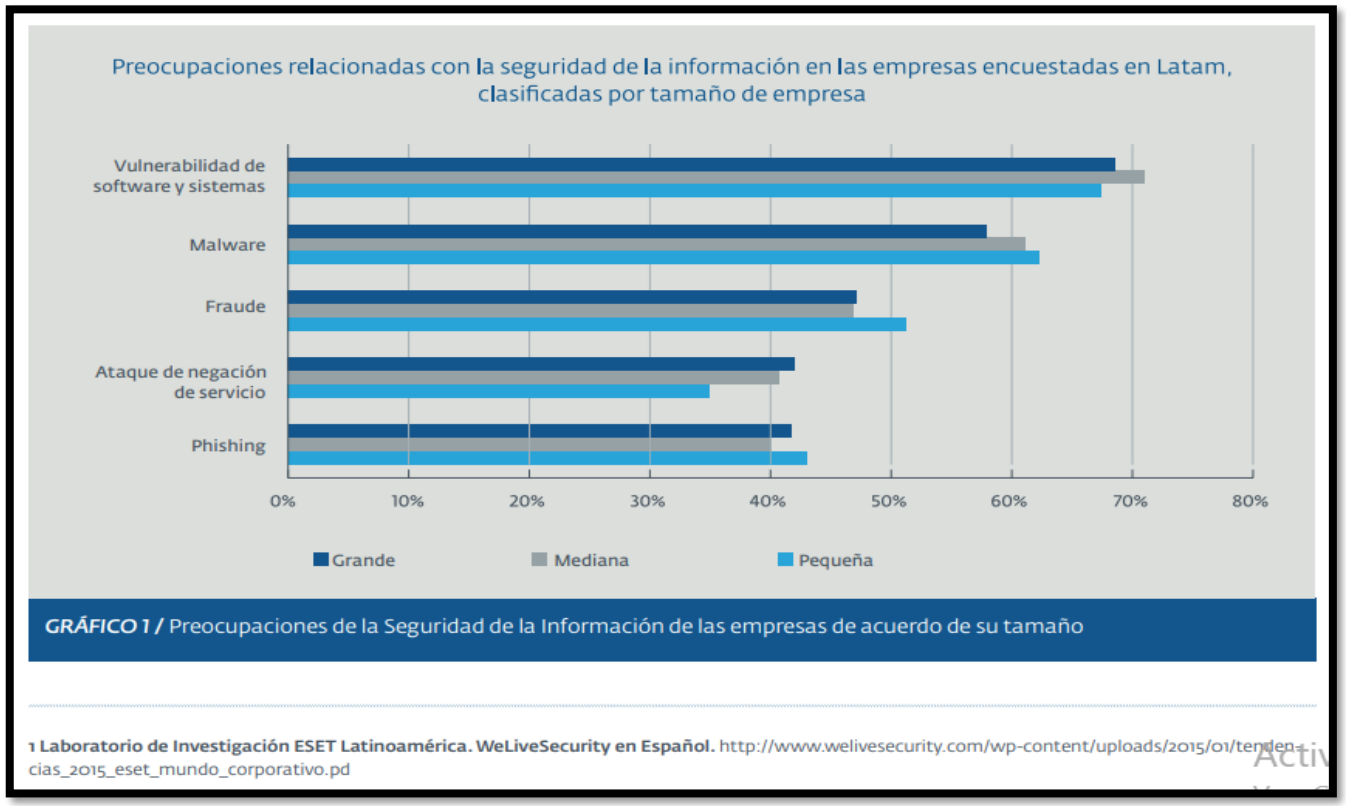
Fuente de la imagen: “Tendencias de Seguridad Cibernética en América Latina y el Caribe”. Symantec Organización de los Estados Americanos OEA (2014) https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

Ilustración 5: Medios Sociales (global) 2013



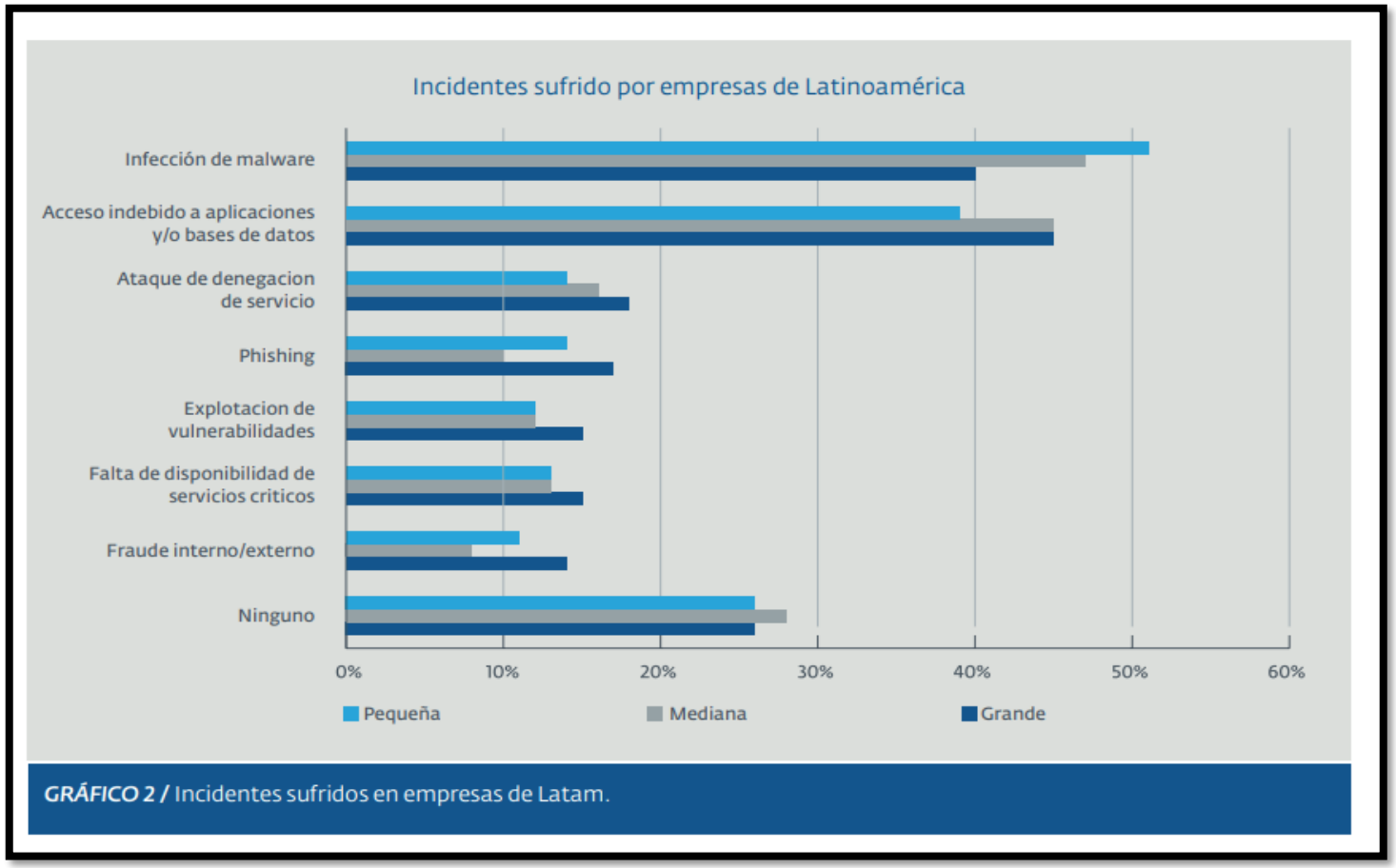
Fuente de la imagen: “Tendencias de Seguridad Cibernética en América Latina y el Caribe”. Symantec Organización de los Estados Americanos OEA (2014) https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf

Ilustración 6: Preocupaciones relacionadas con la seguridad de la información en las empresas encuestadas en América Latina, clasificadas por tamaño de empresa



Fuente de la imagen: “ESET Security Report Latinoamerica 2015”, ESET Latinoamérica (2015), https://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf

Ilustración 7: Incidentes sufridos por empresas de Latinoamérica



Fuente de la imagen: “ESET Security Report Latinoamerica 2015”, ESET Latinoamérica (2015), https://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf

Ilustración 8: Acceso Indebido

Acceso indebido

A diferencia de lo ocurrido en años anteriores, los incidentes relacionados con accesos indebidos a la información fueron los más reportados por las empresas de la región. De hecho, tan solo fueron 5 de los 14 países encuestados en los que menos de la mitad de las empresas tuvieron algún incidente de este tipo. En los 9 países restantes, más de la mitad de las empresas declararon haber tenido un incidente de este tipo.

Encontrar este incidente en la primera posición en todos los países de Latinoamérica es el reflejo de lo que se vio durante todo el año. Casos como los de Sony[5], Home Depot[6] , eBay[7] o Target[8] dejaron en evidencia lo que sucede con la información si no se toman los recaudos de seguridad adecuados.

Fuente de la imagen: “ESET Security Report Latinoamerica 2015”, ESET Latinoamérica (2015), https://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf

ÍNDICE DE ILUSTRACIONES