# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

## FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

# EL CIBERESPACIO Y LA SEGURIDAD NACIONAL DE MÉXICO.

# LA ADHESIÓN DE MÉXICO AL CONVENIO DE BUDAPEST,

# 2001-2016

TESIS

Que para obtener el título de

LICENCIADA EN RELACIONES INTERNACIONALES

Presenta

FABIOLA OLVERA CONTRERAS

Director de tesis: Dr. Roberto Carlos Hernández López


Santa Cruz Acatlán, Naucalpan, Estado de México, 2018

*A mi madre, María Contreras*
*y a mi padre, Alfonso Olvera.*

**AGRADECIMIENTOS**

Mi agradecimiento eterno a la Universidad Nacional Autónoma de México por la oportunidad de recibirme en sus aulas y que pudiera ver este sueño lograrse.

Agradezco al Doctor Roberto Hernández por la confianza y paciencia para dirigir esta tesis y por compartir conmigo todos sus conocimientos metodológicos que me permitieron sostener, de principio a fin, este trabajo.

Muy en especial, agradezco al Maestro Isaac Morales por haber depositado la primera semilla de confianza en mí, por abrirme la puerta del conocimiento y la investigación y por inyectarme la pasión y amor a los estudios internacionales; este trabajo y gran parte de lo que soy hoy, no hubiesen sido posibles sin la fortuna de haberlo conocido.

Mi sincera gratitud también, a la Maestra Araceli Fajardo, a los profesores Carlos González, Diego García, Cinthya Fuentes y al Doctor Alejandro Pisanty, por enriquecer mi trabajo con la amabilidad de sus lecturas y comentarios.

Gracias a mis padres, Alfonso y María, por haberme guiado hasta este momento con todo su amor y sabiduría; a Elvira por ser mi mayor ejemplo de la lucha diaria para abrirse paso en cada sendero y, a Alfonso, quien es la mayor motivación en mi vida para dejar huella. Nosotros somos testigos de que, solo con esfuerzo, los sueños se cumplen. Gracias por la fuerza de sus palabras y por el apoyo y amor que nunca se agotan.

Gracias a Reyna Olvera por su amor y cobijo y, a José E. Iturriaga, por la mejor herencia: la sed de saber.

Finalmente, gracias siempre a Luis por el momento exacto, por el apoyo y cariño incondicionales, así como la firme convicción en el último respiro; gracias también a Jessica y Miguel por su gran ayuda en los detalles finales, a Alma y Quintos por su amistad invaluable y, a mis amigos de la vida, por su aliento y tantos buenos recuerdos que tengo grabados en la memoria a lo largo de este trayecto.

**ÍNDICE**

EL CIBERESPACIO Y LA SEGURIDAD NACIONAL DE MÉXICO. LA ADHESIÓN DE MÉXICO AL CONVENIO DE BUDAPEST, 2001-2016

**ÍNDICE DE CUADROS**

## Introducción

Si algo caracteriza estos últimos lustros de la globalización, es el desarrollo de la ciencia y las tecnologías. En el marco de un mundo globalizado que se intensificó a finales de los años noventa, no solo económicamente, sino también, política, social, ecológica y culturalmente, el nuevo orden internacional se vio acentuado por la modernidad y los avances tecnológicos e hizo del mundo un espacio más interdependiente, complejo, transfronterizo e incierto.

La percepción evolutiva de un mundo con fronteras cada vez más difusas y confusas ha sido posible gracias, en gran parte, al Internet y las tecnologías de la información y comunicación (TICs); a través de ellas hemos encontrado ventajas antes impensables, como el acceso a otras latitudes, crecimiento económico y nuevas formas de compartir información, asimismo, ha fomentado el debate público y promovido libertades fundamentales de cara a lograr un desarrollo sostenible.

Sin embargo, el uso de las TICs también ha modificado el entorno de seguridad internacional, convirtiendo al mundo en un espacio cada vez más incierto e inestable; en la medida en que nos volvemos cada vez más interconectados, se multiplican e intensifican las amenazas de los delincuentes y enemigos de la paz y seguridad internacionales.

Actualmente, el ciberespacio forma parte de la nueva agenda de seguridad internacional y es un tema que nos interpela a todos; por lo que, de cara a los nuevos retos y desafíos que implica en materia de seguridad y desarrollo, es necesario que los actores involucrados fomenten la cooperación internacional y se maximicen los beneficios de la tecnología, al mismo tiempo que se reducen las amenazas.

Como estudiante de la licenciatura en Relaciones Internacionales, bajo el prudente entendimiento de que es una disciplina viva que requiere adaptación a las diversas realidades, la investigación está basada en dos aspectos fundamentales: el carácter contemporáneo del tema y su impacto.

Desde finales de los años treinta y durante el tenso clima de la Guerra Fría, que se extendió hasta los años sesenta, el estudio de la política internacional en las Relaciones Internacionales, y por tanto el de la seguridad, era visto únicamente desde la perspectiva bélica y, por ende, bajo la narrativa del realismo político.

A partir de la década de los setenta, autores como Robert Keohane O. y Joseph Nye[1] cuestionaron seriamente los estatutos del realismo y propusieron el estudio de la paz como la otra cara de la política internacional.

Para Keohane y Nye, la política mundial que marcaron las dos grandes guerras podía ser perfectamente explicada por el realismo; sin embargo, con el paso del tiempo, el mundo abrió espacio a nuevos actores y nuevos temas con grandes capacidades de poder para representar una amenaza igual o mayor que el comunismo, por lo que el realismo resultaba, no incapaz, pero sí insuficiente para explicar los nuevos tiempos.

Para dar cuenta de las nuevas circunstancias, Keohane y Nye desarrollaron su visión liberal por la importancia que depositan en el progreso gradual y en las libertades y los derechos individuales; sin embargo, a diferencia del liberalismo tradicional, el "liberalismo sofisticado", como ellos lo llamaron, no es utópico, ya que recae sobre la normatividad. Es decir que, para promover el bienestar económico y la justicia social, deben existir instituciones "sofisticadas" fundadas a través de la cooperación y que den garantía de las libertades individuales, así como rendición de cuentas.[2]

La realidad es que la seguridad militar y el uso de la fuerza no carecen de atención para la interdependencia compleja, pero si han restado eficacia en la solución de los conflictos emergentes. Hoy día, la probabilidad de enfrentar una guerra mundial

[1] La gran obra de ambos autores fue el libro *Interdependencia y poder*, considerado hoy, como un clásico de las teorías de las Relaciones Internacionales.

[2] Borja, Arturo (Compilador), *Interdependencia, cooperación y globalismo. Ensayos escogidos de Robert O. Keohane,* CIDE, México, 2009, p. 20.

como las que se han registrado en la historia es remota; pero no por ello, la seguridad nacional de los estados deja de estar amenazada.

La información sensible de los actores, así como las estructuras críticas de los Estados, las cuales representan la vulnerabilidad de este, pueden verse amenazadas seriamente por el ciberespacio.

De acuerdo con el *Informe Global de Riesgos 2018*, del Foro Económico Mundial (WEF por sus siglas en inglés), seguido de los riesgos ambientales, los riesgos a la ciberseguridad han crecido significativamente en términos de su prevalencia, así como de su potencial disruptivo; es decir, ataques contra empresas, impacto financiero derivado de violación a sistemas llevados a cabo por *ransomware* y ataques a infraestructuras críticas.[3]

La pregunta central de esta investigación es la firma, o no, por parte de México para adherirse al Convenio sobre la Ciberdelincuencia del Consejo de Europa, también conocido como Convenio de Budapest, creado en 2001 y único tratado internacional en la materia; así como el Protocolo adicional relativo a la criminalización de actos racistas y xenófobos cometidos por medio de sistemas informáticos del 2006.

A lo largo de tres capítulos, mediante la investigación científica aplicada y el método deductivo, he construido una radiografía del ciberespacio desde la seguridad y el desarrollo por separado para, posteriormente, encontrar el punto de intersección y, con ello, sostener la hipótesis de que el Internet es una herramienta habilitadora de desarrollo y la firma del Convenio sobre la Ciberdelincuencia es incompatible con lo anterior porque concibe al ciberespacio únicamente en términos de seguridad, al mismo tiempo que genera desventajas a la soberanía del Estado mexicano, en el entendido de que establece compromisos vinculantes en detrimento de las libertades de los ciudadanos. Bajo esta hipótesis se hace el planteamiento de que el mejor camino a seguir para nuestro país es la cooperación entre estados a través

[3] World Economic Forum, *Global Risk Report 2018*, Executive Summary, Spanish, disponible en http://reports.weforum.org/global-risks-2018/executive-summary-spanish/, consultado el 18 de enero, 2018.

de foros multilaterales que promuevan los usos pacíficos y de desarrollo que traen consigo el Internet y las TICs, al tiempo que puedan generarse estrategias capaces de prevenir, contener y mitigar las amenazas provenientes.

Para ello, el primer capítulo se divide en cuatro partes. La primera de ellas responde al estado del arte desde el abordaje del tema en las investigaciones de la Universidad Nacional Autónoma de México (UNAM). Fueron seleccionadas cinco investigaciones de la colección de tesis de la Biblioteca Central de la UNAM como eje comparativo en cuanto a las teorías de las RR.II.; sin embargo, es importante señalar que este apartado enciende el botón de alarma sobre el número tan bajo de investigaciones que analizan, con rigor académico la problemática y las consecuencias directas del ciberespacio a la seguridad nacional. Si se ingresa como criterio de búsqueda la palabra "ciberseguridad" únicamente se encuentran 5 títulos, mientras que de la palabra "ciberespacio" encontramos 21. De las 26 tesis y tesinas, 11 son aplicadas desde la disciplina de las RR.II., seguidas por 5 de Periodismo y Ciencias de la comunicación y 4 de Docencia y Pedagogía.[4]

En la segunda parte de este capítulo se realiza un esbozo histórico del mundo después de la Guerra Fría y el nacimiento del nuevo milenio que intensificó los procesos de globalización y, convirtió las TICs y el Internet en la herramienta más poderosa de nuestros tiempos. A partir de esto se explica cómo los avances tecnológicos a lo largo de la historia han modificado nuestras vidas y traído mejoras, pero también desventajas, además de que cada vez ocurren de manera más sorpresiva y limitan nuestra capacidad de respuesta.

Posteriormente se analiza el ciberespacio desde los dos extremos: como amenaza a la seguridad nacional y como plataforma habilitadora de desarrollo. Se describen casos como los *malware*, la militarización del ciberespacio, *Wikileaks* y *Anonymous*; asimismo, se mencionan las innovaciones actuales derivadas de Internet, como el

[4] Número de títulos por disciplina: Relaciones Internacionales (11), Periodismo y Comunicación (5), Docencia y Pedagogía (4), Derecho (1), Geografía (1), Arquitectura (1), Antropología (1), Lengua y literatura modernas (1), Sociología (1).

*cloud computing*, la web en tiempo real, geolocalización, realidad aumentada y el internet de las cosas.

En la tercera parte se señala la evolución del concepto de seguridad, desde su acepción tradicional-militar, definida en términos de "poder duro", para dar paso, a través de temas como la pobreza, los refugiados, la migración, el cambio climático, la escasez de alimentos, las epidemias, etc., al concepto de seguridad humana y, a partir de ello, al estudio de la seguridad vista también en términos de seguridad.

Finalmente, este capítulo plantea la relación que existe entre la teoría de la interdependencia compleja y los temas de seguridad actuales; asimismo, se contrasta el concepto de poder, visto desde el realismo y el idealismo, para redefinirse con la interdependencia compleja.

Por su parte, en el capítulo dos se describe la situación actual del debate internacional en torno a la ciberseguridad. Dadas las características del ciberespacio y los diversos actores e intereses que convergen dentro de él, la regulación del mismo ha resultado bastante difícil, por lo que, en un primer ejercicio, se describe el proceso evolutivo de una norma y, en el caso del ciberespacio específicamente, los aspectos que deben ser considerados en la mesa de negociación que, de acuerdo con Richard A. Clarke, son: gobernanza de Internet, libertad en Internet, privacidad en línea, ciberespionaje, cibercrimen y ciberguerra.[5]

Teniendo en cuenta los aspectos anteriores, se ha desarrollado el debate internacional desde dos grupos: los esfuerzos internacionales dentro del marco de Naciones Unidas y los que están fuera de este marco. Ejemplos del primero son: el Grupo de Expertos Internacionales de Naciones Unidas, la Cumbre Mundial de la Sociedad de la Información y el Código Internacional de Conducta para la Seguridad de la Información. Éste último es un acuerdo regional por parte de los países

[5] Clarke, Richard A., *Securing Cyberspace Through International Norms. Recommendations for Policymakers and the Private Sector*, Good Harbor Security Risk Management, LLC., Washington D.C.

miembros de la Organización de Cooperación de Shanghái, pero se incluye en este grupo porque ha sido presentado ante Naciones Unidas.

En el segundo grupo, podemos encontrar los esfuerzos llevados a cabo por el Consejo de Europa mediante el Convenio de Budapest, la Conferencia Global sobre el Ciberespacio y los esfuerzos de la Organización de Estados Americanos a través del Comité Interamericano contra el Terrorismo.

Por último, el capítulo tercero describe el Convenio de Budapest y la relación que guarda con México. Como se mencionó, el Convenio de Budapest se firmó en 2001 y México fue invitado a adherirse en 2007; sin embargo, 10 años después, el gobierno mexicano aún no lo ha firmado, a pesar de haber manifestado estar en consonancia con los estándares y principios contenidos en el Convenio.

Asimismo, se describen los procesos que México lleva a cabo, paralelamente, en materia de ciberseguridad a nivel nacional, regional e internacional, para poder encontrar las posibles razones por las que no se ha llevado a cabo la firma, como el tiempo que implica llevar a cabo la armonización de leyes.

Finalmente, se busca demostrar la utilidad de aplicación de los postulados de Keohane y Nye en el ciberespacio y, a partir de ellos, explicar las ventajas y desventajas que traería para México la firma del Convenio de Budapest, así como las alternativas que tiene nuestro país para fortalecer la cooperación internacional en aras de mantener la seguridad en el ciberespacio.

## CAPÍTULO 1. Marco teórico-conceptual. Antecedentes, conceptos y la relación entre el ciberespacio, el desarrollo y la seguridad nacional.

### 1.1. El ciberespacio y su tratamiento académico.

La penetración de Internet a nuestras vidas o, visto de otro modo, de nosotros en él ha aumentado a una gran velocidad y sin precedentes. Se prevé que, para finales de 2019, el 50% de la población mundial tendrá conexión a Internet; sin embargo, aproximadamente 3,800 millones de personas seguirán "desconectados" y sin poder beneficiarse de las ventajas de este mundo digital en expansión.[6]

En México, de acuerdo con la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares 2017 (ENDUTIH 2017) que realiza año con año el INEGI desde 2001,[7] el número de usuarios de Internet para 2017, fue de 71.3 mexicanos, lo que corresponde al 63.9% de la población nacional y 5.8 millones más que en 2016.[8]

Lo anterior ha generado que el tema sea prioridad en la agenda de seguridad nacional por el secretario de la Defensa Nacional, el general Salvador Cienfuegos Zepeda, quien declaró que: "los riesgos que vemos hoy son los desastres naturales, la delincuencia organizada, lo que hoy se conoce como ciberseguridad, o ciberataques, terrorismo, el tráfico de personas, de flujos migratorios…"[9]

---

[6] ITU, "Comisión de la Banda Ancha de las Naciones Unidas fija objetivos mundiales para poner en línea a 3800 millones de habitantes desconectados", Comunicado de Prensa, 23 de enero 2018, disponible en, https://www.itu.int/es/mediacentre/Pages/2018-PR01.aspx, consultada el 23 de enero 2018.

[7] Desde el 2001 hasta el 2014 se llamaba Módulo sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (MODUTIH), pero a partir del 2015 y hasta hoy, se conoce como ENDUTIH. La información entre ambas no es comparable ya que, previamente, el encuestado daba cuenta desde la perspectiva de todos los miembros del hogar y ahora es desde su propia experiencia.

[8] Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares 2017, disponible en http://www.beta.inegi.org.mx/proyectos/enchogares/regulares/dutih/2017/default.html, consultada el 20 de mayo 2018.

[9] Benavides, Carlos, "Exige general Cienfuegos justicia en caso Tlatlaya", en *El Universal,* Nación, 29 de junio de 2015, disponible en http://archivo.eluniversal.com.mx/nacion-mexico/2015/exige-general-cienfuegos-justicia-en-caso-tlatlaya-1110642.html, consultada el 4 de julio de 2017.

Sin embargo, a pesar de la inmediatez y convivencia habitual de las TICs, parece que existe al mismo tiempo poco entendimiento y ocupación. Causa sorpresa la limitación de la población y el gobierno al uso de las TICs y la falta de conciencia o conciencia tardía para preocuparnos y ocuparnos de las oportunidades y desafíos que traen consigo. Como botón de muestra y con el objetivo de analizar cómo se aborda el tema desde la investigación académica, dentro de la colección de tesis de la UNAM, únicamente existen 26 títulos que refieren al ciberespacio y la ciberseguridad y, la mayoría fueron escritas entre 2016 y 2018; es decir, muy pocas y muy recientes, sin embargo, es alentador observar un crecimiento en la importancia e interés colectivo al tema referido y desde diversas disciplinas como las Ciencias de la Comunicación, la Pedagogía, el Derecho y las Relaciones Internacionales; de esta última, se seleccionaron las siguientes 5 para el análisis comparativo:

1. Palabra clave: ciberespacio.
   Título: La organización internacional ante el desarrollo y regulación del ciberespacio. Inserción de México en la Internet. Año: 2001.[10]

Es una gran investigación y va muy de la mano con el planteamiento del Internet visto desde las mejoras que supone al desarrollo; además, fue realizada en la misma fecha que el Convenio de Budapest, lo que genera un contexto histórico del mundo y de México en esa época.

Se centra en seis organizaciones internacionales:

>Unión Internacional de Telecomunicaciones, UIT.
>Organización para la Cooperación y el Desarrollo Económicos (OCDE)
>Acuerdo de Cooperación Asia-Pacífico (APEC)
>Organización Internacional de la Normalización (ISO por sus siglas en inglés)

[10] Villanueva Romero, Sandra, "La Organización Internacional ante el desarrollo y regulación del ciberespacio. Inserción de México en la Internet", Director: Mtro. Juan Carlos Velázquez Elizarraras, Universidad Nacional Autónoma de México, UNAM, Facultad de Ciencias Políticas y Sociales, 2001.

>Asociación Hispanoamericana de Centros de Investigación y Empresas de Telecomunicaciones (AHCIET)

>Comisión Reguladora de Telecomunicaciones (REGULATEL) de Colombia

Se realiza un análisis minucioso para conocer su función y actividad en la materia, al mismo tiempo que estudia los Grupos de Trabajo y recopila experiencias de otros países para explicar, a través de estas, cómo podría México hacer frente a los beneficios que otorga el Internet y que todos, o la mayoría de los mexicanos, puedan gozar de ellos. Los criterios de selección se deben a que, para la autora, reúnen a todos los actores involucrados, realizan investigaciones específicas mediante grupos de trabajo, recopilan experiencias de diferentes países, abordan el tema "Internet" y a que derivado de que los miembros de algunas de ellas, como APEC, pertenecen a zonas geográficas específicas, la investigación se ve enriquecida por las diferencias económicas, culturales y sociales entre ellos. Asimismo, analiza la historia de las comunicaciones en México y su adaptación a ellas para conocer el estado del sector de telecomunicaciones en México y su desarrollo.

El objetivo principal de la investigación es generar una propuesta para México basada en la cooperación, el trabajo conjunto e iniciativas regionales, para lograr el acceso de todos los mexicanos al ciberespacio, mediante la amplia difusión de los beneficios y el desarrollo que conlleva y, finalmente, crear un código de conducta como intento e inicio de un marco regulatorio.

Rescato la aportación de la OCDE al debate internacional que se suscita en ese momento histórico específico y que hace eclosión en tres modelos de regulación:[11]

>Modelo de mercado: Basado en la premisa de que se necesita la confianza del consumidor, para mantener la relación con el cliente, ya que, con el flujo libre de información, los consumidores son más selectos en ese ambiente que a la vez es más competitivo. Los consumidores ya o tienen una opción, ni dos, sino miles.

[11] *Ibídem,* p. 88.

>Modelo de regulación gubernamental: Su argumento principal lo constituye el hecho de que Internet se encuentra en una fase temprana de desarrollo, por lo que sería prematuro imponer regulaciones gubernamentales rígidas, cuando éstas pudieran obstaculizar el desarrollo tecnológico.
>Modelo de autorregulación: Al parecer es el camino que más simpatizantes tiene, dado que en él se emplea la especialización de las industrias de las telecomunicaciones, la informática y las computadoras, y se toman en cuenta los avances acelerados en el rubro.

De los anteriores, el modelo de regulación gubernamental que plantea la OCDE es probablemente el que, después de 17 años, mejor representa el panorama de México en la actualidad.

Reitero la gran investigación que me pareció, tiene un enfoque muy claro sobre lo que implica el Internet para el desarrollo, no sólo del individuo o de un Estado, sino del mundo; sin embargo, es reducido el análisis sobre el crimen o los actos ilícitos que se cometen a través de él y que no debemos ignorar; es necesaria una aproximación desde ambos extremos para encontrar un balance hacia una regulación íntegra; pero, en general, conjuga perfectamente con mi análisis acerca de hacer uso de los foros de cooperación, reducir la brecha de acceso, hacer expansivos los dividendos digitales y emplear una regulación más flexible.

2. Palabra clave: ciberespacio. Disciplina: Relaciones Internacionales.
   Título: La regulación jurídica internacional del Ciberespacio. Terrorismo Informático. Año: 2007.[12]

Es una investigación basada en el ámbito del delito y la regulación del ciberespacio a través del poder duro; es decir, la ley. En el primer capítulo se define al delito desde el ámbito legal y doctrinario; posteriormente se dan los conceptos y antecedentes del Internet, así como los delitos informáticos, su clasificación y

[12] Morales Galván, Roxana Fabiola, "La regulación jurídica internacional del ciberespacio. Terrorismo informático.", Director: Mtro. Juan Carlos Velázquez Elizarrarás, Universidad Nacional Autónoma de México, UNAM, Facultad de Ciencias Políticas y Sociales, 2007.

características para, en el tercer capítulo, enfocarse en el terrorismo y el terrorismo informático, haciendo mención también, a la piratería informática. Finalmente, en el último capítulo se lleva a cabo un ejercicio de comparación legislativa entre diferentes países de diversas latitudes.

A manera de sinopsis, la autora establece que las medidas de regulación se han llevado a cabo en el terreno nacional sin repercusiones en la escala global, lo que genera discontinuidad en la legislación, inseguridad jurídica y la inaplicación de muchas de las normas de regulación.

La hipótesis por comprobar es que un marco normativo y legal que comprenda "todos" los delitos, prevendrá las situaciones conflictivas que se generen en él; asimismo, dichas estrategias deben ser concebidas desde toda la estructura del Estado-Nación y sustentadas en la inteligencia.[13]

En mi opinión, es una tesis que podría sustentarse de manera más óptima desde la disciplina del Derecho; asimismo, la encuentro limitada en recursos y, por lo tanto, con la puerta demasiado abierta para debate ya que no contempla a los demás actores que forman el ciberespacio y, salvo una ligera mención a la libertad de expresión, no menciona derechos humanos.

3. Palabras clave: ciberespacio y ciberseguridad. Disciplina: Relaciones Internacionales.
   Título: La delincuencia organizada en el ciberespacio, en el marco de la sociedad de la información y el conocimiento: la estrategia de ciberseguridad en México (2013-2015). Año: 2016.[14]

Es una investigación reciente en la que destaco en primer lugar, que en las variables de estudio se incluyen ciberespacio y ciberseguridad, conjugadas perfectamente

[13] *Ibídem*, p. 8.
[14] Jiménez Martínez, Andrés Moisés Ramón, "La delincuencia organizada en el ciberespacio, en el marco de la sociedad de la información y el conocimiento: la estrategia de ciberseguridad en México (2013-2015).", Director: Dr. Alejandro Chanona Burguete, Universidad Nacional Autónoma de México, UNAM, Facultad de Ciencias Políticas y Sociales, 2016.

con una tercera variable que es la delincuencia organizada; esta última es el tema central y me parece muy oportuna porque es una de las grandes dolencias de México.

El autor hace una descripción muy completa sobre cómo la delincuencia organizada se ha sofisticado haciendo uso de las TICs y que las acciones por parte del gobierno para enfrentarla son insuficientes.

Propone, por lo tanto, incorporar más instituciones y coordinar esfuerzos nacionales, así como destinar recursos económicos, humanos y técnicos para protegerse de la delincuencia organizada y proveer confianza a los mexicanos.[15]

Aunado a lo anterior, plantea la necesidad de una estrategia nacional de ciberseguridad en México,[16] basada en una lista de recomendaciones propuestas por la UIT y el análisis de cómo empatan con la realidad de México.

En lo que para efectos del presente trabajo atañe, es la única de las tesis seleccionadas que hace mención al Convenio de Budapest, aunque solo como fuente de referencia para enlistar y describir los delitos, así como para considerarse una directriz.[17]

Destaco, por último, la relación estrecha que señala el autor entre la seguridad y el bienestar y una frase que repite varias veces a lo largo de la investigación: “La ciberseguridad no es un fin en sí misma, sino un medio con el objetivo de construir la confianza en el ciberespacio y la meta de asegurar que la infraestructura de la información funcionará de forma fiable incluso cuando esté bajo amenaza”[18]

[15] *Ibídem*, p. 10.
[16] A partir de noviembre de 2017, México ya cuenta con la Estrategia Nacional de Ciberseguridad. Ver página
[17] *Ibídem*, p. 67.
[18] *Ibídem*, p. 105.

4. Palabras clave: ciberespacio. Disciplina: Relaciones Internacionales.
   Título: La aplicabilidad de las leyes internacionales a los ciberataques y el estatus legal de éstos en el ciberespacio: casos de estudio. Año: 2018.[19]

Estrictamente no es una tesis, sino una tesina; sin embargo, aborda uno de los temas mayormente discutidos en la mesa de los debates internacionales en cuanto al ciberespacio comprende.

Se había mencionado previamente que el estudio de la guerra y la paz internacionales ha sido por décadas el objeto de estudio de las RR.II. y esta investigación aborda el tema de la guerra dentro del ciberespacio.

Los debates al respecto han sentado sus bases en la aplicabilidad del derecho internacional en este nuevo espacio; así como las leyes de guerra, la legítima defensa, el uso de la fuerza y todo lo que este comprende.

En lo personal, es un tema de gran interés pero que definitivamente atañe a otra investigación; sin embargo, esta investigación es un primer gran acercamiento al tema para conocer, tanto los conceptos básicos, como los estudios de caso y la catalogación de los ciberataques basada en los efectos.

Dado que no existen tratados en la materia ─con excepción de Budapest─, mucho menos hay alguno que se refiera a los tiempos de guerra en el ciberespacio; por su parte, el Manual de Tallin que, aunque no es oficial y por ende no refleja la doctrina de la OTAN, se ha dedicado a tratar este tema con todo el rigor del derecho internacional.

Lo cierto es que, hasta el día de hoy, no se tiene registro de ninguna pérdida humana derivada un ciberataque. Si bien un ciberataque podría dañar lo que conocemos como estructuras críticas de información, como plantas nucleares, gaseoductos,

[19] Álvarez Díaz de Rivera, Santiago, "La aplicabilidad de las leyes internacionales a los ciberataques y el estatus legal de éstos en el ciberespacio: casos de estudio", Director: Mtro. Adolfo Arreola García, Universidad Nacional Autónoma de México, UNAM, Facultad de Estudios Superiores Acatlán, 2018.

sistemas de electricidad, etc. y desencadenar catástrofes que ocasionen pérdidas humanas, en estricto sentido, ninguna vida se ha perdido en los casos que se catalogan como “ciberguerras”.

Sin embargo, las ciberoperaciones o los ciberataques durante un conflicto armado tradicional sí son un tipo de multiplicador de fuerza y, por ende, están sujetos a la ley de conflicto armado.[20]

Para el autor, las leyes existentes son insuficientes para regular el ciberespacio y propone la creación de leyes específicas para regularlo; sin embargo, en mi punto de vista y derivado de la falta de consenso internacional en la aplicabilidad del derecho y las leyes internacionales al ciberespacio, la creación de nuevas leyes o tratados ─como Budapest─, tampoco garantizan una solución efectiva; por el contrario, sí creo que pueden adecuarse en algunos casos y bajo las coincidencias que presenta con los espacios físicos.

Existirá la necesidad evidentemente de normas que atañan exclusivamente al ciberespacio, como ocurre en otros espacios, pero en lo que al uso de la fuerza o los tiempos de la guerra supone, los alcances materializados de una ciberguerra no han sido hasta hoy superiores a los de una guerra tradicional. Considero que es un tema que debe continuar en la mesa del debate por la complejidad de este; sin embargo, reitero, es un gran acercamiento al entendimiento elemental del tema.

5. Palabras clave: ciberseguridad. Disciplina: Relaciones Internacionales. Título: La ciberseguridad en México ante desafíos y amenazas del siglo XXI. Año: 2018.[21]

Es la tesis más reciente en el catálogo de búsqueda y por ello me resulta una gran aportación comparativa. Dividida en tres capítulos, el estudio se sustenta en la teoría

[20] *Ibídem*, p. 48.
[21] Zurita Higuera, Andrés, “La ciberseguridad en México ante desafíos y amenazas del siglo XXI”, Director: Mtro. Víctor Francisco Olguín Monroy, Universidad Nacional Autónoma de México, UNAM, Facultad de Estudios Superiores Aragón.

de complejos de seguridad regional de Barry Buzan y Ole Waever, para comprobar la hipótesis de que México se encuentra en un proceso lento de desarrollo y adaptación en materia de ciberseguridad para hacer frente a los desafíos y amenazas del presente siglo.

Destaco el análisis del autor en el capítulo uno, para describir como se ha tergiversado la ciberseguridad, en el entendido de cómo se han usado las prácticas de espionaje, robo de información y violación a la privacidad en aras de mantener la seguridad nacional, cuando por sí mismas son el antítesis de seguridad; asimismo y de manera concisa, en el capítulo dos se describen los trabajos realizados por los principales organismos regionales en la materia (OTAN, UE y OEA), abarcando de esta forma una representación global importante y, finalmente, los trabajos de México en la materia desde una perspectiva individual.

Sin embargo, difiero con la hipótesis señalada, incluso recurriendo a la teoría planteada por el autor, porque México ha sido uno de los países con mayor aportación y representación en la región en temas de ciberseguridad; por otro lado, el autor señala que la Estrategia Nacional de Ciberseguridad no es suficiente por el tiempo que tarde en implementarse, así como la complejidad del tema y la rapidez con la que se desarrollan los avances tecnológicos; sin embargo, a mí me parece una aportación y un compromiso de gran alcance, dada la composición integral de esta.

En este breve ejercicio se pudo observar cómo se estudia el ciberespacio y las principales preguntas que surgen en torno a su existencia y nuestra relación con él; para continuar, se abordará el contexto “espacio”-temporal para comprender las implicaciones y necesidades actuales.

## 1.2. Retos y amenazas en el ciberespacio.

### 1.2.1. La globalización de las Tecnologías de la Información y Comunicación.

Desde muchos años atrás, la visión de los gobiernos alcanzaba límites mucho más allá del terreno local. En la década de 1970, por ejemplo, ya se hablaba de "interdependencia" y se explicaba cómo "nada de cuanto ocurra en nuestro planeta podrá ser un suceso localmente delimitado, sino que todos los descubrimientos, victorias y catástrofes, afectarán a todo el mundo…"[22]

Sin embargo, el hecho de nunca haber vivido totalmente aislados del resto del mundo a menudo se ha enmarcado en el concepto de la globalización; concepto cuya omnipresencia se manifiesta todos los días pero que aún cuesta trabajo definirla en términos monolíticos. Su sigilo y envergadura han dificultado la acepción de una sola definición; a menudo se describe de alguna forma, para más tarde notar que es eso, pero también lo otro.

La perspectiva de la globalización económica que desencadenó la apertura de Europa con la caída del Muro de Berlín representó, para la sociedad internacional, una amenaza, ya que se le otorgó, al sector empresarial, un poder tan grande de negociación política que significó un debilitamiento en las capacidades de poder de los estados. Dicho poder consistía en cuatro fundamentos según Ulrich Beck:

> En primer lugar, podemos *exportar puestos de trabajo* allí donde son más bajos los costes laborales y las cargas fiscales a la creación de mano de obra.
>
> En segundo lugar, estamos en condiciones (a causa de las nuevas técnicas de la información, que llegan a los últimos rincones del mundo) de desmenuzar los productos y las prestaciones de servicios, así como de *repartir el trabajo por todo el mundo*, de manera que las etiquetas nacionales y empresariales nos pueden inducir fácilmente a error.
>
> En tercer lugar, estamos en condiciones de servirnos de los Estados nacionales y de los centros de producción individuales en contra de ellos mismos y, de este modo, conseguir "pactos globales" con vistas a unas condiciones impositivas más suaves y unas infraestructuras más favorables; asimismo, podemos

[22] Beck, Ulrich, *¿Qué es la Globalización?, Falacias del globalismo, respuestas a la globalización*, Paidós, España, 1998, p. 36.

> "castigar" a los Estados nacionales cuando se muestran "careros" o "poco amigos de nuestras inversiones".
>
> En cuarto, y último, lugar, podemos distinguir automáticamente en medio de las fragosidades –controladas- de la producción global entre *lugar de inversión, lugar de producción, lugar de declaración fiscal y lugar de residencia,* lo que supone que los cuadros dirigentes podrán vivir y residir allí donde les resulte más atractivo y pagar los impuestos allí donde les resulte menos gravoso.[23]

Esta perspectiva económica, con frecuencia, ha socavado la importancia del factor histórico y, sobre todo, político del concepto; sin embargo, si privilegiamos estos factores como parte de un todo, podríamos tener un concepto más exacto y con un espectro de entendimiento más amplio.

En primera instancia, convendría diferenciar la globalización del globalismo y la globalidad. El globalismo refiere a "la concepción según la cual el mercado mundial desaloja o sustituye al quehacer político; es decir, la ideología del dominio del mercado mundial o la ideología del liberalismo."[24] Para el globalismo, las dimensiones política, social, ecológica y cultural son subalternas de la dimensión económica. Ulrich Beck habla de un imperialismo económico, donde el mismo Estado es visto como una empresa y, por tanto, debe otorgar al núcleo económico, todo lo necesario para lograr sus objetivos; es decir, el mercado mundial desaloja o sustituye al quehacer político.

Por su parte, el concepto de globalidad es más incluyente; hace alusión a las redes de relaciones económicas, políticas, culturales, ambientales y sociales que se tejen a nivel global y regional, así como la lógica que sostienen las diferentes dimensiones entre sí y en mutua interdependencia. Es importante resaltar que, si no el concepto como tal, la práctica data desde hace muchos años. Como botón de muestra, podemos referirnos a la globalidad ambiental, cuyos cambios han afectado el flujo de pueblos enteros desde hace millones de años y cuyas consecuencias marcaron las primeras prácticas de migración. Asimismo, desde la antigüedad se comprobó que la tesis de los espacios cerrados es ficticia[25] y vivimos en una sociedad mundial,

[23] *Ibídem,* p. 18.
[24] *Ibídem*, p.27.
[25] *Ibídem,* p.28.

la cual, en palabras de Martin Albrow, podemos entenderla como una pluralidad sin unidad, ya que las relaciones que se gestan dentro de esta sociedad no están integradas en la política del Estado-nación ni están determinadas a través de este.

> La globalidad se define como un estado o una condición del mundo en donde existen redes de interdependencia que alcanzan distancias multicontinentales, vinculadas a través de los flujos y las influencias de los capitales y de las mercancías, de la información y de las ideas, de las personas y del trabajo, así como de sustancias que revisten importancia ambiental y biológica (como la lluvia ácida y los agentes patógenos). La globalización y la desglobalización se refieren al aumento o a la disminución de la globalidad.[26]

Por tanto, Beck define la globalización como los "procesos en virtud de los cuales los Estados nacionales soberanos se entremezclan e imbrican mediante actores transnacionales y sus respectivas probabilidades de poder, orientaciones, identidades y entramados varios."[27]

A pesar de que no existe una definición unánime, a finales de los años noventa, cuando la globalización se convirtió en un cliché debido a la reconfiguración de la política internacional tradicional de los Estados nación, que se suplantó en un nuevo orden internacional basado en la transfronterización de la economía, se definieron ciertos criterios clave para abordar el tema:

1. Se ha tomado conciencia de que el fenómeno abarca las distintas manifestaciones de existencia de lo social y que, por ende, no debe visualizarse sólo desde el un ángulo en particular. La globalización es un fenómeno eminentemente global.
2. Más conveniente que hablar de globalización, deberíamos referirnos a globalizaciones.
3. Derivado de lo anterior, si lo que genéricamente definimos como globalización debe visualizarse en una perspectiva plural, no siempre estas diferentes globalizaciones transcurren en el mismo sentido y con la misma intensidad.
4. Como fenómeno global, afecta con diversos grados de intensidad y bajo distintas modalidades a todos los habitantes del planeta.
5. No obstante, las asociaciones que se han producido entre ciertos discursos y la difusión de las tendencias globalizadoras, sean estas favorables o contestatarias de la globalización, los analistas sociales cada vez más se inclinan por una interpretación que deja atrás a la percepción de que esto sería

[26] Robert O. Keohane y Joseph Nye, "Poder, Interdependencia y Globalismo", en Borja, Arturo (Compilador), *Interdependencia, cooperación y globalismo. Ensayos escogidos de Robert O. Keohane,* CIDE, México, 2009, p. 376.
[27] Beck, Ulrich, *Op. Cit* .p. 29.

una influencia externa para entender la globalización como un conjunto de transformaciones que se expresan y realizan en el plano global, regional, nacional e incluso local. Esta noción de globalización también introduce un importante matiz que permite diferenciarla de otras nociones análogas como la internacionalización y la interdependencia. Se asemeja en tanto que alude a una mayor intensificación en los niveles de interacción e intercambio entre actores próximos o a veces distantes, pero se diferencia de ellos en la medida en que alude a la creación de una nueva cualidad porque transforma los fundamentos que hacen posible la existencia de lo global.

6. La globalización, no obstante, su aceleración en determinados momentos como resultado de la introducción y masificación de ciertas tecnologías, ha sido promovida básicamente por la determinación que en este sentido, han tomado algunos actores políticos y económicos.
7. La globalización trae consigo efectos positivos y negativos. Entre los primeros se observa que para los países del sur la actual globalización abre mayores posibilidades para desarrollar actividades en diferentes frentes, lo que les garantiza mejores condiciones de negociación que las que existían en épocas anteriores. Entre los segundos, se amplía el consenso en torno a la necesidad de generar mecanismos de gobernabilidad o regulación de las tendencias globalizadoras porque se han fragilizado los mecanismos de respuesta ante las turbulencias que se presentan en el plano local.[28]

Podemos resumir, de acuerdo con Beck, que la globalización es un fenómeno eminentemente global y plural, que abarca distintas esferas, por lo que lo correcto debería ser hablar de "globalizaciones"; asimismo, estas diferentes esferas mantienen ritmos e intensidades variables y no necesariamente dependientes.

Probablemente, la globalización económica se intensifique al mismo tiempo que las demás áreas se encuentren en un proceso de desglobalización; sin embargo, lo que Hugo Fazio explica, es que, con la caída del Muro de Berlín, las tendencias globalizadoras se sincronizaron a escala planetaria y es por ello que se "alimentó la idea de que la globalización estaría dando origen a una nueva época en la historia de la humanidad."[29]

La globalización, definida a grandes rasgos, como el nuevo orden tecnológico, económico y social, ha desvanecido y hecho confuso los límites de territorialidad de las naciones. Asimismo, se ha visto acentuada por la modernidad y los avances

[28] Fazio Vengoa, Hugo, *La Globalización en su historia*, Universidad de Colombia, Bogotá, 2002, pp. 18-22.
[29] *Ibídem*, p. 20.

tecnológicos, lo que nos conduce a identificar las ventajas comparativas y competitivas que ofrece la globalización, pero principalmente a prestar real atención a los nuevos desafíos e impactos que arroja.

Por ejemplo, los avances tecnológicos de los que hemos sido testigos durante el presente siglo han revolucionado el *bussiness as usual* modificando la forma en la que nos comunicamos e interactuamos; sin embargo, el hecho de que sea un fenómeno "global" no significa que se exprese de la misma manera en todas las regiones y países; lo que para algunos ha significado desarrollo, para otros ha hecho más profundas las desigualdades e injusticias.

Para su funcionamiento, la globalización hace uso de redes capaces de adaptarse y desarrollarse en un contexto evolutivo rápido de comunicación, y con ello, ha evolucionado la tecnología para así, modernizar, transformar, desarrollar y beneficiar a las personas y a las naciones. Asimismo, las Tecnologías de la Información y Comunicación (TICs), en conjunto y como parte de la globalización, han arrojado múltiples beneficios con relación a las formas de comunicación, intercambio, interacción y conexión entre las personas. Uno de estos beneficios y quizás el más significativo es el Internet, el cual constituye la base tecnológica que caracteriza la nueva era de la información, moderniza las comunicaciones y las ejecuta en tiempo real sin importar el lugar desde donde se efectúan. Es la red de comunicación global.

Para Manuel Castells, las TICs son el equivalente histórico de lo que simbolizó la electricidad en la era industrial, y a su vez, el Internet es la red eléctrica. Ha propiciado avances en las ciencias, la educación, la salud y la vida diaria; sin embargo, al ser una tecnología particularmente abierta y moldeable, se constituye por una sociedad heterogénea en constante crecimiento que no se rige bajo el esquema tradicional de territorio, gobierno, cultura, etc. y, a su vez, ha ocasionado un adelgazamiento de las capacidades intrínsecas del Estado, lo que dificulta su control y, por ende, la convierte también en una herramienta potencialmente peligrosa y altamente costosa en términos económicos y sociales.

### 1.2.2. Internet y ciberespacio.

El Internet es un medio de comunicación que permite, por primera vez, la comunicación masiva en tiempo escogido y a una escala global.[30]

Funciona como una red, es decir, posee un conjunto de nodos interconectados, cuya flexibilidad y adaptabilidad le permiten ser un sistema de comunicaciones y una forma organizativa al mismo tiempo. Alrededor de él se ha gestado un nuevo espacio virtual, constituido por una nueva sociedad y nuevas formas de interacción sin precedentes; es decir, el ciberespacio.

La historia del Internet es un proceso que data desde la década de los 60, cuando el Departamento de Defensa de los EE.UU., con varias universidades, como la Universidad de California en los Ángeles, el Stanford Research Institute (SRI), la Universidad de California en Santa Bárbara y la Universidad de Utah, crearon ARPANET (Advanced Research Projects Agency Network, por sus siglas en inglés), y se extiende hasta la década de los 90 con el auge del *World Wide Web* (www).[31]

ARPANET propició la capacidad de introducirse a varios ordenadores y, a su vez, establecer una conexión entre ellos. El objetivo principal era alcanzar un nivel tecnológico superior al de la Unión Soviética y contrarrestar un eventual ataque nuclear mediante un sistema de comunicaciones militar y de investigación avanzada. Como parte del proceso evolutivo original, con el fin de buscar y compartir información, se implementaron mensajes electrónicos directos, pero más tarde, se logró el envío masivo de información entre varios usuarios, es decir, las listas de correo electrónico.

Las listas de correo electrónico facilitaron la creación de grupos con intereses afines –práctica vigente en la actualidad–, la información se enviaba a un punto central y posteriormente se reflejaba a todos los usuarios del grupo; asimismo, permitían que

[30] Castells, Manuel, *La Galaxia Internet*, Plaza y Janés, España, 2001, p.16.
[31] *Ídem.*

los diferentes usuarios pudieran responder y, por tanto, crear canales de comunicación entre todos.

Para que la red de redes fuese posible, es decir, para que las redes de ordenadores pudieran comunicarse entre ellas, era necesaria la creación de protocolos de comunicación estandarizados, para lo que se creó lo que actualmente conocemos como TCP/IP; es decir, el Protocolo de Control de Transmisión (TCP: *Transmission Control Protocol*) y el protocolo interredes.[32]

A partir de entonces y tras varias modificaciones, se fue configurando el Internet; sin embargo, para que llegara a ser lo que conocemos hoy día, en 1990, Tim Berners-Lee, creó la *World Wide Web,* un sistema de hipertexto cuya funcionalidad es la de un navegador o buscador; para ello, requiere de un software, llamado URL, el cual permite intercambiar información desde cualquier ordenador conectado a Internet.[33]

Eventualmente, surgieron un sinfín de modificaciones y varias empresas lograron la creación de diferentes navegadores. En 1995, Microsoft incluyó junto a su software *Windows 95*, el *Internet Explorer*, cuyo éxito subsiste hasta hoy, y es por ello, que a pesar de que sus inicios informáticos y tecnológicos comenzaron en la década de los sesenta desde la esfera académica y gubernamental, para el resto del mundo, incluidas las empresas, inició en 1995.[34]

Contrario al lento proceso de creación del Internet, el proceso de expansión y desarrollo fue bastante rápido. Las empresas pronto buscaron las herramientas y medios para adaptarse a las nuevas tecnologías y con ello generar crecimiento relevante en el mercado; por su parte, la sociedad civil fue adaptándose poco a poco hasta constituir una sociedad digital sin precedentes.

[32] *Ídem.*
[33] *Ídem.*
[34] *Ídem.*

Durante el primer año del uso generalizado del *World Wide Web* (1995), la cifra de usuarios en Internet oscilaba los 16 millones en todo el mundo. A principios de 2001, había más de 400 millones, 1.000 millones de usuarios para 2005[35] y para 2017, el número de usuarios de banda ancha mundial se estimaba alcanzar los 4.3 billones de personas, lo que corresponde al 48% de la población mundial.[36]

Alrededor del periodo de transición, aceptación y adaptabilidad de grandes sectores de la sociedad internacional al Internet, hizo eclosión, también, la preocupación con respecto a sus límites. En 2010, *The Economist* clasificó al ciberespacio como el quinto dominio de guerra junto a la tierra, el mar, el aire y el espacio,[37] y en ese mismo año, la Organización de las Naciones Unidas (ONU) creó el primer Grupo de Expertos Gubernamentales (GGE por sus siglas en inglés) encargados de estudiar las amenazas que se gestan en el ciberespacio con el fin de establecer medidas que garanticen la seguridad del mismo.

Existen grandes similitudes entre el ciberespacio y el resto de los espacios físicos, sin embargo, también existen grandes diferencias que lo convierten en un escenario particularmente interesante.

La seguridad y el desarrollo, desde sus acepciones tradicionales hasta las más extensas, han sido pilares en el estudio del ciberespacio. La crisis del Estado-nación, como consecuencia de la globalización, ha relativizado el concepto de poder y lo ha redistribuido entre más partes, como las Organizaciones Intergubernamentales (OIGs), Organizaciones no Gubernamentales (ONGs), firmas multinacionales e, incluso, actores atípicos como grupos terroristas o del crimen organizado; dificultando, así, las negociaciones, en el entendido de que ya existen más intereses en juego. Por si lo anterior fuese poco, la ausencia de fronteras en el

[35] *Ídem*.
[36] International Telecommunication Union, ITU, *ITU releases 2017 global information and communication technology facts and figures,* Ginebra, 31 de julio, 2017, disponible en https://www.itu.int/en/mediacentre/Pages/2017-PR37.aspx, consultada el 02 de febrero, 2018.
[37] *The Economist,* "Cyberwar. War in the fifth domain", Volume 396, number 8689, July 3rd-9th 2010.

ciberespacio ha reducido a cero las capacidades de ejercer control de los estados sobre algún territorio y extrapolado la acción de cualquier usuario dentro de él.

En lo que concierne al desarrollo, es innegable que el ciberespacio es una plataforma de desarrollo sin precedentes; por tanto, hay que ser estrictamente cautelosos al establecer medidas de seguridad si no se quiere frenar el acceso y esparcimiento del mismo ni violar derechos fundamentales.

### 1.2.3. El ciberespacio como amenaza a la seguridad nacional.

El mundo, hoy en día, tiene una creciente dependencia a las TICs; sin embargo, esta dependencia, de acuerdo con el uso que se le dé, puede servir como trampolín al desarrollo o un factor clave para generar mayor vulnerabilidad, conflictos y, por ende, inseguridad.

Los ciberataques hoy en día están catalogados como una de las principales amenazas a la seguridad de los estados y de las principales organizaciones internacionales como la Organización del Tratado del Atlántico Norte (OTAN) y la Unión Europea (UE), por la flexibilidad y adaptabilidad del Internet; pero, principalmente, por el impresionante incremento de usuarios en la red.

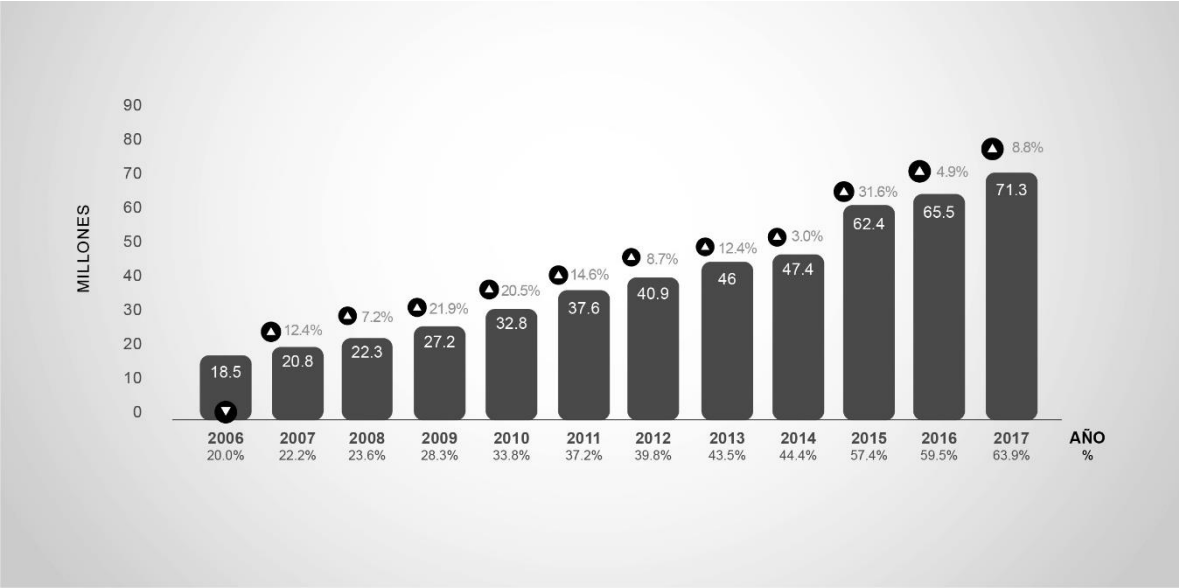
De acuerdo con los datos de la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés), entre el 2000 y 2015 la penetración de usuarios a Internet se multiplicó por 7, pasando de 6.5% al 43% de la población mundial, siendo los países en desarrollo los que mayor número de usuarios habían aportado a este índice.[38] Para 2017, las cifras registradas por el mismo organismo, indican una penetración de usuarios del 48% de la población mundial; sin embargo el aspecto a destacar es el incremento en la presencia de la población joven (15-24 años). En los países desarrollados el 94% de los usuarios de Internet se encuentran en este rango de edad, comparado con el 67% de los países en desarrollo y el 30% de los países

[38] International Telecommunication Union, ITU, *La UIT publica los datos sobre las TIC de 2015,* Ginebra, 26 de mayo, 2015, disponible en http://www.itu.int/net/pressoffice/press_releases/2015/17-es.aspx#.V-laZYjhDIU, consultada el 16 de septiembre, 2016.

menos desarrollados. Asimismo, de la población total de jóvenes que están en línea (830 millones), el 39% están en China e India.[39]

En el caso de México, de acuerdo con cifras del Instituto Nacional de Estadística y Geografía (INEGI)[40] y de la Asociación de Internet,[41] en 2017, México alcanzó el 63.9% de penetración de usuarios de Internet entre la población de personas mayores a 6 años.

**Cuadro 1. Usuarios de Internet en México, 2006 – 2017.[42]**




[39] ITU (2017), *Op. Cit.*

[40] INEGI, "Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares 2017", disponible en http://www.beta.inegi.org.mx/proyectos/enchogares/regulares/dutih/2017/, consultada el 26 de septiembre, 2017.

[41] Asociación de Internet. MX, *13° Estudio sobre los Hábitos de los Usuarios de Internet en México 2017*, 08 de agosto, 2017, disponible en, https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/13-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2017/lang,es-es/?Itemid=, consultada el 18 de septiembre, 2017.

[42] De 2006 – 2014: INEGI. Modulo sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares, MODUTIH.
De 2015 – 2017: INEGI. Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en Hogares, ENDUTIH.

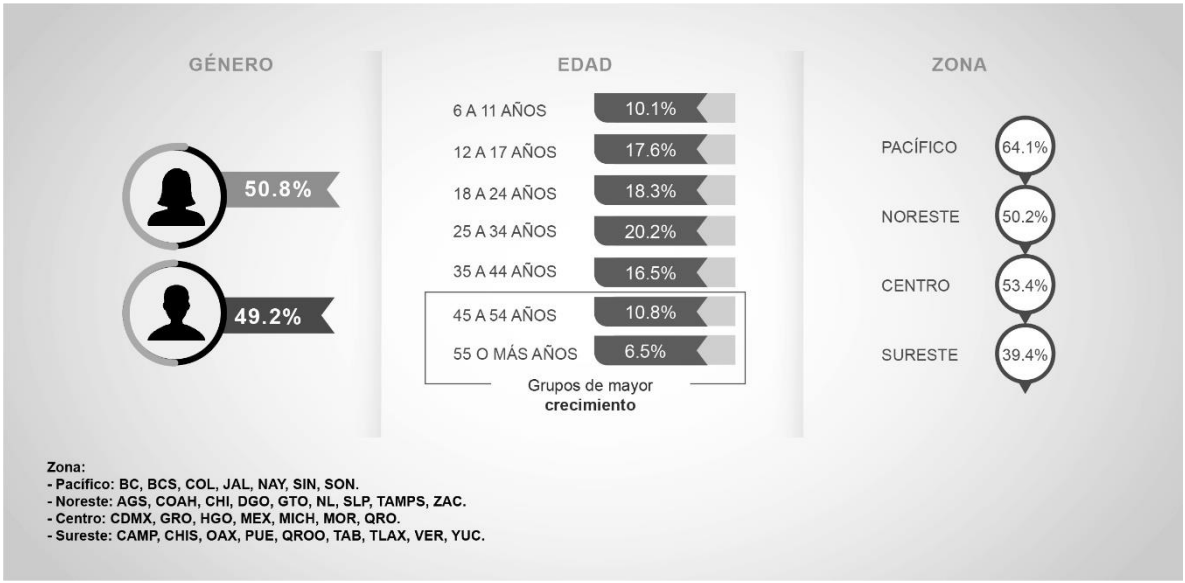
**Cuadro 2. Usuarios de las Tecnologías de la Información y Comunicación, 2017.[43]**

| AÑO | USUARIOS DE INTERNET | | USUARIOS DE COMPUTADORA | | USUARIOS DE TELÉFONO MÓVIL | |
|---|---|---|---|---|---|---|
| | ABSOLUTOS | % | ABSOLUTOS | % | ABSOLUTOS | % |
| 2017 | 71,340,853 | 63.9 | 50,591,325 | 45.3 | 80,721,678 | 72.2 |

*Cifras correspondientes al mes de mayo.

En el siguiente cuadro podemos observar la distribución por género, edad y región del total de usuarios en 2017:

**Cuadro 3. Perfil del internauta mexicano, 2017.[44]**




[43] INEGI. Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en Hogares, ENDUTIH.
[44] *Ibídem.*

En cuanto al género, las cifras son muy cerradas; las mujeres tienen mayor acceso solo por un .8% por encima de los hombres; sin embargo, aun cuando no es objetivo de esta investigación, el tema del género es obligado mencionar. Aunque el acceso sea notoriamente igual para hombres y mujeres, la equidad de género y sus consecuencias es una lucha que debe mantenerse en el ciberespacio. Los discursos y acciones que vulneran, discriminan y violentan a las mujeres han sido reproducidos también en los espacios virtuales y a través de las TICs.

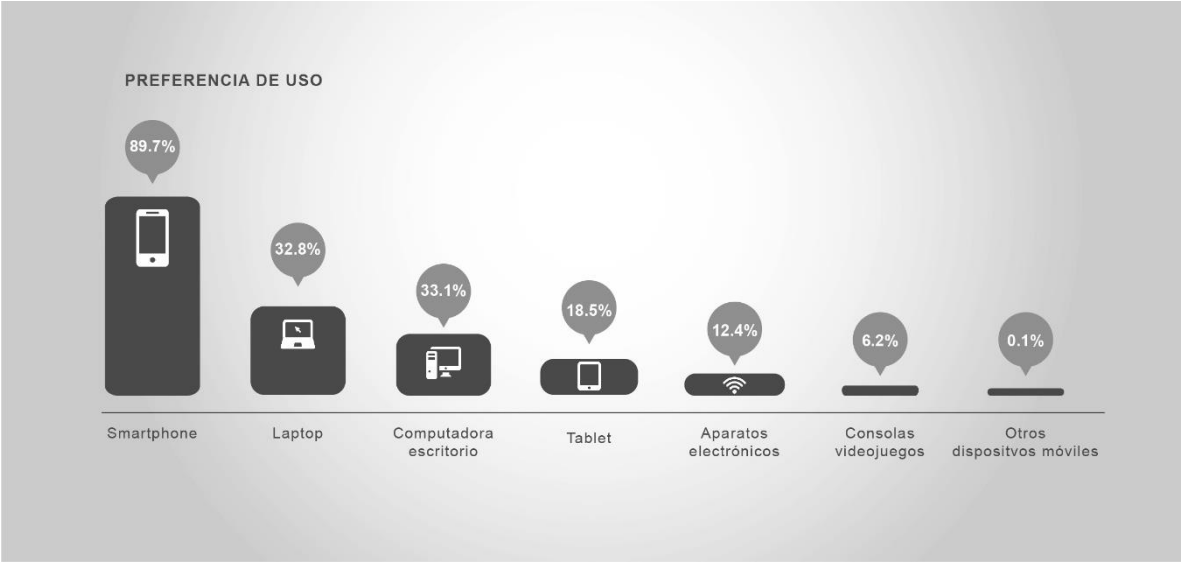
No es algo sorprendente que las dolencias que padecemos como sociedad se reproduzcan en otros medios, como los virtuales ahora, pero es obligación de todos, usar estos mismos medios en un sentido positivo y como herramienta de apoyo para contrarrestar todas las desigualdades que sufren las minorías y los grupos vulnerables.

El cuadro plantea además otras reflexiones, por ejemplo, el crecimiento que han tenido las personas mayores resultado del trabajo que se realiza para reducir las brechas de acceso e inclusión; por otro lado, la región con menor acceso es la de sureste que, como sabemos, comprende a las entidades federativas más pobres del país, donde son una constante los problemas para satisfacer las necesidades básicas de todas las poblaciones.

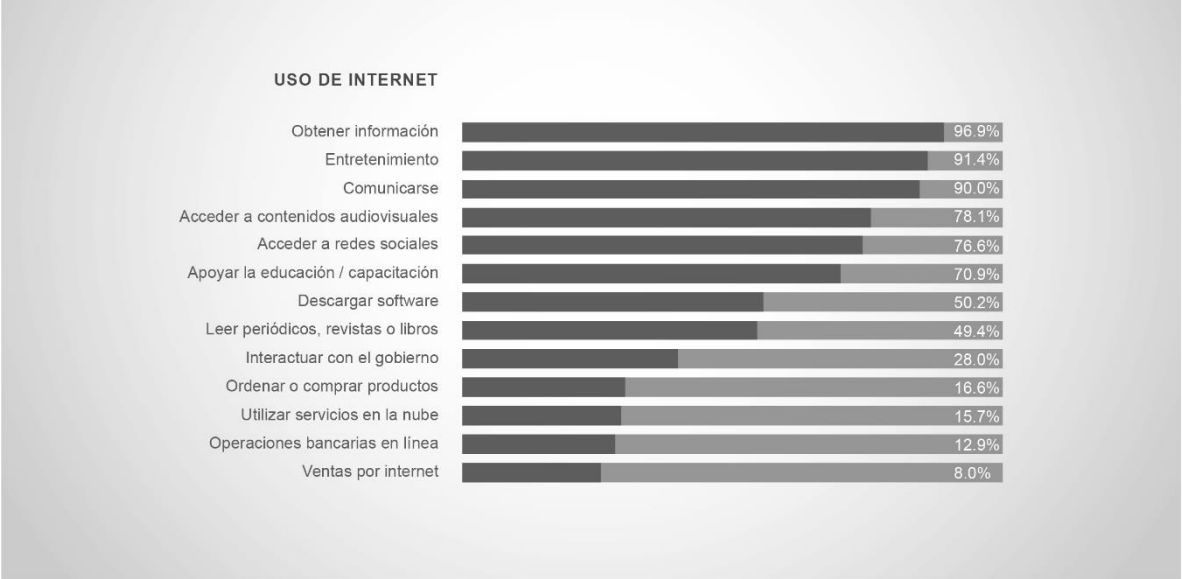
Es importante identificar donde se encuentran ubicados nuestros dolores para poder prestar especial atención y ayuda al desarrollo de nuestros pueblos.

Continuando con los grupos de personas en México que tienen acceso a Internet, los cuadros siguientes construyen una radiografía de los principales hábitos de los usuarios de Internet desde los dispositivos en los que se conectan, las actividades que realizan, los problemas que presentan y el tiempo que destinan para conectarse.

## Cuadro 4. Dispositivos de conexión, 2017.[45]

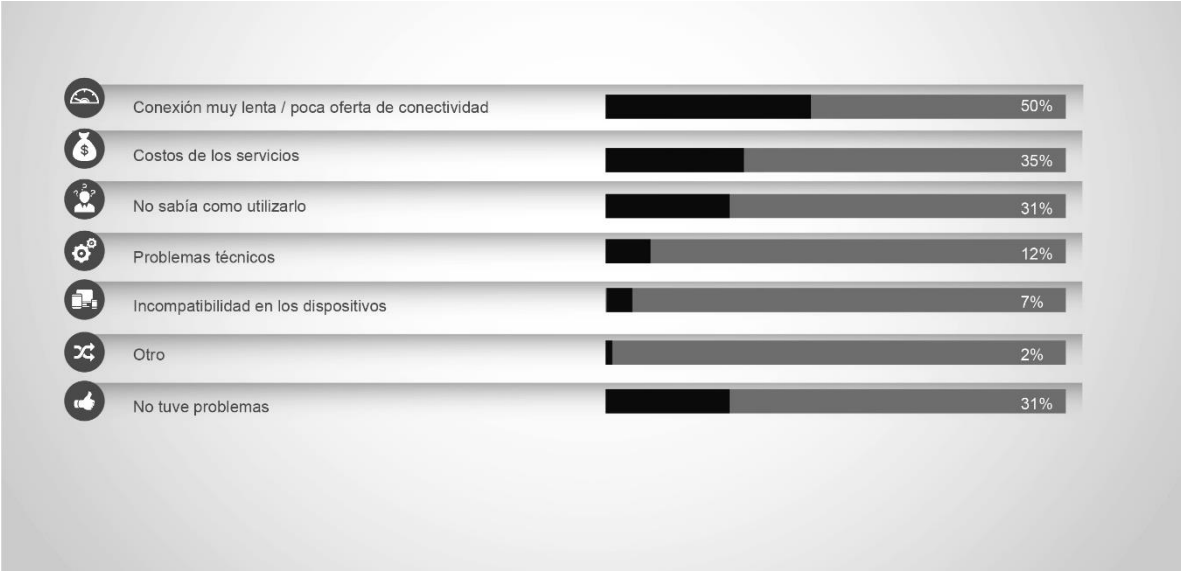



## Cuadro 5. Actividades online, 2017.[46]

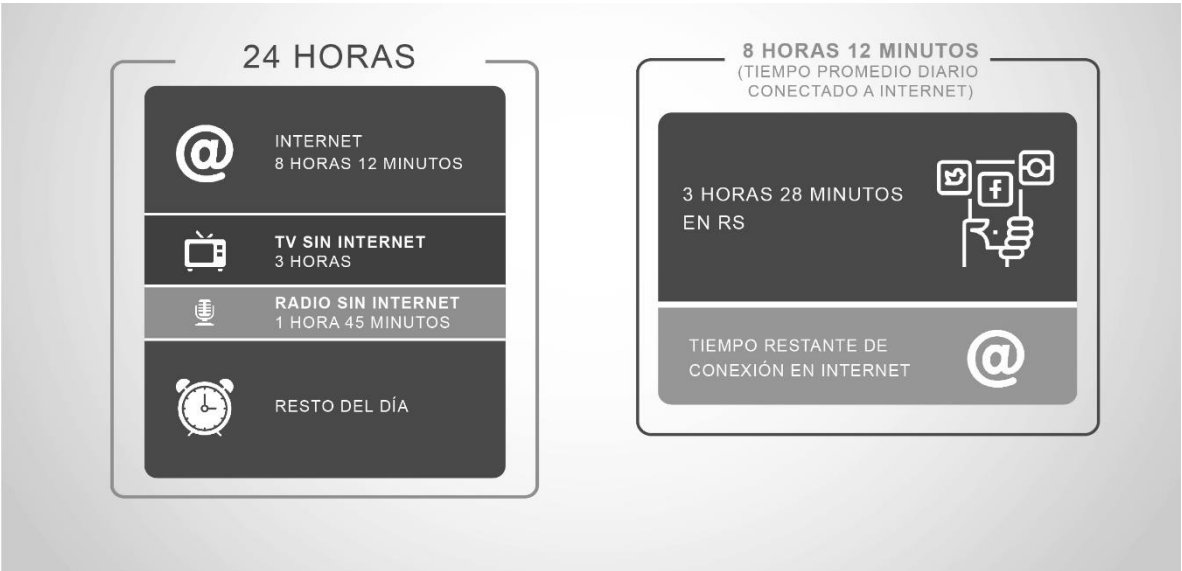



[45] *Ibídem.*
[46] *Ibídem.*

## Cuadro 6. Barreras de acceso.[47]




## Cuadro 7. Tiempo de conexión.[48]




[47] *Ibídem.*
[48] Asociación de Internet, *Op. Cit.*

Las cifras crecientes de usuarios y los daños que se han originado desde el ciberespacio han encendido las luces de alerta de los gobiernos por la incapacidad que tienen para garantizar seguridad. A continuación, se mencionarán algunos ejemplos de (in)seguridad cibernética:

### ***Stuxnet, Flame* e Irán**

El 28 de septiembre del 2010, *El País* publicó el ciberataque perpetrado en las instalaciones nucleares de Irán: "alrededor de 30,000 ordenadores se vieron afectados por el gusano informático Stuxnet".[49] Dicho ataque se efectuó como sabotaje al programa nuclear iraní y los Estados Unidos de América (EE.UU) e Israel, fueron señalados como responsables.

*Stuxnet* es considerada la primera arma cibernética del mundo y el ataque a Irán el primer ejemplo de guerra cibernética. Funciona como un *malware* altamente complejo que permite penetrar las estructuras críticas de un Estado como oleoductos, plataformas petroleras, centrales eléctricas, plantas nucleares, etc., y puede ser activado a distancia en cualquier momento sin que el portador sea consciente.

La primera versión de *Stuxnet* fue creada y probada en 2007 bajo la administración de George W. Bush, cuando Irán presumía un enriquecimiento de uranio tan grande como para crear una bomba. Posteriormente, se crearon dos versiones más agresivas en 2009 y 2010 bajo la administración de Barack Obama y cuya efectividad se confirmó con el ataque a Irán. El ataque de *Stuxnet* consistió en daños físicos, por medio de sistemas computarizados a las centrifugas y válvulas de gas de la planta nuclear.

[49] Espinosa, Ángeles, "Irán sufre un ataque informático contra sus instalaciones nucleares", *El País*, 28 de septiembre, 2010, disponible en http://elpais.com/diario/2010/09/28/internacional/1285624808_850215.html, consultada el 13 de marzo, 2015.

Más tarde, en 2012, nuevamente EE.UU e Israel se involucraron en la creación de un nuevo virus informático llamado *Flame*,[50] que es capaz de activar micrófonos y cámaras, así como movilizar teclas para realizar acciones de captura de pantalla en los ordenadores infectados con el objetivo de recopilar y robar información estratégica. Es el *software* de espionaje posiblemente más complejo de la historia.[51]

La efectividad de ambos *malwares* se traduce en el freno al programa nuclear y el desequilibrio que generó dentro del gobierno iraní donde incluso el jefe del programa nuclear fue destituido y con ello se pudo establecer nuevas sanciones a Irán. Sin embargo, el éxito también desató un debate intenso por parte de Estados Unidos y la sociedad internacional: por un lado, se celebra el cumplimiento del objetivo, pero, por el otro, cualquiera, llámese persona, corporación o Estado, mantiene una amenaza latente de ser un blanco fácil para *Stuxnet* o cualquier otro *malware.*

**Guerra Fría cibernética**

Los ataques y el espionaje cibernético se han convertido en una de las principales preocupaciones para los diferentes gobiernos de los estados. Para EE.UU., por primera vez encabezan la lista de amenazas al país por encima del terrorismo tradicional.[52]

El cibercrimen representa, para los estados, pérdidas económicas multimillonarias y supone catástrofes incluso naturales, en caso de afectar instalaciones críticas. De acuerdo con algunas cifras, el gasto en ciberseguridad en 2017 fue de $86.4 MMD

[50] EFE, "Israel y Estados Unidos son los creadores del virus informático de espionaje Flame", *El País,* 20 de junio, 2012, disponible en http://tecnologia.elpais.com/tecnologia/2012/06/20/actualidad/1340176288_675950.html, consultado el 13 de marzo, 2015.
[51] *Ídem.*
[52] Saiz, Eva, "Los ciberataques sustituyen al terrorismo como primera amenaza para EE.UU." en *El País*, 13 marzo, 2013, disponible en http://internacional.elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html, consultada el 13 de marzo, 2015.

y se espera que para el 2018 sea de $93 MMD.[53] Asimismo, se estima que para el 2021 el costo económico global del cibercrimen sea de $6 trillones anuales, en comparación con la cifra de 2015 de $3 trillones.[54]

Las ventajas que se han suscitado en el ciberespacio, en todos los ámbitos, han abierto también las puertas del cibercrimen; por lo que algunos gobiernos, como los de EE.UU., Israel, Reino Unido, España, entre otros, han adoptado, como medida para garantizar la ciberseguridad, la "militarización del ciberespacio".

La Guerra Fría cibernética consiste en que las agencias de inteligencia recluten expertos en informática con el fin de crear un ejército informático capaz de hacer frente a una guerra cibernética, llevando a cabo acciones como ciberataques y contraciberataques.

Los nuevos *hackers* se encargan, en primer lugar, de la defensa de los sistemas militares de información, neutralizando posibles ataques enemigos y reparando los sistemas dañados en el caso de que se produzca una infiltración peligrosa. Y, en segundo lugar, también se encargan de tareas relacionadas con la inteligencia, estando capacitados para entrar en sistemas adversarios si fuera necesario.[55]

Lo anterior sin duda representa una amenaza a la paz internacional, en el entendido de que cualquier Estado puede realizar trabajos de ciberespionaje o, en un peor escenario, ejecutar un ciberataque con el pretexto o no de sentirse amenazado, asimismo, estas actividades se llevarían a cabo en "desigualdad" de condiciones, ya que no todos los estados poseen las mismas capacidades de defensa y ataque en el ciberespacio.

---

[53] Cybersecurity Ventures, *2017 Cybercrime Report*, Herjavec Group, 2017, disponible en, https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf, consultada el 14 de enero, 2018.

[54] *Ídem.*

[55] Vargas, Alberto, "Ciberseguridad: el ejército Español busca hackers informáticos para una nueva unidad", en *Zoom News*, 4 de diciembre, 2013, disponible en http://www.zoomnews.es/152254/actualidad/espana/ciberdefensa-ejercito-espanol-busca-hackers-informaticos-nueva-unidad, consultada el 29 de septiembre, 2016.

Para muchos estados, el elemento primordial para determinar las capacidades reales de poder de los mismos, tienen su origen en la geografía simple. El control físico de los flujos de petróleo o gas determina los roles de dominación, subordinación, e incluso aislamiento en el mundo; de igual forma ocurre con los flujos de información.

Los flujos de información viajan a través de cables de fibra óptica, cuyas coordenadas se sitúan en espacios físicos, "se extienden a través de los suelos oceánicos, satélites que giran sobre nuestras cabezas, servidores alejados en edificios de ciudades que van desde Nueva York hasta Nairobi y los flujos bancarios que sustentan la economía."[56]

De esta manera, quienes controlan los espacios físicos de los flujos de información, tienen el poder sobre las comunicaciones mundiales, que entre las principales repercusiones, se encuentran las violaciones a la soberanía de los estados, por un lado, y a la libertad de comunicación de los ciudadanos, por otro.

Se destacan dos ejemplos de lo que Julian Assange define como el intervencionismo del S. XXI. El primero es Latinoamérica, debido a la infraestructura de Internet, cuyo tráfico se dirige desde y hacia Latinoamérica sobre líneas de fibra óptica que cruzan físicamente las fronteras de Estados Unidos.[57] Ante esto, Assange, desde *wikileaks*, desenmascaró el ciberespionaje masivo que Estados Unidos mantiene sobre el continente americano.

Existen almacenes virtuales del tamaño de ciudades enteras, controlados desde territorio estadounidense, capaces de recabar y procesar comunicaciones segundo a segundo provenientes desde cualquier latitud. Asimismo, empresas vendedoras de "seguros" para la protección de información sensible a gobiernos latinoamericanos, "gozan de lazos cercanos con los servicios de inteligencia

[56] Assange, Julian, *Cypherpunks. La libertad y el futuro de Internet,* Temas de Hoy, México, 2013, p. 20.
[57] *Ibídem*, p.13.

estadounidenses,"[58] de tal manera que, en lugar de proteger información, son utilizados como mecanismos para robar información.

El segundo ejemplo refiere al continente africano. El poder geopolítico de China se ha reforzado y expandido a través de un "intervencionismo suave" dentro de países como Uganda, el cual consiste, en proveer de servicios de Internet a estos países, a cambio de grandes contratos que permitan que China invierta (intervenga) en el crecimiento del sistema medular de fibra óptica.

Visto desde otro enfoque, la fragilidad de nuestras comunicaciones es directamente proporcional a la fragilidad en la infraestructura de cables de fibra óptica. Más del 99% de las comunicaciones internacionales se transmiten por medio de cables submarinos y el 75% de las fallas se deben a ataques externos, entre ellos, actividades humanas como la pesca, dejando el 25% restante a factores naturales como tsunamis; sin embargo, resulta alarmante que el rompimiento de las comunicaciones a nivel mundial resulte tan sencillo.[59]

### *Wikileaks*

*Wikilieaks* es uno de los fenómenos que puso en relieve la importancia de la seguridad de la información y la débil ciberseguridad de los estados, al dar a conocer información confidencial y sensible de forma no autorizada.

Se define como "Un servicio público internacional cuya misión es permitir a periodistas e informantes poner a disposición del público materiales que han sido censurados".[60]

---

[58] *Ibídem*, p.14.

[59] Para más información ver, "Así se ve el Internet en realidad: cables submarinos que atraviesan la tierra", *CNN Noticias,* 4 marzo, 2014, disponible en http://cnnespanol.cnn.com/2014/03/04/asi-se-ve-el-internet-en-realidad-cables-submarinos-que-surcan-la-tierra/#0, consultada el 03 de enero, 2017.

[60] Riestra, Laura, "Las claves del caso Wikileaks", en *ABC.*es, 21 de agosto, 2013, disponible en http://www.abc.es/internacional/20130821/abci-claves-caso-manning-201308211907.html, consultada el 03 de octubre, 2016.

El sitio web se creó en diciembre del 2006; sin embargo, se consideró enemigo de las naciones, principalmente de EE.UU., hasta 2010 cuando, en medio de la crisis de legitimidad por la invasión a Irak, dio a conocer un video donde mueren dos periodistas en tal país. Lo anterior solo fue el comienzo de lo que más tarde se convertiría en miles de cables informáticos que, en principio, acusaban a la administración estadounidense de dar cifras falsas acerca de los civiles muertos en Afganistán, así como el trabajo en conjunto con los Servicios Secretos de Pakistán y la insurgencia talibán, pero que más tarde, el resto del mundo también sería evidenciado.

La operación de *Wikileaks* se fundamenta en el artículo 19 de la Declaración Universal de Derechos Humanos, que establece lo siguiente:

> "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."[61]

Funciona a través de la recepción de información, cuyas fuentes permanecen anónimas, para posteriormente someterla a trabajos de investigación y análisis, y poder acreditar su veracidad; asimismo, la información es encriptada con el fin de evitar que pueda ser eliminada al subirse a la red.

Finalmente, se publica en el sitio web de la organización y se difunde, en primera instancia, por los principales medios de información escrita en el mundo, como *Le Monde, The New York Times, El País*, entre otros; sin embargo, el Internet por sí solo se encargará de hacerlo llegar a cualquier parte del mundo.

*Wikileaks* se caracteriza por "socializar la información", como *Wikipedia*, pero a diferencia de este sitio, la información no puede ser modificada por los lectores o usuarios, lo cual permite que se mantenga control sobre lo publicado y difundido.

[61] Organización de las Naciones Unidas, ONU, *Declaración Universal de los Derechos Humanos,* 10 de diciembre de 1948, disponible en http://www.derechoshumanos.net/normativa/normas/1948-DeclaracionUniversal.htm?gclid=COjNgKG9ldECFRuBswodJ8YBgQ, consultada el 27 de diciembre, 2016.

Julian Paul Assange, creador y editor de la página de Internet *wikileaks.org*, es, sin duda, la punta de lanza para lo que fue el desnudo cibernético internacional y de las relaciones internacionales desleales, junto a su nombre, se enlistan nombres como el de Edward Snowden, el soldado Bradley Manning (hoy Chelsea Manning), el alemán Daniel Domscheit-Berg y Adrian Lamo, por mencionar algunos.

Con el Internet, la vulnerabilidad de la información se ha acrecentado debido a que una de las grandes desventajas es el control del flujo de la misma, ya que además de complicado y costoso, es sumamente difícil. Basta con que expertos en informática desarrollen sus habilidades y hagan caso a la curiosidad para poner a temblar a cualquier parte del mundo, incluso a la más poderosa. *Wikileaks* es el gran ejemplo, y para los gobiernos y las grandes corporaciones, ha sido una amenaza inminente que ha dado a conocer información sensible y puesto en entredicho los valores que predican, así como el fracaso de las relaciones diplomáticas.

Entre las noticias que *Wikileaks* ha puesto al descubierto se encuentran historias de fracaso en las guerras contra Afganistán e Irak, así como torturas, asesinatos y detenciones deliberadas en Guantánamo; despilfarro de recursos para financiar una guerra; represión a la libertad de expresión y libertad de prensa; espionaje; abusos a la naturaleza; corrupción y cultos y otros grupos religiosos de abuso y violencia.

En el caso de México se revelaron cables diplomáticos entre los que resaltan los siguientes:

- El Cable 09MEXICO2778, en el que se relaciona a Enrique Peña Nieto con Carlos Salinas, ubicándolo como su ahijado y planeado su estrategia rumbo a las elecciones de 2012.[62]

[62] La jornada, *Wikileaks en la jornada,* disponible en, http://wikileaks.jornada.com.mx/cables/gobierno-felipe-calderon/sugieren-a-valenzuela-pedir-a-mexico-que-respalde-sin-ambiguedades-la-politica-estadunidense-para-honduras-cable-09mexico3423/, consultada el 03 de octubre, 2016.

- El cable 06VATICAN61, en el cual se vincula al cardenal Sandoval Iñiguez (Guadalajara) con el gobierno de Estados Unidos, pidiendo que frene el avance de López Obrador en la contienda presidencial de 2006.[63]
- El cable 228410, que fue difundido por el diario *El* País, señalaba que el gobierno de México había admitido haber perdido el control en ciertas zonas del país debido al narcotráfico, y que había sido a partir de esto que varios funcionarios se habían dirigido al gobierno de Estados Unidos pidiendo ayuda de manera "angustiosa".[64]
- El cable 09mexico2759, señala que, el entonces procurador general del Estado de Chihuahua, Arturo Chávez, mantenía nexos con el crimen organizado, específicamente con algunas figuras de los carteles de la droga, este cable fue enviado por el embajador estadounidense Carlos Pascual, tres días antes de que Chávez fuera ratificado como titular de la PGR.[65]

La información revelada por este medio de comunicación ocasionó muchos daños, a la ya de por sí deteriorada imagen internacional de México.

### *Anonymous*

*Anonymous* es un grupo internacional de ciberactivistas. Su estructura es horizontal, es decir, no hay líderes y se organizan y toman decisiones en diferentes foros virtuales y redes sociales.

Son responsables de una lista interminable de ciberataques en diferentes páginas web, caídas de servidores y difusión de datos privados, mismos que se llevan a cabo por medio de la Denegación de Servicios Distribuidos (DDOS); es decir, el ataque consiste en saturar un servidor hasta que su banda ancha quede al límite y sea incapaz de funcionar normalmente, ocasionando así, la caída del mismo. Es difícil poder prevenir o evitar estos "ciberataques", puesto que muy pocos servidores tienen la capacidad de aguantar gran cantidad de peticiones al mismo tiempo.

[63] *Ídem.*
[64] *Ídem.*
[65] *Ídem.*

Dentro de los principales ciberataques perpetuados por parte de *Anonymous*, se encuentran los realizados a la página web de la Sociedad General de Autores y Editores (SGAE), al Ministerio de Cultura Español y la Academia de Cine y Televisión española, así como de varios partidos españoles que apoyaron la Ley Sinde-Wert.[66]

Caso similar ocurrió en México cuando diversas Secretarías de Estado fueron víctimas de *Anonymous* como protesta en contra de la Reforma Laboral del ex presidente Felipe Calderón Hinojosa y de las leyes Döring, SOPA (Stop on Line Piracy Act) y ACTA (Acuerdo comercial anti-falsificación), que establecieron combatir la piratería en el ciberespacio, pero han sido consideradas como métodos de censura por los defensores de las libertades en Internet.[67]

En el primer caso se vieron afectadas la Secretaría de Hacienda y Crédito Público (SHCP), la Secretaría del Trabajo y Previsión Social (STPS) y la Confederación Patronal de la República Mexicana (COPARMEX) y en el canal de *Anonymous* en YouTube publicaron un video donde se exponían los puntos más sensibles a dicha reforma, tales como el *outsourcing* o la contratación por horas.[68]

En el segundo caso se dejó sin servicios a los sitios web de la Secretaría de Gobernación (SEGOB), al Senado de la República y a la Cámara de Diputados, igualmente, fue afectada la página del PAN en Sinaloa y la página http://copyrightalliance.org.

---

[66] La Ley Sinde-Wert es el nombre informal con el que se le conoce a un apartado particular de la Ley de Economía Sustentable española por iniciativa de la Ministra de Cultura, Ángeles González-Sinde y posterior aprobación del Ministro de Educación, Cultura y Deportes, José Ignacio Wert, la cual se refiere a los Derechos de Autor y que como muchos países en el orbe, tiene como objetivo central la creación de regulaciones que impidan que, por medio del Internet, se lucre con la creatividad ajena. Dicha Ley causó un debate extenso por las irregularidades desde su gestión hasta las injusticias por su ejecución. Arcos, Eduardo, "¿Qué es y cómo funciona la Ley Sinde?", *Hipertextual*, 25 de enero, 2011, disponible en https://hipertextual.com/2011/01/que-es-la-ley-sinde, consultada el 03 de octubre, 2016.

[67] Expasión, *Anonymous ataca los sitios del Senado y Gobernación por la ley Döring*, 27 de enero, 2012, disponible en https://expansion.mx/tecnologia/2012/01/27/anonymous-ataca-los-sitios-del-senado-y-gobernacion-por-la-ley-doring?internal_source=PLAYLIST, consultada el 03 de octubre, 2016.

[68] Austria, Xóchitl, "5 travesuras de Anonymous en México"*, Alto Nivel,* 17 de enero, 2013, disponible en, http://www.altonivel.com.mx/33468-los-ataques-de-anonymous-en-mexico.html, consultada el 03 de octubre, 2016.

Los portales de la Secretaría de la Defensa Nacional (SEDENA), la Secretaría de Marina-Armada (SEMAR) y la Comisión Nacional de Seguridad (CNS) también han sido paralizados en más de una ocasión, asimismo, el grupo de ciberactivistas ha manifestado su desaprobación hacia el Partido Revolucionario Institucional (PRI) y del presidente Enrique Peña Nieto. Lo demostró previo a las elecciones del 2012 apoyando al movimiento *#YoSoy132* y realizando ataques a diferentes páginas priístas. Destaca el ciberataque a la página oficial del PRI y a la casa encuestadora Mitofsky, argumentando tener algún tipo de relación que favorecía al PRI en las encuestas.

*Anonymous* también ha actuado en contra de grupos del crimen organizado y narcotráfico. En 2011, el grupo mexicano de narcotraficantes “Los Zetas” secuestró a un miembro del grupo de *hacktivistas* en Veracruz por lo cual, mediante un video, se pedía la liberación del compañero o mediante la operación *Paperstorm* se revelaría información delicada sobre vínculos entre el grupo delictivo y políticos, empresarios, policías y militares.

Sin embargo, poco antes de dar inicio a la operación, se dio a conocer a través de redes sociales, que la víctima había sido liberada a cambio de no revelar información o de lo contrario, se tomarían represalias en contra de la familia del plagiado.

*Anonymous* es un ejemplo de la organización que existe entre la *cibersociedad civil* y ejemplifica la facilidad con la que cualquier persona puede acceder al ciberespacio y representar una amenaza desde el ciberespacio; sin embargo, en el siguiente apartado se expone la otra cara del ciberespacio, aquella que saca ventaja del ciberespacio, lo explota y lo usa en pro del desarrollo humano.

### 1.2.4. El ciberespacio como habilitador de desarrollo.

El concepto tradicional de desarrollo se ha edificado en torno a cuestiones de índole económica, donde el crecimiento económico ha sido el mayor símbolo de desarrollo.

Bajo la sombra de esta acepción, se excluyen aspectos de orden político, social, cultural y tecnológico que también determinan el desarrollo humano.

El Internet ha potenciado el desarrollo en el ámbito económico (cuantitativo) y generado paradigmas de gran impacto social (cualitativas) como el *Cloud computing* o La nube, la web en tiempo real, la geolocalización, la realidad aumentada y el Internet de las cosas.

***Cloud computing***

La Nube es un almacén infinito, compuesto por un conjunto de servidores de información en el que albergan y distribuyen un sinfín de datos (*big data*) y aplicaciones Web.

Dicho almacén está a disposición de cientos de miles de usuarios, que descargan y ejecutan programas y aplicaciones de un catálogo virtual, como Gmail, Facebook, Twitter o YouTube, las veces que quieran, desde cualquier lugar y en varios dispositivos; asimismo, la Nube es capaz de almacenar los datos que el usuario quiera guardar.

Igual que el Internet en su momento, la nube se ha insertado de manera sigilosa. Los datos y las aplicaciones son repartidos en los servidores de ordenadores que pertenecen a los gigantes de Internet como Microsoft, Google, Oracle y Amazon –por mencionar algunos–, y en menor cantidad de las empresas o universidades que van creando poco a poco sus centros de datos para poner a disposición de la comunidad interna.

Las “app stores” son probablemente los sistemas nube más exitosos que existen en la actualidad y han revolucionado la forma en que los usuarios hacen uso de sus dispositivos.

La Nube ha sido posible gracias a los sistemas de velocidad y banda ancha, así como a la innovación y crecimiento de dispositivos conectados a Internet; es una

combinación de hardware, software, infraestructura y almacenamiento, que en conjunto, facilitan la entrada y salida de la información como un servicio.

**La Web en tiempo real**

Gracias a los Medios Sociales (*Social Media)*, como los *blogs, wikis* o las redes sociales, y la Web 2.0, donde el usuario es consumidor y productor de contenidos al mismo tiempo, nos encontramos inmersos en una proliferación de información en tiempo real desde cualquier parte del mundo.

Actualmente, a través de una serie de tecnologías y procedimientos, la información se actualiza de manera automática y podemos obtener la inmediatez de las noticias y gestionarlas minuto a minuto.

**La Geolocalización**

Los sistemas de GPS *(Global Positioning System),* que han sido instalados en los celulares principalmente, permiten identificar las coordenadas geográficas de cualquier lugar o persona, asimismo, pueden propiciar información de cualquier tipo, por ejemplo, horarios o el tiempo aproximado de llegada y desde diferentes medios de transpote. En la actualidad, las aplicaciones de geolocalización han sido tan desarrolladas, que son capaces de indicar rutas alternas, puntos de lento tránsito y accidentes.

**Realidad Aumentada**

La combinación entre la realidad y la virtualización ha sido uno de los grandes experimentos que ha logrado la tecnología. Funcionan como la creación de un entorno mixto entre un espacio real, combinado con elementos virtuales y en tiempo real. Uno de los ejemplos más recurrentes al respecto, son los videojuegos.

## Internet de las cosas

Los sueños hechos realidad son una metáfora de los avances tecnológicos. Cada día nos vemos rebasados por cosas impensables años atrás. Hoy, por ejemplo, existen miles de dispositivos de uso cotidiano capaces de acceder a un servidor de Internet, desde dispositivos móviles, hasta automóviles, televisiones, consolas de videojuegos, dispositivos de video y ahora electrodomésticos, los cuales han facilitado la vida diaria y traído grandes beneficios a organizaciones y empresas de toda índole.

La onda expansiva de las TICs y, a su vez, del Internet, ha potenciado un crecimiento en las comunicaciones sin precedentes y desarrollado diferentes aspectos de la vida cotidiana desde diferentes ámbitos.

Además de comunicarnos, el Internet ha facilitado el acceso a la información sobre cualquier tema, así como el intercambio cultural; ha servido como plataforma entre el gobierno y la sociedad civil y desarrollado la educación, las ciencias, las artes y las capacidades del sector empresarial. Todo lo anterior se ha visto reflejado en términos de crecimiento y desarrollo económico y social en gran parte del mundo.

Los avances tecnológicos están vinculados con el desarrollo desde diversas perspectivas, por ejemplo, han impulsado el crecimiento, ampliado las oportunidades y mejorado la prestación de servicios; miles de millones de vidas se han salvado por las mejoras en la infraestructura tecnológica del sector salud y en el ámbito económico, hay muchos ejemplos a destacar, por ejemplo, la reducción de costos en las transacciones o la facilidad para concretar negocios; asimismo, se ha incrementado la productividad de las mujeres o las personas con discapacidades, gracias a las nuevas herramientas de comunicación. [69]

[69] Banco Mundial (2016), *Informe sobre el desarrollo mundial 2016: Dividendos Digitales*, cuadernillo del "Panorama General", Banco Mundial, Washington DC. Licencia: Creative Commons de Reconocimiento CC BY 3.0 IGO.

Los dividendos digitales son los beneficios más amplios en términos de desarrollo, derivados de la utilización de las tecnologías digitales; gracias a ellos, las empresas son más productivas, las personas encuentran mejores empleos y tienen más oportunidades, y los gobiernos, prestan mejores servicios públicos a la sociedad; sin embargo, han puesto en relieve que, a pesar de que la globalidad es un proceso eminentemente global y la globalización de las TICs ha aumentado, la distribución de los dividendos digitales, no es igualitaria. [70]

Dentro de los sectores favorecidos por el acceso a las tecnologías digitales (Internet, teléfonos móviles y todas las demás herramientas para recopilar, almacenar, analizar y compartir información en forma digital), el cual representa el 40% de la población mundial, se han encendido las señales de alerta debido a los riesgos y ataques perpetrados a raíz de la creciente conectividad y, con ello, se ha dejado en segundo plano la inclusión del 60% de la población restante.[71]

El debate internacional se ha centrado en la pregunta ¿hasta qué punto debe frenarse el desarrollo, en aras de mantener la seguridad? O viceversa, ¿hasta qué punto se debe ponderar el desarrollo sobre la seguridad? Ambas preguntas hacen alusión a que ambos conceptos se repelen; sin embargo, el tiempo actual, ha manifestado el estudio de los grandes tópicos de las Relaciones Internacionales desde el binomio seguridad-desarrollo y no por separado.

De acuerdo con el Informe sobre el desarrollo mundial 2016, cuyo tema de estudio son los dividendos digitales, la desigualdad en la expansión de los mismos, se debe a dos motivos; el primero al desarrollo y el segundo a la seguridad, como si ambos fueran incompatibles.

Por un lado y como se mencionó, el 60% de la población mundial no tiene acceso a Internet y, por ende, no puede participar en la economía digital, lo que ocasiona entonces que ciertos sectores de la población no puedan competir por mejores

[70] *Ibídem,* p. 2.
[71] *Ibídem*, p. 3.

trabajos; “Y dado que la economía de Internet favorece los monopolios naturales, la falta de un entorno de negocios competitivo puede resultar en una mayor concentración de los mercados. Lógicamente, las personas más instruidas, mejor conectadas y más capaces han recibido la mayor parte de los beneficios, lo que circunscribe los dividendos de la revolución digital.”[72]

El segundo motivo se refiere a los riesgos que existen en el ciberespacio y que han contrarrestado los esfuerzos en materia de desarrollo. La situación de vulnerabilidad y riesgo a la que estamos expuestos al acceder a la red es innegable y es una tarea importantísima para los gobiernos y todos los actores involucrados, hacer del ciberespacio un sitio seguro; sin embargo, es igualmente grave la situación de exclusión y de desigualdad en el tema. “De hecho, quedar al margen de dichas redes es la forma de exclusión más grave que se puede sufrir en nuestra economía y en nuestra cultura”.[73]

Un gran número de procesos democráticos, de simple y llana comunicación y acceso a la información, así como los relacionados con actividades económicas, se llevan a cabo a través de plataformas digitales, lo cual se debe a los bajos costos de la información y de las transacciones económicas y sociales para las empresas, las personas y los gobiernos; así como la eficacia y facilidad para llevarlas a cabo.

A diferencia de otras innovaciones tecnológicas, cuyo esparcimiento ha sido más lento, el Internet y las tecnologías digitales se han reproducido con gran rapidez. De acuerdo con cifras del Banco Mundial, este rápido esparcimiento se concentra en los países en desarrollo, donde son más las personas que poseen un teléfono móvil que las que tienen acceso a servicios básicos como electricidad o agua potable.[74]

En el caso del Internet, su acceso ha sido más lento, “solo el 31% de la población de los países en desarrollo tenía acceso a esa tecnología en 2014, frente al 80% en los países de ingreso alto. China tiene el mayor número de usuarios de Internet,

[72] *Ídem.*
[73] Castells, Manuel, *Op. Cit.,* p. 17.
[74] Banco Mundial (2016), *Op. Cit.,* p.5.

seguida de Estados Unidos; India, Japón y Brasil completan los cinco países que encabezan la lista."[75]

De acuerdo con el informe del Banco Mundial, las tecnologías digitales promueven tres aspectos importantes para el desarrollo, el primero de ellos es la inclusión, seguida por la eficiencia e innovación.

Para una mayor inclusión, el acceso a una fácil y rápida búsqueda de información es primordial. Al llevar a cabo ciertas transacciones, no importa de qué índole, es importante que las partes involucradas conozcan información del otro para generar confianza y transparencia, así como asimetría en la información, es decir, que uno no posea una mayor cantidad de información que el otro. Los bajos costos y la facilidad para recabar información han dado como resultado transacciones más exitosas, como la expansión del comercio, la generación de empleos y el aumento en el acceso a los servicios públicos; es decir, la creación de mercados genera mayor inclusión.

A partir de la llegada de Internet, las transacciones se han caracterizado por ser más fáciles, más rápidas y más baratas; es decir, son más eficientes. En primer lugar, porque los bajos costos de las tecnologías digitales han permitido que los gobiernos y las empresas hagan uso de ellas para automatizar algunos procesos y actividades; es por ello que, hoy día, existe una gran cantidad de servicios en línea para poder realizar trámites de cualquier índole. Y, en segundo lugar, porque las tecnologías digitales fomentan la productividad y, por ende, aumentan la rentabilidad del capital humano. "Internet, al racionalizar las tareas y aumentar la productividad de los factores existentes, puede aumentar considerablemente la eficiencia económica de las empresas, los trabajadores y los Gobiernos".[76]

Por si lo anterior fuese poco, el Internet ha permitido que las cosas impensables o extraordinarias, se conviertan en una realidad. Cuando el vínculo existente entre el

[75] *Ibídem,* p.6.
[76] *Ibídem,* p. 11.

usuario y las tecnologías digitales se lleva a cabo de manera casi automática y el costo es tan bajo, podemos decir que es el grado máximo de la eficiencia; para ello, son indispensables plataformas digitales de grandes capacidades de búsqueda, de comercio electrónico, de música, etc.

La “nueva economía”, como lo define el Banco Mundial, son los crecimientos a gran escala que se generan por medio de la creación de plataformas digitales. Evidentemente, la inversión para llevar a cabo la creación de plataformas es alto (costo fijo), pero el costo de expansión (costo marginal) es prácticamente nulo, lo que atrae a más compradores y vendedores y, por ende, se genera un circulo virtuoso.

Las redes sociales, por ejemplo, son una plataforma gigante, cuyo éxito se debe al aumento de usuarios; a través de ellas se establecen infinidad de actividades, desde las referentes a la comunicación, búsqueda de información, comercio, e incluso, organización, por ejemplo, movilizaciones sociales y protestas políticas.

Dentro del Internet, convergen con frecuencia los tres elementos. En un terreno cercano, podemos referirnos al auge que han tenido los servicios de transporte digitales como Uber o Cabify, cuya plataforma realiza la búsqueda, y posterior vínculo, entre el chofer y el usuario casi de manera automática. De esta manera, ambas partes se benefician, por un lado, el chofer genera ingresos y, por otro, el usuario adquiere un servicio que le brinda (en teoría) mayor seguridad, confianza y, en la mayoría de los casos, precios más bajos. En ese orden, hablamos de innovación, eficiencia e inclusión.

En el terreno global, Internet expande el comercio al permitir la inclusión de muchas pequeñas y medianas empresas en el sector, a partir de esto, la utilización del capital existente mejora, se hace más productiva y, en consecuencia, más eficiente, para finalmente, fomentar la competencia y favorecer la innovación.

Internet se ha convertido en parte de la infraestructura de los países y en una parte importantísima en los procesos democráticos al aumentar las capacidades de los

Gobiernos y fomentar la participación ciudadana; así como en los procesos económicos al promover la creación de empleos y hacer más productivo el capital humano.

A pesar de ello, las TICs constituyen un segmento bastante pequeño en la economía; en los países miembros de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), su proporción en el PIB es de apenas el 6%.[77] En los países desarrollados, por ejemplo EE.UU., a pesar de la gran cantidad de empresas de tecnología que habitan en dicho país, las TICs contribuyen con el 7% del PIB estadounidense.[78]

Para que las TICs y los dividendos digitales puedan distribuirse de manera igualitaria a lo largo y ancho del mundo, se requiere de las capacidades humanas que las tecnologías digitales no pueden proveer. Internet es solo una parte del proceso, es solo una herramienta para facilitar y automatizar determinados procesos; sin embargo, el manejo de los mismos, así como el entorno óptimo para su ejecución, dependen de una armonización *offline*, es decir, de "complementos analógicos";[79] de lo contrario, se incubarán antítesis de desarrollo.

Por ejemplo, si Internet facilita el crecimiento a escala de las empresas, pero el entorno *offline* no facilita la competencia, lejos de obtener una innovación futura, se concentrará el poder de mercado y se crearán monopolios. Por otro lado, es importante que las personas reciban capacitaciones en materia tecnológica para poder ser más eficientes y conocer los riesgos que conlleva el acceso a las TICs para poder estar más alerta e incrementar las medidas de seguridad, como usuario y como proveedor; si existen problemas de desigualdad en el capital humano, éste se verá sesgado y la facilidad para automatizar procesos por medio del Internet, no cumplirán su propósito. Asimismo, es necesario que los Gobiernos efectúen y

[77] *Ibídem,* p. 12.
[78] *Ídem*. En EE.UU. se encuentran 8 de las 14 compañías de tecnología más grandes del mundo.
[79] El Banco Mundial define estos "complementos analógicos" como las normas que garantizan un elevado grado de competencia, las habilidades que permiten sacar provecho de la tecnología y las instituciones que rinden cuentas a los ciudadanos.

mejoren los sistemas democráticos y de rendición de cuentas para generar mayor inclusión en la población y optimizar el acceso a la información que las TICs proveen.

El ciberespacio debe ser un lugar libre, seguro y universal. El debate político sobre los impactos de la tecnología debe cernirse sobre la seguridad y el desarrollo en conjunto, ya que ejercer seguridad absoluta sobre cualquier ámbito, tiende a privar derechos fundamentales.

## 1.3. La seguridad nacional.

### 1.3.1. La concepción tradicional-militar de la seguridad nacional.

El concepto de seguridad encuentra sus raíces en el latín *securitas/securus*, que a su vez proviene de *sine cura*. *Sine* significa sin y *cura*, cuidado, preocupación, problema y atención. Así, *sine cura*, significa sin cuidado, sin preocupación o sin problema.[80]

La seguridad se refiere a la libertad de sentirnos sin preocupaciones o a salvo de cualquier riesgo o daño que algo o alguien pueda ocasionarnos; sin embargo, con esa definición, el concepto resulta demasiado ambiguo. Una persona puede creer que está en peligro y no estarlo, es decir, la seguridad puede determinarse por percepciones y no necesariamente por situaciones concretas.

Por su parte, la seguridad nacional en las ciencias sociales se construyó, en gran medida, por la escuela realista y las aportaciones de Hans Morgenthau y, anteriormente, Walter Lippmann, por mencionar algunos.[81] La seguridad nacional ha prevalecido bajo el concepto restringido y unidimensional que se vincula al uso de la fuerza y a los asuntos concernientes a la guerra; asimismo, se ha vinculado

[80] Bárcena Coqui, Martha, "La reconceptualización de la seguridad", en *Seguridad Internacional en el siglo XXI: los retos para América Latina y el Caribe*, primera edición 2004, Senado de la República, México, p. 17.
[81] Rockwell C. Richard y Richard H. Moss, "La reconceptualización de la seguridad: un comentario sobre la investigación", en *En busca de la seguridad perdida. Aproximaciones a la seguridad nacional mexicana*, Sergio Aguayo (comp.), Ed. Siglo veintiuno, primera edición 1990, México, p. 44.

directamente al Estado, como único actor involucrado en los asuntos referentes a la seguridad.

Para los autores Rockwell y Moss, siguiendo la escuela realista, “una nación está segura cuando su gobierno tiene suficiente poder y capacidad militar para impedir el ataque de otros estados a sus legítimos intereses y, en caso de ser atacada, para defenderlos por medio de la guerra”;[82] para mantener la estabilidad, el Estado estaba obligado a defender militarmente su territorio y soberanía, así como cualquier influencia ideológica que pudiera amenazar a su población; es decir, la amenaza comunista.[83]

En las Relaciones Internacionales, el concepto de seguridad ha estado presente a través de los años y a pesar de los diferentes significados que las teorías clásicas le han otorgado.

Como se sabe, los conflictos bélicos del siglo pasado dotaron de predominante fuerza a los teóricos realistas, desacreditando severamente a los idealistas profanadores de la cooperación y compatibilidad de intereses en la sociedad internacional.

Para los idealistas, existían ciertos valores morales compartidos entre los estados, capaces de contrarrestar acciones violentas; sin embargo, durante los conflictos de los años veinte y treinta, así como el desencadenamiento de la Segunda Guerra Mundial, hicieron que los idealistas perdieran credibilidad ante la sociedad internacional y creciera la afinidad hacia los realistas.

Para los realistas, la conducta humana es determinada por la naturaleza humana, misma que está cargada de valores negativos como la ambición y el egoísmo y, por ende, las relaciones humanas están definidas en términos de conflicto, competencia y anarquía.

[82] *Ibídem,* p. 44.
[83] *Ídem*.

Los más antiguos antecedentes del realismo político, recaen en el pensamiento de Tucídides (año c. 460 al 400 a. C.) durante la guerra entre atenienses y espartanos, documentada en *La historia de la guerra del Peloponeso*.[84] Para Tucídides, la naturaleza humana es ambiciosa y ávida de dominación, por tanto, las relaciones entre los estados se ejercen en función del poder y no de la justicia.

Más tarde, durante la Edad Media, Nicolás Maquiavelo (1429-1527) da forma al paradigma realista mediante el posicionamiento de los Estado-nación como la unidad política suprema y el factor moderno de poder.[85]

Para Maquiavelo, los estados, la política y las instituciones son creadas por los hombres para responder a sus propios intereses de poder, riqueza y bienestar; la supervivencia del Estado es lo más importante y bajo cualquier medio, incluyendo la guerra.[86]

En la misma línea, el *Leviatán* de Tomas Hobbes (1588-1679), describe que "el hombre es el lobo del hombre" y, por tanto, solo los más fuertes sobreviven. El estado natural del ser humano, lo obliga a vivir en competencia y conflicto para garantizar su supervivencia y su seguridad.[87]

Para los realistas, el sistema internacional es anárquico y de conflicto, y la preservación del Estado-nación lo más importante. Dado que la guerra es el factor más utilizado, la única manera de mantener a los estados seguros, dependerá de la capacidad militar que posean y el uso legítimo de la fuerza es exclusivo del Estado.

Como hemos observado, el poder es un concepto ligado de manera automática, al concepto tradicional de seguridad, pero no solo a éste, sino a la política internacional en su conjunto.

---

[84] Jiménez, Claudia G. "Las teorías de la cooperación internacional dentro de las relaciones internacionales" en, *Polis. Investigación y Análisis Sociopolítico y Psicosocial*, 03 Vol. DOS, UNAM, México, pp. 115-147.
[85] *Ídem.*
[86] *Ídem.*
[87] *Ídem.*

Max Weber define al poder como “la probabilidad de imponer la propia voluntad dentro de una relación social, aún contra toda resistencia y cualquiera que sea el fundamento de esa probabilidad”.[88] Dentro del pensamiento *weberiano*, el poder constituye el elemento central dentro de la naturaleza de la política y del Estado.

En otras palabras, “el poder –definido en términos de interés nacional– determinará lo que un Estado pueda o no hacer en la política internacional. El interés nacional –definido, a su vez, en términos de seguridad– será aquello que defina y oriente las políticas que el Estado lleve a cabo para su consecución, sean o no éticas o morales.[89]

La corriente idealista, como la realista, se remonta a la Antigua Grecia con Aristóteles (384 – 322 a. C.) cuya aportación recae en el reconocimiento de las virtudes y la ética de los hombres; sin embargo, uno de los conceptos primordiales del pensamiento aristotélico y que, a su vez, acompañó al pensamiento idealista, es el concepto de la libertad.[90]

Para los idealistas, el objetivo principal es la consecución de la paz y rechazan la creencia realista del uso de la fuerza como el único medio para garantizar estabilidad y resolver conflictos. En contraste con esta idea, la creación de instituciones políticas podría contrarrestar los abusos por parte de los estados y serían garantes de justicia.[91]

Durante la Ilustración, Immanuel Kant es el idealista por excelencia. En la *Paz Perpetua,* Kant afirma que la paz solo podrá lograrse a través de la razón, el derecho y la justicia.[92]

---

[88] Weber, Max, *Economía y sociedad*, Ed. Fondo de Cultura Económica, 2da. Edición, México, 1979, pág. 43.
[89] Zavaleta, Sandra, *Más allá de la visión tradicional de la seguridad y del desarrollo. Hacia la consecución de la seguridad humana y el desarrollo humano en las relaciones internacionales contemporáneas,* UNAM, México, 2012, p. 24.
[90] Jiménez, Claudia G., *Op. Cit.*
[91] *Ídem.*
[92] *Ídem.*

El periodo entre guerras y durante un lapso de la Guerra Fría, se marcó el auge de la corriente realista, obligando a los idealistas a redefinirse; sin embargo, a finales de los años sesenta, el realismo clásico entró en crisis debido a las relaciones interdependientes y transnacionales que se gestaron durante la Guerra Fría, a causa de la descolonización de África y la transformación de los conflictos Este-Oeste para dar paso a los conflictos Norte-Sur, y que, a su vez, derivaron de los daños causados a los pueblos y sociedades de la periferia.

La década de los ochenta, con el fin de la Guerra Fría, marcó el resurgimiento del liberalismo como alternativa al realismo, así como los paradigmas cualitativos que demandaron la ampliación del concepto de seguridad, fuera de la acepción tradicional y estato-céntrica.

### 1.3.2. Seguridad humana.

Desde mediados de la década de los ochenta, el Grupo de los Seis o G-6 (Francia, Alemania Occidental, Italia, Japón, Reino Unido y Estados Unidos) advirtió sobre las repercusiones sociales derivadas de la guerra y vulnerabilidad de los pueblos por la paz armada; sin embargo, fue hasta el término de la Guerra Fría y posterior colapso de la Unión Soviética en 1991, cuya razón en gran medida se debió al gasto exacerbado en la carrera armamentística, que otros aspectos relacionados al bienestar de las sociedades e irrelevantes en el sistema bipolar, comenzaron a tomar espacio en diferentes medios internacionales y de análisis, tornando urgente la necesidad de replantear la agenda de amenazas a la seguridad internacional, así como el concepto de seguridad en sí mismo.

Aunado a ello, la globalización abrió la puerta a actores no estatales para participar en los tópicos de la agenda internacional, ocasionando de esta manera, el desvanecimiento de los límites entre lo interno y lo externo, y dando paso a una serie de problemáticas que salían de los límites tradicionales y estato-céntricos del concepto de seguridad que se mantuvo durante el periodo entre guerras y gran parte de la Guerra Fría.

A pesar de los estudios preliminares de algunos académicos, así como de organismos internacionales enfocados en ciertas áreas —realizados en la década de los setenta—, los noventa y los primeros años del presente siglo, formaron un parteaguas histórico en las relaciones internacionales basadas en la edificación de conceptos más amplios, sistémicos y multidimensionales.

La agenda de seguridad estato-céntrica y militar resultó insuficiente para garantizar la seguridad y el desarrollo mundiales debido al descuido de las necesidades más básicas para el desarrollo y la prosperidad de las personas. Conflictos perpetrados dentro de los estados y no entre ellos, pero que se proyectaban al exterior como el narcotráfico y el crimen organizado enfatizaron la necesidad de replantear la agenda de amenazas a la seguridad nacional; sin embargo, las guerras civiles, los genocidios, así como los tópicos relacionados con las migraciones masivas y el aumento en el número de refugiados y desplazados, el crecimiento demográfico, las muertes por VIH/Sida, las crisis económicas, alimentarias y ambientales, desigualdad de género, procesos democráticos y derechos humanos, pusieron en relieve, que la agenda de seguridad también debía atender asuntos centrales en la seguridad y el desarrollo de la persona y no solo del Estado como era tradición.

Durante ese periodo, las coordenadas del conflicto Este-Oeste cambiaron para posicionarse en los conflictos Norte-Sur, colocando el acento en el desarrollo y en bloques regionales más que en estados unitarios.

> Actualmente, para la mayoría de las personas, el sentimiento de inseguridad se debe más a las preocupaciones acerca de la vida cotidiana que al temor de un cataclismo en el mundo. La seguridad en el empleo, la seguridad del ingreso, la seguridad en la salud, la seguridad del medio ambiente, la seguridad respecto del delito: son éstas las preocupaciones que están surgiendo en todo el mundo acerca de la seguridad humana.[93]

Cuando la amenaza comunista desapareció, el concepto de seguridad se fue construyendo bajo el umbral del subdesarrollo. En 1980, el Informe Brandt definió el concepto de seguridad económica; en 1987, la Comisión Brundtland, publicó el

[93] *Ibídem,* p. 3.

informe *Nuestro futuro común* e introdujo el concepto de seguridad medioambiental; paralelamente, la Organización de las Naciones Unidas para la Agricultura y la Alimentación (FAO por sus siglas en inglés) y la Organización Mundial del Comercio (OMC) aportaron el concepto de seguridad alimentaria y la Organización de los Estados Americanos (OEA), el concepto de seguridad democrática, para finalmente, en 1994, el Programa de las Naciones Unidas para el Desarrollo (PNUD) utilizar por primera vez el concepto de seguridad humana.[94]

Con el fin de alcanzar la seguridad humana, se ponderó la importancia de un nuevo paradigma de desarrollo como elemento fundamental para lograr la paz y seguridad internacionales.

> […] el desarrollo humano sostenible favorece a las personas, promueve el empleo y favorece a la naturaleza. Asigna la máxima prioridad a reducir la pobreza y promover el empleo productivo, la integración social y la regeneración del medio ambiente. Establece un equilibrio entre las cantidades de seres humanos, por una parte, y por la otra, la capacidad de absorción de las sociedades y la capacidad de sustento de la naturaleza. Acelera el crecimiento económico y lo traduce en mejoras en las vidas humanas, sin destruir el capital natural necesario para proteger las oportunidades de futuras generaciones. Además, reconoce que no es mucho lo que puede lograrse si no se cuenta con una mejora muy sustancial en la condición de la mujer y si no se abren ampliamente todas las oportunidades económicas a la mujer. Y el desarrollo humano sostenible fomenta la autonomía de las personas, posibilitando que diseñen los procesos y acontecimientos que conforman sus vidas y participen en ellos.[95]

La seguridad humana no solo se refiere a la protección de la persona, sino a la prevención y el empoderamiento del ser humano como persona y comunidad, para valerse por sí mismos y lograr una vida digna y estable. Si bien el Estado sigue siendo el proveedor fundamental, cuando falla y no es capaz de proporcionar seguridad a su población, puede, incluso, convertirse en una amenaza para los mismos.

---

[94] "La seguridad humana no es una preocupación por las armas; es una preocupación por la vida y la dignidad humanas", "Nuevas dimensiones de la seguridad humana", en *Informe sobre desarrollo humano 1994*, Programa de las Naciones Unidas para el Desarrollo (PNUD), FCE, México, 1994.
[95] *Ibídem,* p.5.

> En suma, la aparición del concepto de seguridad humana responde sobre todo a dos nuevas ideas formuladas en la década o década y media anterior: a) la seguridad debe centrarse en las personas; y b) la seguridad de las personas se ve amenazada no sólo por la violencia física, sino también por otras amenazas a su subsistencia en condiciones de dignidad. […] A estas ideas habría que añadir una tercera, referida a los medios: la seguridad no puede alcanzarse mediante la confrontación y las armas, sino mediante la cooperación y la política.[96]

Al mismo tiempo, esta concepción amplia de la seguridad no exime de la agenda la amenaza de una guerra, sino que la complementa y convierte en interdependiente, ya que, si se gestara una nueva guerra, se gestarían al mismo tiempo problemas de otra u otras índoles. "Los ámbitos individual, familiar, comunitario, estatal, regional y global se influyen dialécticamente."[97]

Eventualmente, el concepto de seguridad humana desencadenó un debate en las diferentes esferas de la política nacional e internacional para intentar esclarecer los límites y alcances del concepto de seguridad humana; por un lado, los llamados minimalistas (*freedom from fear*) y, por otro, los maximalistas (*freedom from want*).[98]

Dentro del primer grupo, la seguridad humana se limita a las consecuencias extremas de un conflicto, como crímenes de lesa humanidad o genocidios bajo el argumento de que, de otro modo, se corre el riesgo de *seguritizar* en sentido negativo la agenda.[99]

Sin embargo, el segundo grupo extiende el concepto hasta cuestiones de derechos humanos y desarrollo, y rechaza que las consecuencias humanas de una guerra sean las condicionantes para atender asuntos de seguridad humana, pues para

---

[96] Pérez de Armiño, Karlos, "El concepto y el uso de la seguridad humana: análisis crítico de sus potencialidades y riesgos", en *Revista CIDOB d'Afers Internacionals, Seguridad Humana: conceptos, experiencias y propuestas*, Núm. 76, Fundación CIDOB, España, p. 62.

[97] Zavaleta, Sandra, *Op. Cit.*, p.132.

[98] Rosas, María Cristina (Coord.), *La seguridad por otros medios. Evolución de la agenda de seguridad internacional en el siglo XXI: lecciones para México*, La Seguridad Humana: ¿Nuevo Paradigma para la Seguridad Nacional de México en el Siglo XXI?, Ed. Centro de Análisis e Investigación sobre Paz, Seguridad y Desarrollo Olof Palme A.C., México, 2011.

[99] La Dra. María Cristina Rosas explica dos acepciones del término *Seguritizar.* El primero y positivo se refiere a poner en relieve un tema para coronarlo como prioridad; sin embargo, el segundo y negativo hace alusión a poner cualquier tema o amenaza como un problema de seguridad.

algunas personas, la idea de tener un empleo bien remunerado o el acceso a los servicios de salud, por ejemplo, les da la idea de una vida segura.

La Cumbre del Milenio, celebrada en septiembre del año 2000, fue probablemente el trabajo más ambicioso respecto a la nueva agenda de seguridad internacional; estuvo conformada por la pobreza, los refugiados, la migración, el cambio climático, la escasez de alimentos, las epidemias, entre otros asuntos. Sin embargo, al año siguiente, los ataques terroristas del 11 de septiembre viraron todos los esfuerzos en materia de seguridad humana, para posicionar nuevamente la seguridad nacional en la cima de la agenda de seguridad mundial.

Empero, a lo largo de la primera década del siglo XXI, diversos acontecimientos, como el huracán Katrina, la influenza AH1N1 o los terremotos en Haití y Chile, terminarían por convencer al mundo entero que la necesidad de ampliar la agenda de seguridad de los estados era inminente.

El mundo ha cambiado y resulta insostenible mantener como única prioridad los conflictos bélicos tradicionales, por ello, una definición actualizada del concepto de seguridad nacional es la de Edmundo Hernández-Vela, el cuál sale de la concepción tradicional y nos acerca al concepto amplio:

> La seguridad nacional es el conjunto de políticas, estrategias, normas, instituciones y acciones que tienden a la armonización plena de los elementos constitutivos del Estado, protegiéndolos y salvaguardándolos de actos o situaciones de cualquier naturaleza, internos o externos, que perjudiquen o afecten de alguna manera su integridad o su óptimo desempeño y aprovechamiento en el impulso del proceso de desarrollo y el progreso del país en todos los órdenes.[100]

### 1.3.3. El binomio seguridad-desarrollo.

La desaparición de la amenaza socialista y el fortalecimiento de la hegemonía de Estados Unidos, así como de la economía capitalista, trajo consigo la inserción de un “Nuevo Orden Internacional” que, aunado a la proliferación de organismos

[100] Hernández-Vela Salgado, Edmundo, *Diccionario de Política Internacional*, Tomo II (Letras J-Z), Sexta Edición, Ed. Porrúa, p. 1094.

internacionales, se ponderaron las relaciones internacionales basadas en la cooperación.

En septiembre del 2000 se celebró la denominada “Cumbre del Milenio”, donde 189 países adoptaron la Declaración del Milenio. En dicho documento se acordaron ocho ambiciosos objetivos, llamados los Objetivos de Desarrollo del Milenio (ODM), cuyo cumplimiento debía alcanzarse para el año 2015.

Reducir la pobreza, mejorar los niveles de bienestar y generar oportunidades de desarrollo de los pueblos eran las metas más importantes para medir la eficacia de las políticas nacionales e internacionales. Los ODM constituyen el primer marco acordado por consenso, con el respaldo de la mayoría de los países que forman la comunidad internacional y que establecen medidas concretas para cumplirse en un periodo determinado.

Después del 2015, grandes asuntos quedaron aún sin resolverse, por lo que la agenda de desarrollo se redefinió para un periodo entre el 2017 y 2030. Los nuevos objetivos, son un listado de 17 objetivos y 169 metas llamados los Objetivos de Desarrollo Sostenible, con los que se pretende “liberar a la humanidad de la tiranía de la pobreza y las privaciones, y a sanar y proteger nuestro planeta”, asimismo, se puntualiza el carácter integrado e indivisible, así como la conjugación de las tres dimensiones de carácter sostenible: económica, social y ambiental.[101]

Los objetivos antes citados son un trabajo sin precedentes en cuanto a cooperación multilateral se refiere y en beneficio de la seguridad y el desarrollo humanos.

Tal como ocurrió con la seguridad y el desarrollo, el concepto de cooperación también tuvo que reedificarse a través de la historia y, actualmente, podemos comprender, casi por sentido común, la problemática de cooperar o no y sus consecuencias.

[101] Organización de las Naciones Unidas, ONU, *Proyecto de documento final de la cumbre de las Naciones Unidas para la aprobación de la agenda para el desarrollo después de 2015*, Asamblea General, 12 de agosto, 2015, p. 2.

La realidad es que el mundo hoy no es el mismo que el del nuevo milenio, e incluso, ni siquiera es el mismo que hace 5 años; nos encontramos sumergidos en cambios constantes y muchas veces somos rebasados por ellos.

Si bien las amenazas tradicionales aún existen, las repercusiones de las mismas causan estragos cada vez más fuertes y se convierten en problemas de igual o mayor índole; asimismo, son estas mismas las que se generan con mayor frecuencia, durante mayor tiempo y se expanden como municiones en racimo.

Lo cierto es que no podemos ignorar ni estudiar por separado la seguridad y el desarrollo. Con el paso del tiempo ambos conceptos se estrechan cada vez más y caminan en una misma dirección; asimismo, en un mundo tan interdependiente como el actual, la cooperación resulta ser el mejor camino para sortear los problemas que acechen a la paz, la seguridad y el desarrollo mundial.

### 1.4. La interdependencia compleja.

El estudio de las Relaciones Internacionales (RI), desde finales de los años treinta y durante gran parte de la Guerra Fría, fue dominado bajo la narrativa del realismo político. Las dos grandes guerras y los primeros años de la Guerra Fría delinearon un panorama despiadadamente bélico que, coherentemente, orilló a concebir la política internacional en términos dominantemente de la guerra.

Sin embargo, más tarde, la realidad se redefinió en la época de la posguerra. A partir de la década de los setenta, autores como Robert O. Keohane y Joseph Nye cuestionaron seriamente los estatutos del realismo por considerarlos insuficientes, y desarrollaron una teoría amplia del estudio de las Relaciones Internacionales; al estudio de la guerra, se sumó el de la paz y, a partir de ello, surgió la Interdependencia Compleja.

La Guerra Fría fue marcada por el incremento exacerbado del arsenal militar de las grandes potencias, al mismo tiempo que el bipolarismo representaba la mayor amenaza a la paz mundial; sin embargo, los estragos sociales que dejaron las dos

grandes guerras y que se mantuvieron en un segundo plano, pronto comenzaron a intensificarse y a generar alerta en algunos sectores. Cuestiones relacionadas con la migración, los refugiados, las pandemias y las crisis económicas, así como medioambientales, llevaron a repensar la agenda de seguridad internacional y con ello, darle un nuevo enfoque al estudio de las relaciones internacionales.

### 1.4.1. El realismo y la interdependencia compleja.

De acuerdo con Keohane y Nye, el realismo se sustenta en tres pilares; el primero de ellos recae en la percepción de los estados como unidades racionales egoístas y predominantes en la política mundial; el segundo, justifica el uso de la fuerza como el método más eficaz para ejercer el poder; y finalmente, en consonancia con lo anterior, el tercer supuesto pondera la importancia de la seguridad militar sobre los asuntos económicos y sociales, definiendo la primera como "alta política" y a los segundos como "baja política".[102]

Para estos autores, el realismo es un tipo ideal de política mundial que define un conjunto de condiciones extremas.[103] Dentro del realismo, los conflictos entre los estados determinan la política internacional, lo que resta relevancia a nuevos actores y nuevos temas; paralelamente, la tensión bélica es una constante y la cooperación e integración entre los estados, además de ser escasa, durará solo el tiempo que sirva a los intereses propios de cada Estado.

Por su parte, la interdependencia compleja posee tres características:

1. Canales múltiples que conectan a las sociedades,
2. Ausencia de la jerarquía entre los temas, y
3. Papel menor de la fuerza militar[104]

[102] Robert O. Keohane y Joseph Nye, *Op. Cit.,* p. 126.
[103] *Ídem*.
[104] *Ibídem*, p.125.

La primera de ellas pone en relieve la existencia de otros actores que, junto a los estados, también son predominantes en la política mundial; por ejemplo, organizaciones transnacionales, organizaciones no gubernamentales (ONG's) o incluso terroristas y grupos del crimen organizado; cuyos nexos son de tipo interestatales, transgubernamentales y transnacionales. "Las relaciones interestatales son los canales normales supuestos por los realistas; las relaciones transgubernamentales aparecen cuando se flexibiliza el supuesto realista de que los estados actúan coherentemente como unidades, y las relaciones transnacionales surgen cuando se flexibiliza el supuesto de que los estados son las únicas unidades".[105]

La segunda premisa se concibe como la ampliación del concepto de seguridad y, a su vez, de la agenda internacional; por ejemplo, temas relacionados con la economía, el petróleo, las epidemias o el cambio climático, para algunos actores representan un riesgo mayor que la seguridad militar preponderante del realismo; ejemplo de ello fue, en 1994, cuando el Programa de las Naciones Unidas para el Desarrollo (PNUD) estableció el concepto de Seguridad Humana.[106]

Derivado de lo anterior, el tercer punto refiere al uso innecesario de la fuerza en algunos conflictos, contrario a los realistas que lo consideran como el método más eficaz para ejercer el poder. Para la interdependencia compleja, la cooperación y las instituciones, o lo que más tarde Joseph Nye definiría como *soft power*,[107] representa el canal idóneo para la solución de conflictos, que entre otras cosas, disminuye costos e incrementa beneficios.

La interdependencia compleja también es un tipo ideal y no pretende desacreditar al realismo; la aplicación de cada marco teórico dependerá de las situaciones en cuestión, no obstante, su espectro amplio permite adecuarse a un mayor número de las diferentes aristas de la política internacional actual.

---

[105] *Ibídem*, p. 128
[106] *Informe sobre desarrollo humano 1994*, (PNUD), *Op. Cit.*
[107] Nye Jr., Joseph S., "Soft Power", *Foreign Policy*, No. 80, Twentieth Anniversary, Autumn, 1990, pp. 153-171.

### 1.4.2. El liberalismo y la interdependencia compleja.

A lo largo de la historia, el liberalismo ha sido severamente desacreditado por la corriente realista al ser considerado ingenuo y utópico. Sin embargo, para Keohane y Nye, el liberalismo formula el argumento positivo de la política internacional, ya que pondera la importancia del progreso gradual y las libertades y los derechos individuales.

Los autores de la interdependencia compleja adoptan esta idea y la desarrollan en una más compleja, cuyo centro recae en la normatividad. El "liberalismo sofisticado", como ellos lo llamaron, considera que, para promover el bienestar económico y la justicia social, deben existir instituciones "sofisticadas" fundadas en la cooperación y que den garantía de las libertades individuales, así como rendición de cuentas.[108]

Una de las principales manifestaciones no se hizo esperar por parte de los realistas, quienes tacharon la interdependencia compleja de utópica, así como mengua con respecto al riesgo permanente de conflicto en un sistema internacional naturalmente anárquico; ante esto, Keohane y Nye argumentan que la presencia de un conflicto es inminente, sin embargo, la manera de ejercer el poder ha cambiado.

Asimismo, para llegar al liberalismo sofisticado se retoman tres perspectivas específicas del liberalismo tradicional, así como algunos precedentes de *La paz perpetua*, de Kant.[109]

El primero es el liberalismo republicano que, de acuerdo con Kant, se sostiene en el estado de derecho y la igualdad social de las repúblicas constitucionales, y junto con la teoría de la paz democrática, prescribe que las democracias liberales no hacen la guerra entre sí.[110]

[108] Borja, Arturo (Comp.)*, Op. Cit.,* p. 20.
[109] Kant, Manuel, *La paz perpetua*, Ed. Porrúa, México, 1998.
[110] Borja, Arturo (Comp.), *Op. Cit.*, p.19.

El segundo se refiere al liberalismo comercial, que, de acuerdo con los economistas clásicos y neoclásicos, para lograr una armonía natural en una sociedad libre, impulsada por el interés individual se requiere algo más que competencia, se requiere una legislación adecuada.

Por último, el liberalismo regulador es probablemente el precepto más importante para defenderse en lo que respecta al liberalismo utópico señalado por los realistas. El liberalismo regulador pone en relieve la importancia de las normas e instituciones; funciona como un ente regulador y preventivo ante las injusticias que puedan propiciarse dentro del sistema internacional. Un botón de muestra son las instituciones internacionales que se crearon los años posteriores a la Segunda Guerra Mundial; por ejemplo, el Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT, por sus siglas en inglés) y el Banco Mundial (BM).

> La creación de instituciones internacionales liberales "sofisticadas", es decir, que sean fundadas a través de la cooperación y se expandan gradualmente a través de la persuasión; que respeten las libertades individuales; que rindan cuentas a la sociedad civil internacional y que, en fin, promuevan el bienestar económico y la justicia social, resume la prescripción que se deriva de la obra de Robert Keohane.[111]

Para ello, hubo que partir de un concepto retomado de Hedley Bull[112] sobre una "sociedad transnacional" contenida en los países de Occidente, la cual comparte valores culturales importantes y se agrupa en torno a intereses específicos, sin que necesariamente exista la presencia de la figura del Estado. Pero es algo más que eso.

Para Bull, la corriente realista, al sentar su análisis en los estados como unidades egoístas y anárquicas, deja a un lado el carácter societario del sistema internacional, sin embargo, él retoma las relaciones sociales basadas en la cooperación y ayuda mutuas, aún en un contexto de anarquía.

---

[111] *Ibídem*, p.20.

[112] Bull, Hedley, *La Sociedad Anárquica. Un estudio sobre el orden en la política mundial.*, Tercera Edición, Ed. Catarata, España, 2005.

A partir de la existencia de intereses comunes y valores compartidos, es posible crear instituciones internacionales capaces de crear orden y paz internacional.

### 1.4.3. Poder.

Por tanto, el liberalismo es el preámbulo ideológico de la interdependencia compleja, sin olvidar que su apego a las normas, leyes e instituciones lo separan de la utopía. Asimismo, la existencia consciente de actores transnacionales, las relaciones que establecen y la agenda extensa de tópicos en política internacional, circunscriben un modelo internacional seriamente complejo que posee capacidades para incidir en la justicia y la paz internacionales.

Paralelamente, el concepto de poder, en la época de la posguerra, amplió sus latitudes. Keohane y Nye dieron cuenta de que la interdependencia no disminuía la consecución clásica del poder; es decir, la referente a cuestiones militares y de seguridad; sin embargo, se había extendido hacia otras áreas y con ello, se había modificado la forma de concebirlo y ejercerlo.

La asimetría es una característica natural del poder; sin embargo, contrario a la percepción unidimensional clásica del poder internacional, la interdependencia compleja, explica que la asimetría dependerá del área de política internacional en cuestión. Por ejemplo, con anterioridad, el Estado con capacidades militares más grandes, era el más fuerte; sin embargo, con la ampliación de temas en la agenda de seguridad internacional, ese Estado, no necesariamente es el más fuerte en otras áreas.

Por otro lado, los estados ya no poseen el monopolio del poder, dicho de otro modo, existen otros actores en el orbe capaces de vulnerar a los mismos estados. Los atentados del 11 de septiembre en Estados Unidos de América (EUA) y el huracán Katrina, podrían ser muestra de lo anterior. Durante la Guerra Fría, la Unión de Repúblicas Socialistas Soviéticas (URSS) era la única amenaza para EUA y hubiese resultado inimaginable que un grupo terrorista “autónomo” como Al-Qaeda pudiera vulnerar de tal manera al país más poderoso del mundo;

asimismo, años más tarde, en el 2005, el huracán Katrina causó daños de gran magnitud que puso en jaque la seguridad nacional de EUA, al mismo tiempo que evidenciaba la incapacidad del gran vencedor de la Guerra Fría, para atender temas diferentes a la seguridad militar.

La realidad es que, la seguridad militar y el uso de la fuerza no carecen de atención para la interdependencia compleja, pero si han restado eficacia en la solución de los conflictos emergentes. Hoy día, la probabilidad de enfrentar una guerra mundial como las que se han registrado en la historia es remota; pero no por ello, la seguridad nacional de los estados deja de estar amenazada.

La información sensible de los actores, así como las estructuras críticas de los estados, las cuales representan la vulnerabilidad del mismo, pueden verse amenazadas seriamente por un nuevo tópico de política internacional: el ciberespacio.

Tal como en el espacio terrestre, aéreo, marítimo y espacial, en el ciberespacio, los actores buscan la consecución de poder; sin embargo, la sociedad virtual que compone al ciberespacio carece de un poder de Estado como lo conocemos. Lo anterior no significa que no exista un control, pero sí, que como la interdependencia compleja refiere, existen nuevos actores que han superado las capacidades de los estados y que, a su vez, pueden incidir fuertemente en las relaciones de poder dentro del ciberespacio.

Asimismo, la complejidad del ciberespacio radica, entre otras cosas, en la capacidad dual para ser “juez y parte”. El realismo podría considerarlo como un mecanismo para la guerra; sin embargo, por sí solo, es ya un tema nuevo en la agenda de la política mundial y pensarlo en términos de guerra, resulta bastante limitado para un asunto de infinitas aristas.

El globalismo del que somos testigos ahora ha crecido en gran medida gracias a las Tecnologías de la Información y su contemporaneidad puede ayudarnos a repensar la manera de concebir las relaciones internacionales. Aunque presenta grandes

similitudes con el resto de los escenarios, también muestra diferencias significativas como la intangibilidad, y son estas diferencias las que lo convierten en un reto, pero al mismo tiempo, brindan la oportunidad para poner a prueba los trabajos en materia de cooperación y desarrollo.

Recientemente, muchos países han considerado la ciberseguridad un tema primordial en la agenda y el tema puede abordarse desde diversas perspectivas; sin embargo, como se ha mencionado repetidas veces, el poder que tienen los diferentes actores que convergen en el ciberespacio y que no son únicamente los estados; así como la capacidad para pensarlo en términos de seguridad y desarrollo y donde la fuerza militar carece de importancia, hace que un marco como el de Keohane y Nye sea el más idóneo para abordarlo.

## CAPÍTULO 2. El entramado normativo de la ciberseguridad.

Debido al desarrollo de las TICs, el incremento alarmante de ciberataques y ciberdelitos que se registran diariamente en el ciberespacio y el conjunto de intereses tan diversos de las partes que lo integran, la definición de instituciones y normas que estandaricen y den cauce a las necesidades en materia de ciberseguridad, han representado un reto en términos de política internacional.

Sin embargo, existen al menos seis diferentes asuntos clave a tomar en cuenta a la hora de establecer un entramado normativo concerniente a la ciberseguridad: gobernanza de Internet, libertad en Internet, privacidad en línea, ciberespionaje, cibercrimen y ciberguerra.[113]

Para hacerles frente, los regímenes normativos internacionales pueden poseer diferentes características, por ejemplo, los mecanismos (formales, informales, tratados), el nivel de soporte institucional que los envuelve, membresía (abiertos, cerrados, bilateral o multilateral, universal o afines), la función que realizan y el grado en el cual son incluidos, el sector privado u otros actores no gubernamentales, en el desarrollo o su implementación.[114]

A pesar del disentimiento entre todas las partes involucradas sobre qué es el ciberespacio y la ciberseguridad, así como la forma en que deben ser manejadas, convendría comenzar a cultivar normas generales sobre el ciberespacio, así como crear medidas de fomento de confianza (*Confidence Building Measeures, CBMs*), que puedan prevalecer y evolucionar a través del tiempo.

Las medidas de fomento de confianza son actividades llevadas a cabo conforme a acuerdos internacionales, para reducir la probabilidad de malentender el alcance, significado, intento o consecuencias, de actividades realizadas. Las CBMs incluyen el intercambio de información, pasos para incrementar la transparencia, mejoras en

[113] Clarke, Richard A., *Op. Cit.,* p. 11.
[114] *Ibídem*, p. 6.

las comunicaciones, uso de observadores y un acuerdo para limitar el alcance o naturaleza de ciertas actividades.[115]

Las normas establecen parámetros de conducta apropiada, mas no lo institucionalizan, sin embargo, el proceso de institucionalización comienza con la existencia de normas aceptadas que, posteriormente, se legalizan dentro de la esfera del derecho internacional.

El proceso de creación de estándares de conducta adecuada en el ciberespacio es el primer paso idóneo y garantiza mayores resultados debido a que supone más un acto de cooperación que de obligación. Para ello, el desarrollo de normas requiere tres aspectos: 1. Que las normas sean claras, útiles y realistas;[116] 2. Que los actores vean que el cumplimiento de las mismas genera más beneficios que costos y 3. Facilitar a los actores su cumplimiento incrementa la probabilidad de que ellos continúen con el comportamiento prescrito deseado.[117]

Las normas no se aceptan inmediatamente, por el contrario, también deben cumplir con un proceso de persuasión, aceptación y, más tarde, mecanismos que garanticen su cumplimiento, sin embargo, para que una norma sea exitosa, además de cumplir con las características anteriores, también puede hacer uso de marcos normativos ya establecidos, donde la norma nueva pueda adecuarse, por ejemplo de Derechos Humanos o de guerra; asimismo, si se trabajan los diferentes temas simultáneamente, pero por separado entre actores *likeminded*, el tiempo podrá ser más redituable que si solo se concentran todos los esfuerzos en un solo ejercicio, como son los tratados y, además, podrán propagarse con facilidad.

---

[115] *Ibídem*, p. 5.

[116] Finnemore, Martha, "Cultivating International Cyber Norms", en *America's Cyber Future: Security and Prosperity in the Information Age*, Vol. II, eds., Kristin M. Lord and Travis Sharp (Center of a New American Security: Washington, 2011), p.90.

[117] Student Conference on the United States Affairs, SCUSA 63, *Thinking Beyond Boundaries: Contemporary Challenges to U.S. Foreign Policy*, Governing Cyberspace, U.S. Military Academy at West Point, New York, 2-5 November 2011, p.2.

Por otro lado, un tratado implica la armonización de leyes internas, lo que a veces puede alentar el proceso o desmotivar a los actores; sin embargo, las normas sirven más como una herramienta complementaria a las legislaciones de cada país, y si además esto viene acompañado con asistencia técnica de actores clave, los niveles de conformidad y aceptación, pueden incrementarse considerablemente.

Los estados pueden ser persuadidos de cumplir con los marcos normativos internacionales mediante una mezcla de estímulo, coerción y presión moral; asimismo, las industrias y la sociedad civil pueden serlo a través de un proceso de enseñanza cultural, para que, así, todas las partes involucradas trabajen en conjunto y logren alcanzar una "cultura global de la ciberseguridad",[118] contrario a un tratado que toma ventaja del uso de la fuerza y la obligatoriedad, lo que, por ende, implica sanciones en caso de incumplimiento; asimismo, los estados no son los únicos actores involucrados en el ciberespacio, la tecnología se encuentra principalmente en manos privadas, lo que conlleva a un grado mayor de dificultad lograr que las empresas colaboren de la misma forma que otro Estado o tenga los mismos intereses.

Por otra parte, el consenso de definiciones seguirá en el limbo dependiendo del uso e interés que cada actor involucrado da al ciberespacio; lo que para unos representa una amenaza, para otros puede ser un derecho humano; sin embargo, las normas pueden conjugarse con estatutos o posicionamientos (*statements)*, los cuales juegan un importante rol en la definición, difusión y adopciones de normas internacionales, ya que permiten identificar actores afines y es probable incrementar una estabilidad estratégica. Es importante resaltar que las normas no garantizan que los involucrados nunca violen el conjunto de principios establecidos, pero sí pueden evidenciar a los que no cumplen, difundir en los medios entre la comunidad internacional y ejercer presión moral de esta manera.

[118] Stevens, Tim, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace", en *Contemporary Security Policy,* Vol. 33, No 1, 2012, pp. 148-170.

Dado que el Internet es omnipresente y forma parte de la vida de la mayoría de las personas, todos tienen interés en él y una percepción sobre cómo debe ser gobernado, principalmente en el ámbito militar, económico y con respecto a los grupos de la sociedad civil; por ello, no solo se debe buscar endurecer el ciberespacio, también se deben preservar las libertades de una sociedad conectada globalmente, así como lograr reducir la brecha de conectividad que existe en el mundo. Un marco normativo "justo" requiere de colaboración y diálogo entre los gobiernos y el sector privado, grupos de la sociedad civil y la academia.

**Gobernanza**

De acuerdo con la definición del *Informe sobre el desarrollo mundial 2017: La gobernanza y las leyes*, y para efectos del presente trabajo, la gobernanza es el proceso mediante el cual, actores estatales y no estatales interactúan para diseñar e implementar políticas dentro de un conjunto de reglas, formales e informales que, a su vez, dan forma y son moldeadas por el poder.[119]

Para que una política sea efectiva y se logren los objetivos de desarrollo, como son la seguridad, el crecimiento y la inhibición de los niveles de desigualdad dentro y fuera de los límites territoriales, es fundamental la decisión sobre quiénes participan, o no, en la mesa de negociación; asimismo, una mesa de negociación equilibrada brinda legitimidad sobre el entramado normativo que se adopte.

La gobernanza de Internet se ha convertido en un tema crucial, en la medida en que el Internet se fue expandiendo. Durante los primeros años de la *World Wide Web*, su funcionamiento técnico fue controlado por los estadounidenses, pero con muy poca influencia gubernamental. Incluso el Grupo de Trabajo de Ingeniería de Internet (*Internet Engineering Task Force, IETF),* creado en 1986 como un lugar para desarrollar estándares de protocolo de Internet, para asegurar que las redes

[119] World Bank. 2017. *World Development Report 2017: Governance and the Law.* Washington, DC: World Bank.

novatas operaran de forma pareja, fue conformado por investigadores, operadores y otros proveedores, pero ningún representante del gobierno.[120]

De la misma forma, hasta los primeros años de la década de los 90, el Sistema de Nombres de Dominio (*Domain Name System, DNS)*, fue dirigido mucho tiempo por un solo hombre, Jon Postel; sin embargo, en 1998, por sugerencia del Departamento de Comercio de Estados Unidos y debido al crecimiento del Internet, fue creada la Corporación de Internet para la Asignación de Nombres y Números (*Internet Corporation for Assigned Names and Numbers, ICANN*) con el fin de mejorar la administración del DNS; pero en general, la influencia del Estado en el proceso de gobernanza de Internet fue mínima y los asuntos relacionados a la ciberseguridad nacional fueron periféricos.[121]

Sin embargo, en los albores del nuevo milenio, el Internet ya se encontraba inmerso en muchas actividades de la vida diaria de diferentes grupos alrededor del mundo y por ende, se convirtió en un asunto de interés gubernamental para los estados.

En 2003 y 2005, la Cumbre Mundial sobre la Sociedad de la Información (World Summit on the Information Society, WSIS), en Ginebra y Túnez, respectivamente, dio lugar a fuertes críticas por parte de los países en desarrollo, debido a que el ICANN y el proceso de la gobernanza de Internet era dominado por Estados Unidos. Ante esto, prevaleció la decisión de preservar el modelo *multistakeholder*, dando voz y voto a los gobiernos, el sector privado y los grupos de la sociedad civil, así como una posición clara para los estados con respecto a la política pública de Internet.[122]

Como parte de estas políticas públicas, la ciberseguridad ocuparía un lugar primordial, estableciendo el derecho soberano a los estados para tratar con políticas públicas *online*, mientras se creaba un lugar no vinculante, donde se pudieran llevar a cabo discusiones sobre política pública y asuntos técnicos entre los estados y los

[120] Clarke, Richard A., *Op. Cit.,* p. 12.
[121] *Ídem*.
[122] *Ídem*.

grupos privados en el Foro de Gobernanza de Internet (*Internet Governance Forum, IGF*).[123]

En lo que respecta a las normas que establecen el rol de los gobiernos en el ciberespacio, los foros que deben liderar la gobernanza de Internet y los temas que deben ponerse sobre la mesa, aún no se han dado por sentado; sin embargo y como casi cualquier tema global, el debate se ha suscrito bajo los intereses de cada Estado y aquellos más desarrollados han tomado ventaja de sus capacidades, posicionándose por delante en las negociaciones.

El ejemplo más claro es la posición contrapuesta entre EE.UU. y China, principalmente; ambos han hecho declaraciones claras sobre lo que representa Internet para ellos y la forma de gobernarlo, dando prioridad a la seguridad y segregando el desarrollo.

Para EE.UU. es muy importante defender la infraestructura crítica, como la red de energía o los sistemas financieros; mientras que, para China o Rusia, además de esto, el libre flujo de información es una amenaza latente a su estabilidad interior.

El resto de los países ha ido trazando su ruta de afinidad hacia uno de los dos puntos, por ejemplo, los países de África y Medio Oriente presionan para un mayor rol del Estado-nación en las funciones de Internet, incluido el control directo sobre el DNS; mientras que, por otro lado, Canadá, Europa, América Latina (AL) y algunos países de Asia se han mostrado afines a los intereses de EE.UU., aunque es importante resaltar que se mantienen escépticos ante lo que parece un claro ejemplo del sistema occidental de la gobernanza de Internet.

Muchos países, donde destaca claramente EE.UU., han tomado muy en serio el ciberespacio dentro de la política interna, independientemente del sesgo internacional en la materia, incluso se ha limitado el margen de acción de los grupos

[123] *Ídem*.

no gubernamentales, subrayando las profundas divisiones de la gobernanza de Internet.

**Libertad en Internet**

El Artículo 19 de la Declaración Universal de los Derechos Humanos de 1948, señala que "Todo individuo tiene derecho a la libertad de opinión y expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión."[124]

En consonancia con lo anterior y haciendo uso de otros mecanismos, como la aprobación de la Agenda 2030 para el Desarrollo Sostenible,[125] la resolución A/HRC/20/L.13 del Consejo de Derechos Humanos de Naciones Unidas, "Afirma que los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos."[126]

También se puntualiza el uso de Internet como fuerza impulsora de la aceleración de los progresos hacia el desarrollo, por lo que exhorta a los diferentes estados a promover y facilitar la cooperación internacional encaminada al desarrollo de las TICs, así como fomentar la alfabetización digital y facilitar el acceso a la información en Internet de los pueblos con el fin de reducir la brecha digital y promover el desarrollo.[127]

---

[124] Organización de las Naciones Unidas, *Declaración Universal de los Derechos Humanos*, *Op. Cit.*

[125] Resolución 70/1 de la Asamblea General

[126] Organización de las Naciones Unidas, ONU, Asamblea General, "Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo", Resolución A/HRC/32/L.20 (2012), disponible en http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf , consultada el 19 de junio, 2017.

[127] *Ibídem*, p.3. Es importante señalar que en el proyecto de resolución no están presentes la República Popular China ni la Federación Rusa.

Asimismo, enfatiza la importancia de "instituciones nacionales democráticas y transparentes basadas en el estado de derecho, de forma tal que se asegure la libertad y la seguridad en la red para que pueda seguir siendo un motor enérgico del desarrollo económico, social y cultural."[128]

Evidentemente, deben existir algunas excepciones al derecho, como los discursos de odio, xenofobia o la pornografía infantil; sin embargo, la lucha por los derechos, como en cualquier espacio, es una lucha diaria y compete a múltiples partes, como en todo el proceso de gobernanza de Internet.

Otro esfuerzo referente a DD.HH. es la Iniciativa de Red Global (The Global Network Initiative, GNI), una organización sin fines de lucro, conformada principalmente por empresas relacionadas con las TICs, grupos de la sociedad civil, inversionistas y universidades, que han creado un conjunto de principios y guías de implementación para asegurar que empresas del sector TICs defienden la libertad de Internet. Los miembros del GNI incluyen a Google, Microsoft, Yahoo, the Center for Democracy and Technology, y Human Right Watch, y el principio fundamental recae sobre el respeto a la libertad de expresión, aun cuando exista presión de los gobiernos.

Sin embargo, aun con los esfuerzos por parte de los grupos privados en la materia, los estados siguen siendo capaces de socavar ciertos derechos humanos. En el caso de EE.UU., el ciberespacio es considerado un medio para todos los discursos (incluidos los de odio y xenofobia) y está protegido por la Primer Enmienda de la Constitución; en el caso de Europa, el ciberespacio también es considerado como un medio de expresión con la diferencia de que los discursos negativos si están criminalizados en el Protocolo Adicional de Cibercrimen de la Convención del Consejo de Europa en 2001; pero en algunos regímenes autoritarios o semi autoritarios como China, el ciberespacio funciona como el resto de los espacios físicos en esos territorios, y el gobierno ejerce el control total sobre la información como método de estabilidad del régimen.

[128] *Ibídem,* p.4.

En 2015 los países miembros de la Organización de Cooperación de Shanghai, (SCO por sus siglas en inglés, *Shanghai Cooperation Organization*)[129] presentaron, ante la Asamblea General de Naciones Unidas, un Código de Conducta Internacional para la Seguridad de la Información, mejor conocido como "El código" o *The Code*, cuya intención es empujar el debate internacional de las normas internacionales de la seguridad de la información, y forjar un consenso en el tema;[130] sin embargo, ha sido severamente criticado y debatido debido al tema de los DDHH. La narrativa de "El código" hace énfasis en la soberanía y territorialidad del ciberespacio y sobre todo este, asimismo es dominado por los imperativos de inteligencia, seguridad nacional y estabilidad de régimen.[131]

El primer trabajo de "El código" se presentó en 2011 por China, Rusia, Tayikistán y Uzbekistán; sin embargo, para el 2015 ya todos los países miembros del SCO formaban parte.

"El código" es un trabajo regional significativo, principalmente por lo que representan, en términos de poder, China y Rusia en la esfera internacional, pero principalmente porque a través de los años han ido atrayendo la atención de muchos países fuera de la región debido a que han sabido hacer buen uso (de acuerdo con sus intereses) de los riesgos y amenazas que se gestan en el ciberespacio, así como evidenciado a EE.UU. y su posición dominante.

El Internet no es objeto de un derecho humano, sin embargo, sí debería ser considerado como un bien común, por tanto, su acceso constituye un derecho humano; asimismo, dentro de él, debe prevalecer la defensa de los DD.HH y las garantías humanas más elementales a las que cualquier ser humano debe tener

[129] China, Rusia, Kazajistán, Kirguistán, Tayikistán y Uzbekistán.
[130] Organización de las Naciones Unidas, ONU, Asamblea General, "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General", Resolución A/69/273 (2015), disponible en http://www.un.org/Docs/journal/asp/ws.asp?m=A/69/723, consultada el 5 de Julio, 2017.
[131] McKune, Sarah, *An Analysis of the International Code of Conduct for Information Security*, Septiembre, 2015, disponible en https://citizenlab.org/2015/09/international-code-of-conduct/, consultada el 5 de Julio, 2017.

acceso, por ejemplo, la libertad de expresión, el derecho a la privacidad y el acceso a la información, por mencionar algunos.

### Privacidad en línea

Como en el apartado anterior, las normas que protegen la privacidad en línea tienen que ver con la ideología política de cada Estado. En teoría, los países de Occidente, a diferencia de los regímenes autoritarios o semi autoritarios, tienen estipulado el derecho a la privacidad a pesar de que, en la práctica, existen ejemplos que demuestran violaciones a este derecho.

Bajo el discurso de "mantener la seguridad nacional", muchos países llevan a cabo prácticas ilegales, mermando los avances en materia de desarrollo y violando DD.HH.; asimismo, toda la información que viaja por Internet, lo hace a través de servidores privados; es decir, el ciberespacio se ha prestado para ser un medio idóneo de negocios y transacciones multimillonarias. "Vivimos la era del bazar donde se subasta la privacidad de las personas".[132]

De esta manera se va conjugando el rol que cubren cada uno de los actores en la gobernanza del ciberespacio y la responsabilidad que tienen no solo los gobiernos, sino todos de proteger la privacidad de los datos de cada habitante del mundo, dentro y fuera de cualquier territorio.

### Ciberespionaje

Si bien la práctica del espionaje data desde muchos siglos atrás, el ciberespacio ha revolucionado la forma de llevarlo a cabo. El ciberespionaje debe distinguirse de un ciberataque debido a que no priva, en ningún momento, del uso del sistema; el daño

[132] Raphael, Ricardo, "Contra el espionaje, el periodismo", en *El Universal*, 13 de agosto, 2015, disponible en http://www.eluniversal.com.mx/entrada-de-opinion/columna/ricardo-raphael/nacion/2015/08/13/contra-el-espionaje-el-periodismo, consultada el 10 de agosto, 2015.

no es otro más que el robo de información,[133] y el objetivo es adquirir ventaja política, económica, comercial o militar con la información recabada; sin embargo, es común que a menudo se considere un "ataque". La diferencia consiste en el fin y no en los medios; es decir, a pesar de que se usen virus informáticos o mecanismos afines para llevar a cabo robo de información a gran escala, nunca se produce la disrupción o corrupción de un sistema.

Asimismo, y a diferencia de un ciberataque, el ciberespionaje raramente puede ser considerado un acto de guerra,[134] ya que, para muchos estados, se considera y se ejerce como una práctica común de inteligencia.

Por el contrario, si puede, en algunos casos, considerarse un crimen cibernético —que se estudiará más adelante—; sin embargo, es importante señalar que, en los últimos años, esta práctica ha crecido exponencialmente en cuanto a cantidad, fuerza, tamaño y forma, superando la "práctica común" y acrecentado la preocupación de la sociedad internacional por estar vigilados constantemente; aunado a esto, el espionaje cibernético ha dado pauta a lo que se conoce como espionaje corporativo, donde el Internet es visto como un negocio y considerado como la mayor transferencia de riqueza en la historia de la humanidad.[135]

Uno de los objetivos más comunes del ciberespionaje es el robo de información. Mediante esta práctica, se pueden obtener credenciales de autentificación, información personal y, ahora, datos biométricos (huellas dactilares).

Uno de los casos más representativos es el que se perpetró en julio del 2015, mediante un robo masivo a la Oficina de Administración de Personal de EE.UU.

---

[133] Libicki, Martin C, *Cyberdeterrence and Cyberwar*, RAND Corporation, Santa Mónica, 2009, disponible en http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf, consultada el 26 de Julio, 2017, p. 23.
[134] *Ídem.*
[135] Clarke, Richard A., *Op. Cit.*, p. 17.

(U.S. Office of Personnel Management, OPM), obteniendo la información de más de 20 millones de empleados federales y huellas dactilares de 5.6 millones de ellos.[136]

El gobierno estadounidense adjudicó el robo al gobierno chino, debido a los antecedentes que China tenía sobre la construcción de bases de datos masivas con información de ciudadanos estadounidenses por medio del espionaje al *Homeland Security*, así como a bases de datos de seguros médicos.[137]

De esta manera, China ha sido señalada de llevar a cabo múltiples actividades de ciberespionaje a través de la Unidad 61398, cuyo nombre formal es Segundo Bureau del Tercer Departamento del Ejército Popular de Liberación. La unidad 61398 ha sido acusada de llevar a cabo robo de documentos oficiales, propiedad intelectual, proyectos industriales, planes de negocios, estrategias de alianzas comerciales y otros textos confidenciales.[138]

Sin embargo, no solo China ocupa el lugar de experto en el ciberespionaje; probablemente el caso que mayor revuelo causó en el mundo tiene que ver con las revelaciones de Edward Snowden. En 2013, Snowden reveló la vigilancia masiva de la *U.S. National Security Agency (NSA)* hacia su población, así como a diferentes gobiernos de todo el mundo, donde destaca el monitoreo de las comunicaciones de la presidenta de Brasil, Dilma Rousseff, el presidente mexicano Felipe Calderón y, el entonces candidato presidencial, Enrique Peña Nieto.

---

[136] Peterson, Andrea, "OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought", *The Washington Post*, 23 de Septiembre, 2015, disponible en, https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?utm_term=.68e388af59bc, consultado el 04 de agosto, 2017.

[137] Nakashima, Ellen, "Chinese hack of federal personnel files included security-clearance database", *The Washington Post*, National Security, 12 de Junio, 2015, disponible en, https://www.washingtonpost.com/world/national-security/chinese-hack-of-government-network-compromises-security-clearance-files/2015/06/12/9f91f146-1135-11e5-9726-49d6fa26a8c6_story.html, consultado el 04 de agosto, 2017.

[138] BBC Mundo, "La Unidad 61398, el nuevo enemigo de EE.UU.", *BBC*, 20 de mayo de 2014, disponible en, www.bbc.com/mundo/.../05/140520_tecnologia_hackers_china_unidad_61398_mz, consultada el 04 de agosto, 2017.

El espionaje tiene sus límites sometidos a la ley y control judicial; sin embargo, las nuevas tecnologías han dejado muy al margen del espionaje tradicional las leyes y convertido el espionaje en un juego asimétrico, donde hasta hace al menos unos años, ningún Estado poseía las capacidades de EE.UU. para poder llevar a cabo espionaje de este tipo ni podía protegerse de los mismos.

El espionaje cibernético llevado a estas latitudes ha ocasionado daños importantes en las relaciones diplomáticas y en la cooperación internacional; sin embargo, existen otros casos de ciberespionaje a nivel nacional.

En 2015, se dio a conocer que la empresa italiana *Hacking Team*, creadora de *Remote Control System* (*RCS*), mejor conocida por los productos *Da Vinci* y *Galileo* y cuya especialidad es la de intervenir dispositivos móviles y obtener la mayor cantidad de información posible, había sido, irónicamente, víctima de un *hackeo.*

La información robada reveló que 30 países en el mundo contrataron sus servicios, entre ellos, diferentes instancias gubernamentales de México, principalmente el Ejército, la Marina, la Policía Federal, el Centro de Investigación y Seguridad Nacional (CISEN) y 11 gobiernos estatales, siendo México el principal cliente de *Hacking Team* al sumar 5 millones 808,875 euros.[139]

Llevar a cabo este tipo de espionaje cuesta 700 mil dólares por una instalación "media" y consiste en intervenir los dispositivos a control remoto, extraer mensajes, conversaciones e historiales, rastrear el *GPS* y activar el micrófono y cámara del dispositivo sin que el usuario pueda darse cuenta.[140]

---

[139] Sánchez Onofre, Julio, "Vulneración a Hacking Team confirma abuso de espionaje en México", en *El Economista*, 06 de Julio del 2015, disponible en http://eleconomista.com.mx/tecnociencia/2015/07/06/vulneracion-hacking-team-confirma-abuso-espionaje-mexico, consultada el 07 de agosto, 2017.

[140] Gallagher, Ryan, "Goverments turn to hacking techniques for surveillance of citizens" en *The Guardian*, Tech, 01 de noviembre, 2011, disponible en https://www.theguardian.com/technology/2011/nov/01/governments-hacking-techniques-surveillance, consultada el 04 de agosto, 2015.

De acuerdo con el informe “Hacking Team. Malware para la vigilancia en América Latina”, la interceptación de comunicaciones está regulada bajo orden judicial en cada uno de los países latinoamericanos que se relacionaron con *Hacking Team*;[141] sin embargo, el *software* es contrario a los estándares legales de cada uno y además, violatorio de los derechos a la privacidad, a la libertad de expresión y al debido proceso.[142]

Un RCS es mucho más invasivo que una mera interceptación de comunicaciones, por lo que debería existir una orden judicial por cada una de las interceptaciones; sin embargo, como no está regulado en las legislaciones, dudosamente existirá una orden judicial para acceder a los sistemas de geolocalización, por ejemplo.[143]

AL ha sido marcada históricamente bajo el sello de autoritarismos, violaciones a DD.HH., impunidad y corrupción, espiando a periodistas, disidentes políticos y defensores de DD.HH.;[144] por lo que es importante regular el uso de estas tecnologías, así como mecanismos de transparencia en el uso y adquisición de las mismas.

En el caso de México, la interceptación de comunicaciones privadas exige una orden judicial y solo puede llevarla a cabo “exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente”;[145] sin embargo, gobiernos estatales contrataron los servicios de espionaje a pesar de no estar facultados para ello. Asimismo, actividades de geolocalización o incautación no están reguladas de acuerdo con parámetros de DD.HH. y fueron llevadas a cabo.[146] Estamos frente a

[141] Los países latinoamericanos clientes de *Hacking Team* son: Brasil, Chile, Colombia, Ecuador, Honduras, México y Panamá. Argentina, Guatemala, Paraguay, Uruguay y Venezuela llevaron a cabo negociaciones pero no concretaron la compra, al menos, durante la filtración.
[142] Pérez de Acha, Gisela, *“Informe: Hacking Team. Malware para la vigilancia en América Latina”,* Derechos Digitales. Derechos Humanos y Tecnología en América Latina, Marzo, 2016.
[143] Panamá es el único país que ha abierto procesos en este caso. *Ibídem*, p. 8.
[144] *Ibídem*, p. 10.
[145] *Constitución Política de los Estados Unidos Mexicanos*, Art. 16, México, Ed. Porrúa, 2014.
[146] *Ibídem*, p. 44.

un problema, característico de la región, que recae en la mala aplicación de la ley y, en consecuencia, en abusos.

**Cibercrimen**

El uso del Internet para cometer delitos financieros es una práctica bastante común y recae en el concepto de cibercrimen; sin embargo, y a pesar de ser el área con mayor avance en cuanto a normatividad refiere, no hay un consenso sobre todo lo que engloba dicho concepto; incluso se ha hablado sobre considerar el ciberespionaje como parte del cibercrimen. Las actividades asociadas son numerosas, destacan, por ejemplo, las actividades terroristas dentro del ciberespacio, o usando éste como apoyo; el aumento de ataques a infraestructuras críticas y a todo tipo de servicios que caracterizan a las sociedades modernas; ataques por parte de los estados disfrazados de ataques perpetrados por grupos criminales, grupos de choque, activistas, etc., o ataques de civiles que poseen un mínimo de conocimiento informático, mal enfocado y que por curiosidad o simple y llana diversión pueden llevar a cabo acciones maliciosas.

En 2001, la Convención de Budapest sobre Delitos Informáticos tipificó el cibercrimen mediante las prácticas de acceso ilegal a algún sistema de cómputo ajeno, interceptación ilegal de datos, interferencia de datos y sistemas, pornografía infantil, delitos contra la propiedad intelectual y fraudes financieros o falsificaciones mediante el uso de sistemas de cómputo.[147]

La evolución del ciberespacio ha permitido, a su vez, la evolución del cibercrimen. Podemos hablar de tres generaciones: la primera es aquella en la que se hacía uso de las computadoras para llevar a cabo crímenes más complejos; la segunda, tiene que ver con ilícitos que se producen en las redes, por ejemplo, *hackeo y crackeo*.[148] La diferencia entre ambos grupos, es decir, *hackers* y *crackers*, tiene que ver con

[147] Anexo A. Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, "Título 2 – delitos informáticos", Serie de Tratados Europeos – n° 185, Budapest, 23 de noviembre, 2001.
[148] Rosas, María Cristina, "Ciberespacio, crimen organizado y seguridad nacional", en *ALAI, América Latina en Movimiento*, 09 de mayo del 2011, disponible en http://alainet.org/active/46432, consultada el 14 de agosto, 2017.

una serie de principios éticos y morales; los *hackers* han trascendido diversas generaciones bajo la idea de que la información en Internet debe ser libre,[149] y tienen como objetivo erradicar los abusos por parte de los gobiernos, así como la defensa de DD.HH., como la libertad de información y expresión;[150] por su parte, los *crackers* no se rigen bajo ningún principio ético ni moral.

La tercera generación del cibercrimen es la más compleja y se refiere a crímenes que solo pueden llevarse a cabo en el ciberespacio y operar a través de las TI; es decir, son el resultado de las oportunidades creadas por Internet y solo pueden llevarse a cabo en el ciberespacio.[151] Cristina Rosas destaca el vandalismo virtual y las descargas ilegales.

Asimismo, la criminología del cibercrimen se clasifica en: 1) crímenes que afectan la integridad de las computadoras, es decir, que vulneran la seguridad del acceso a los sistemas de red, por ejemplo *hackeo*, *crackeo*, espionaje o la denegación de servicio; 2) crímenes asistidos por computadoras, que son las actividades ilícitas que requieren de una computadora para obtener beneficios económicos principalmente, por ejemplo el *phishing,* que consiste en el robo de información mediante correos electrónicos o mensajería instantánea; y 3) crímenes por contenidos en computadoras, por ejemplo comercio y distribución de pornografía o discursos de odio e intolerancia.[152]

Dado el incremento en cantidad y peligrosidad de los diferentes ataques perpetrados, los estados han optado por defender el estado de bienestar dentro y fuera del ciberespacio mediante trabajos de ciberdefensa; es decir, la militarización de la red. Esta militarización funciona como una cuestión de derecho que permite a los estados desarrollar capacidades defensivas y ofensivas en el ciberespacio.

---

[149] McCormick, Ty, "Hacktivism: A Short History", en *Foreign Policy*, 29 de abril del 2013, disponible en http://foreignpolicy.com/2013/04/29/hacktivism-a-short-history/, consultada el 14 de agosto, 2017.
[150] Podemos destacar al grupo de *Anonymous, WikiLeaks* y E. Snowden.
[151] Rosas, María Cristina, *Op. Cit.* P. 2.
[152] *Ibídem*, p.3.

La militarización cibernética hace ruido por la ambigüedad jurídica que prevalece en el ciberespacio. Las unidades militares especiales de ciberguerra deberían ser solo la obligación que tienen los ejércitos de adecuar sus actividades a las TICs; sin embargo, la duda surge por las arbitrariedades que se cometan con el uso de las armas cibernéticas.

Otra manera de hacer frente a los ciberataques es mediante la disuasión cibernética. La disuasión se explica principalmente, en términos nucleares, como la intención, predisposición o amenaza de un Estado víctima de un ataque, hacia el atacante de hacerle un daño mayor en justa represalia y en legítima defensa;[153] sin embargo, en el ciberespacio es difícil identificar rápidamente y con certeza al atacante, por lo que la reacción al no ser inmediata no sería válida mediante el argumento de legítima defensa.

EE.UU. es uno de los países más activos en el ámbito de la disuasión cibernética. La estrategia de seguridad nacional de la Casa Blanca se basa en dos principios: defensa y disuasión.[154] El primero de ellos consiste en crear medidas de defensa más robustas para evitar ser atacados, así como mitigar planes para aislar y limitar el daño en caso de que el ataque sea exitoso;[155] el segundo, por su parte, es un poco más complejo y requiere un estudio por separado.

La disuasión cibernética demanda que EE.UU. incremente los costos asociados a una represalia, cuyo daño sea mayor al beneficio que cualquier atacante espere obtener. En el caso de las armas nucleares, la disuasión funciona porque, de acuerdo con las leyes internacionales, solo algunos países pueden desarrollar armas nucleares y su uso está controlado; sin embargo, en el caso de la disuasión cibernética, no queda claro cómo debe usarse ni que restricciones o bajo qué fundamentos; por lo que, además de costoso, podría resultar ilegítimo.

---

[153] Ganuza, Néstor, "La Situación de la Ciberseguridad en el Ámbito Internacional y en la OTAN", en *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*, Instituto Español de Estudios Estratégicos, España, 2010, p. 172.

[154] El texto original los define como *dissuasion and deterrence*; sin embargo, la traducción al español de ambos conceptos es disuasión. SCUSA 63, *Op. Cit.*, p. 3.

[155] *Ídem*.

Por lo anterior, algunos autores afirman que "el concepto de disuasión en el ciberespacio debe cambiar totalmente su filosofía y basarse en la prevención, en hacer al atacante no rentable el ataque y en una sólida colaboración internacional y no en una represalia instantánea."[156]

Continuando en la línea del cibercrimen, el 13 de mayo de 2017 se registró un ciberataque a la sede de la compañía Telefónica, en España, por medio del *ransomware* llamado *WannaCry,* que más tarde se extendió a casi 100 países. El ataque consistió en el "secuestro" de datos para posteriormente solicitar un "rescate" a través del pago de *bitcoins*.[157]

El éxito del *ransomware* se debe a la facilidad para introducirse y propagarse dentro de los sistemas *Windows*; puede llevarse a cabo a través de un correo electrónico por ejemplo o a través de un *watering hole*, que consiste en afectar una página completa, por ejemplo, la red intranet de una empresa.[158]

El ciberataque principalmente se realiza hacia las empresas con información valiosa y que están dispuestas a pagar por ella; sin embargo, en este caso también fueron atacados hospitales y centros de salud en Londres, así como oficinas gubernamentales en Rusia y Ucrania; asimismo, la cifra de rescate aumenta conforme avanza el tiempo y no es garantía de la liberación.[159]

Todos los días se llevan a cabo ataques cibernéticos de diferentes dimensiones incluso muchos de ellos van más allá de la seguridad pública en estricto sentido y llegan a niveles de seguridad nacional; sin embargo, muy pocos países tienen el poder económico para desarrollar sistemas de armamentos tan potentes para

---

[156] Ganuza, Néstor, *Op. Cit.*, p. 173.

[157] Los *bitcoins* son una moneda virtual, encriptada y difícil de rastrear.

[158] Oliveira, Joana, "El ataque de "ransomware" se extiende a escala global", en *El País*, Madrid, 15 de mayo, 2017, disponible en https://elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html?rel=mas, consultada el 31 de julio, 2017.

[159] Para más información, consultar: Mullen, Jethro, "El mundo intenta recuperarse del masivo ciberataque que afectó a casi 100 países", en *CNN*, 13 de mayo 2017, disponible en: http://cnnespanol.cnn.com/2017/05/13/el-mundo-intenta-recuperarse-del-masivo-ciberataque-que-afecto-a-casi-100-paises/ , consultada el 31 de julio, 2017.

causar el colapso de un sistema financiero, sistemas de red eléctrica o elecciones democráticas incluso, tal es el caso de EE.UU. e Israel con el gusano *Stuxnet*, o vínculos asociados con China y Rusia.

Por otro lado, hay que tener en cuenta que en el ciberespacio convergen intereses de tipo económico, político, social y cultural, y no solo militar, por ende, resulta arriesgado mirar el ciberespacio únicamente desde el prisma de la seguridad militar, dado que ello podría mermar el desarrollo y generar abusos al resto de las esferas que confluyen en él. Es importante desarrollar las capacidades técnicas, económicas y sociales de cada Estado para poder crear normas en conjunto que salvaguarden los derechos y obligaciones de cada actor involucrado; solo de esta manera podremos identificar los retos y las oportunidades que el ciberespacio tiene para todos.

**Ciberguerra**

En lo referente a las normas y tratados relacionados al cibercrimen, mucho se ha hablado sobre la necesidad de crear nuevos tratados, instituciones, organismos, etc., en la materia, o bien, adaptar lo ya existente al ciberespacio.

En el caso de la ciberguerra ocurre lo mismo; los instrumentos legales existentes sobre lo que comprende un conflicto armado y lo que constituye un objetivo legítimo, han arropado la idea de cómo y cuándo podemos hablar de ciberguerra.

Cuando un ciberataque alcanza el umbral de un conflicto armado, las reglas generales de derecho internacional referentes al uso de la fuerza y la legitima defensa juegan un papel importante, principalmente bajo la jurisdicción de la Corte Internacional de Justicia, así como la ley internacional humanitaria y de DDHH.

En términos generales, un ciberataque es considerado como una disrupción o corrupción deliberada por parte de un Estado, sobre un sistema de interés de otro

Estado;[160] asimismo, un ataque constituye un acto de guerra mediante tres formas: universalmente, multilateralmente o unilateralmente.[161]

La definición universal es aquella en la que "todos los estados" están de acuerdo; es decir, que la ONU así lo determine o que la mayoría de los estados hayan firmado un tratado relacionado. En cuanto a la definición multilateral, es cuando un grupo de países postulan lo que para ellos constituye un acto de guerra, por ejemplo la OTAN. Y, por último, la individual, ocurre cuando un Estado declara lo que para sí mismo constituye un acto de guerra; sin embargo, algunos estados pueden tomarlo como válido o no, así como los atacantes.[162]

Entre los ejemplos más significativos en la historia de los ciberataques que han evolucionado para ser considerados actos de ciberguerra, podemos identificar los casos de Estonia en 2007 y Georgia en 2008.

Los ciberataques en Estonia y Georgia se llevaron a cabo en medio de un conflicto político importante con la Federación Rusa, por lo que, entre las fricciones que ambos países mantenían con los rusos y una serie de indicadores técnicos y políticos durante los ataques, se han señalado, aunque no mediante una declaración formal, como los responsables de ambos sucesos.

El caso de Estonia se originó cuando el gobierno de Estonia tomó la decisión de reubicar el monumento conocido como "el soldado de bronce" a un panteón militar en Tallin, decisión que no fue de total agrado para la comunidad rusa, por lo simbólico que es para los rusos dicho monumento. Sin embargo, se cree que la verdadera razón fue como respuesta al desagrado por parte del Kremlin de la adhesión de Estonia a la OTAN en 2004 y la reubicación de soldado de bronce fue solo catalizador.[163]

---

[160] Traducción propia. Texto original en inglés: "[…] is the deliberate disruption or corruption by one state of a system of interest to another state." Libicki, Martin C., *Op. Cit.* P. 23.
[161] *Ibídem*, p. 179. *(Appendix A)*
[162] *Ibídem*, p. 179 y 180.
[163] Ganuza, Néstor, *Op. Cit.*, p. 177

Bajo esta situación, comenzaron manifestaciones, que pronto se intensificaron y se convirtieron en enfrentamientos violentos raramente vistos en Estonia.

Paralelo a las manifestaciones en las calles, el 27 de abril del 2007, mientras se llevaban a cabo los enfrentamientos, comenzaron los primeros ciberataques hacia varios medios de comunicación, así como a los sistemas de información de la infraestructura pública y privada. Dichos ataques consistieron principalmente en denegación de servicio (DoS), desfiguración de sitios web (*website defacement*), a servidores de sistemas de dominio (DNS por sus siglas en inglés) y mediante correo basura (*spam*).[164]

El primero de ellos (DoS), constituye uno de los ataques más comunes y consiste en bloquear a un servidor web desde un solo punto utilizando el protocolo TCP/IP, de tal manera que los usuarios legítimos no puedan acceder. Si, por el contrario, se utilizan varios puntos, se llama ataque distribuido de denegación de servicio (DDos) y se hace uso de *botnets* o robots informáticos. El ataque consiste en realizar un número enorme de peticiones simultáneas al servidor, de tal manera que se sature el ancho de banda del servidor y se produzca lo que normalmente se conoce como "caída del servidor".[165]

La desfiguración de sitios web, por su parte, consiste en acceder ilegalmente a un sitio web y modificar su contenido visible; mientras que el *spam*, que también es muy común, son aquellos mensajes que aparecen en el correo electrónico, sin haberlos solicitado y generalmente aparecen en los no deseados con contenido publicitario.[166]

Sin embargo, los ataques a los servidores de sistemas de dominio son más complejos y más peligrosos, ya que el DNS constituye una pieza fundamental para el funcionamiento de Internet.

[164] *Ibídem*, p. 180
[165] *Ibídem*, p. 181 y 182.
[166] *Ibídem*, p. 182.

> Un sistema de nombres de dominio es un sistema jerárquico que asocia información variada con nombres de dominios asignados a cada uno de los participantes en servicios o recursos conectados a Internet o a una red privada. Su función más importante, es traducir nombres inteligibles para los humanos en identificaciones binarios asociados con los equipos conectados a la red, con el propósito de poder localizar y direccionar estos equipos mundialmente.[167]

El ataque consiste en la modificación de los registros, suplantar las conexiones legítimas y manipular el acceso del usuario para redirigirlo a otros sitios web cuya naturaleza sea fraudulenta.

Estonia es uno de los países con mayor desempeño de funciones a través de las TICs, lo cual lo hizo un blanco de ataque sumamente fácil, en el sentido de que un ataque con éxito podía provocar una crisis en todas las esferas que comandan al Estado; pero también un blanco de ataque importante ya que, al ser miembro de la OTAN, el atacante buscaba poder medir la capacidad de respuesta de la organización en el área del ciberespacio.

El caso de Estonia es importante desde muchas aristas, además de las ya señaladas, por la capacidad de reacción del gobierno estonio, que es de reconocerse. En primer lugar, el gobierno dio el peso que tenía que dar a los ciberataques, dimensionándolos como una crisis que podía ser de seguridad nacional y no subestimándolos como fallas técnicas. En segundo, destaca por la capacidad de respuesta que tuvo el gobierno estonio ante los ataques. Se tomaron acciones mediante un grupo multidisciplinario y coordinado para dar todas las respuestas pertinentes, las cuales consistían en: eliminar funciones de las páginas web para poder reducir el ancho de banda, solicitar a los proveedores un aumento de la misma y finalmente cortar las conexiones con el exterior.

Cuando se dio cuenta que las páginas web estaban sobrepasando su capacidad en peticiones, se tomó la medida de eliminar ciertas funciones como comentarios, fotografías, videos y publicidad para poder liberar ancho de banda, pero los ataques comenzaron a variar en forma, por lo que se solicitó aumento de ancho de banda a

[167] *Ibídem,* p. 183.

los proveedores. A pesar de esto, no era posible mantener los servidores operativos por lo que la medida definitiva consistió en cortar conexión con el mundo.

Grupos de diferentes países llevaron a cabo acciones de cooperación internacional que consistían en rastrear el tráfico y así descubrir la procedencia de los ataques, haciendo notable que la mayoría de las peticiones provenían de servidores rusos. En primera instancia se bloqueó únicamente el tráfico de Internet procedente de ellos, pero después se multiplicaron las peticiones desde Egipto, Vietnam y Perú, países cuyas medidas jurídicas son menos desarrolladas. A partir de esto, se tomó la decisión de bloquear las conexiones con el exterior, recuperando el ancho de banda de manera casi automática.

Asimismo, hubo lecciones legales importantes dentro y fuera de Estonia. En primer lugar, porque los crímenes cibernéticos de esta magnitud no estaban previstos dentro de la ley interna; en segundo, por la poca o nula jurisdicción, disposición o capacidad del exterior.[168]

Un año más tarde, en 2008, se suscitaron los ataques a Georgia. A diferencia de Estonia, Georgia tiene poca dependencia hacia las TICs, lo que reduce el nivel de daño en caso de un ciberataque; sin embargo, esta misma característica lo limita en cuanto a capacidad de respuesta se refiere.

Osetia del Sur es un territorio ubicado en el Cáucaso, en la frontera entre Rusia y Georgia. Durante la existencia de la URSS ocupaba el título de Óblast dentro de la República Socialista Soviética de Georgia; sin embargo, en 1989, tras ganar una guerra con Georgia, se declaró independiente. Sin embargo, para Georgia y la comunidad internacional, Osetia del Sur seguía siendo considerado como parte del territorio georgiano, lo que ocasionó que se presentaran conflictos continuamente.

En 1992, como una medida para establecer paz, la Organización para la Seguridad y la Cooperación en Europa (OSCE) creó una fuerza de mantenimiento de la paz

[168] *Ibídem,* pp. 184-195.

conformada por tropas de Rusia, de Osetia del Sur y de Georgia, bajo el mando de la Autoridad Militar Rusa.[169]

En 2008, las Fuerzas Armadas de Georgia realizaron un ataque contra fuerzas separatistas, lo que desencadenó la Guerra de Osetia del Sur, con Georgia de un lado y Osetia del Sur, Abjasia y Rusia, por el otro. Mientras en el caso de Estonia, se desestabilizaba al Estado por medio de manifestaciones, en el caso de Georgia hablamos de operaciones militares por parte de los rusos en territorio georgiano y, más tarde, se extendió hasta el Mar Negro.

Los dos meses previos al conflicto, se llevaron a cabo los primeros ataques DDos contra sitios web oficiales de Georgia y durante la guerra se perpetraron ataques mejor organizados y coordinados contra sitios pertenecientes a la Presidencia, el Parlamento, los ministerios de Defensa y Asuntos Exteriores, así como al Banco Nacional y los principales medios de comunicación.

A medida que los conflictos armados se intensificaban, también crecían, en número, los ciberataques, ocasionando de esta manera el debilitamiento por parte del gobierno para tomar decisiones; así como de comunicación entre el gobierno y la población.

Con el término de conflicto armado, se redujeron significativamente los ciberataques; sin embargo, continuaron por algunos días más hasta desaparecer por completo debido a la poca rentabilidad que tenían.

Similar al caso de Estonia, los ataques consistieron principalmente en ataques de tipo DDos, aunque el uso de redes sociales fue de gran ayuda para que la población descargara *malware;* asimismo, los ataques iban dirigidos hacia los sitios web más importantes como la presidencia o el Parlamento, así como al Banco Nacional o el Ministerio de Defensa.

[169] *Ibídem,* p. 196.

Dada la poca capacidad técnica de Georgia respecto a las TICs, la ayuda y cooperación internacional fue fundamental. Las respuestas consistieron en bloquear el dominio ".ru" y el traslado de sitios web a otras plataformas fuera de las fronteras georgianas.[170]

Un tercer caso tuvo lugar en diciembre del 2015, cuando Ucrania sufrió un ataque a su sistema de red eléctrica, provocando un corte de energía significativo. El ataque se atribuyó a Rusia por parte del gobierno de Kiev, precedido por una investigación llevada a cabo por varias firmas encargadas de la ciberseguridad. La investigación reveló que el ataque se debió a un *malware* que pudo introducirse exitosamente en el sistema de infraestructura eléctrica de Ucrania, logrando desconectar las subestaciones eléctricas.[171]

Debido a que las TICs son esenciales para el buen funcionamiento de los estados modernos, las vulnerabilidades en los sistemas de comunicación han preocupado a los estados, en términos de los efectos potenciales para la seguridad nacional y la economía mundial y han posicionado el tema del ciberespacio como prioridad en la agenda de estrategia y política nacional e internacional.

Sin embargo, mientras los países más desarrollados crean ejércitos cibernéticos entrenados para atacar y contraatacar, existen muchos países cuyas capacidades tecnológicas y de defensa son pocas o nulas, lo que limita su participación en las negociaciones en la materia o es difícil que puedan, desde el interior, trabajar de una manera conjunta con el resto del mundo, lo cual nos lleva a pensar que la prioridad en el ciberespacio convendría enfocarse en reducir la brecha digital, expandir los dividendos digitales y que todos los países se encuentren en igualdad de condiciones en la medida de lo posible.

---

[170] *Ibídem*, pp. 196-200.

[171] Maurer, Tim, "The New Norms: Global Cyber-Security Agreements Face Challenges", en *Carnegie. Endowment for International Peace*, 5 de Febrero, 2016, disponible en http://carnegieendowment.org/2016/02/15/new-norms-global-cyber-security-agreements-face-challenges-pub-63031, consultada el 23 de agosto, 2016.

Asimismo, y a pesar de que necesariamente deba existir un nexo territorial para llevar a cabo cualquier actividad, el ciberespacio sigue sin constituir una nueva forma de “espacio exterior” y ningún Estado puede, en una cuestión de derecho internacional, ejercer jurisdicción; sin embargo, en términos de viabilidad técnica, los estados y/o los organismos internacionales están en posición de regular la conducta en el ciberespacio y acordar reglas más específicas sobre estados específicos para regular ciertos comportamientos.

## 2.1. El debate multilateral.

La presencia de actores no estatales, como socios clave en la definición de políticas, caracteriza las discusiones en el seno de los organismos y mecanismos multilaterales. En este momento podemos afirmar que la discusión se encuentra atomizada en diversos espacios que responden a las necesidades específicas de los estados, así como del sector privado, la academia y la sociedad civil.

En términos generales, puede establecerse una clasificación simple de los esfuerzos multilaterales por dar cabida al tema de la ciberseguridad: los esfuerzos internacionales dentro y fuera de Naciones Unidas.

### 2.1.1. Esfuerzos internacionales en el marco de Naciones Unidas.

#### 2.1.1.1. El Grupo de Expertos Gubernamentales (GGE).

Las respuestas dentro de la ONU se han inscrito en los esfuerzos ya existentes en materia de seguridad internacional como de las sociedades de la información y el Internet.

El Grupo de Expertos Gubernamentales, sobre los avances de las TICs en el contexto de la seguridad internacional (GGE por sus siglas en inglés), es el principal esfuerzo por establecer una serie de estándares aplicables a todos los estados.

La Asamblea General de Naciones Unidas, estableció un Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones

en el Contexto de la Seguridad Internacional a fin de examinar las amenazas reales y potenciales, derivadas de la utilización de las TICs por los estados, así como las acciones necesarias para hacerles frente, incluidas normas, reglas, principios y medidas de fomento de la confianza. Además, el Grupo examina la forma en que el derecho internacional se aplica a las TICs por los estados.

Se han establecido cinco grupos desde 2004, siendo el quinto el correspondiente al periodo 2016/2017.[172] Los primeros tres grupos se conformaron por 15 estados, incluidos los miembros permanentes del Consejo de Seguridad de Naciones Unidas; para el cuarto grupo se aumentó la membresía a 20 países y, finalmente en el quinto grupo, son miembros 25 estados; México, por su parte, ha sido miembro durante los periodos 2004/2005, 2014/2015 y el más reciente, 2016/2017.

A partir del periodo 2009/2010, cada GGE debe presentar un reporte de resultados mediante consenso que, a pesar de no ser legalmente vinculante, ha sido de gran influencia en el campo de la ciberseguridad global. Asimismo, se le atribuyen al GGE dos grandes logros: delinear la agenda mundial de ciberseguridad e introducir el principio que el derecho internacional es aplicable al espacio digital.[173]

En 2015, considerando que las TICs pueden ser una fuerza impulsora para acelerar los progresos hacia el desarrollo y en consonancia con la necesidad de preservar la conectividad mundial y el flujo libre y seguro de la información, consideró útil señalar posibles medidas que podrían adoptarse para su labor.

Dentro de los principales resultados del Grupo, en 2015 se recomendó que los estados colaboraran para evitar la aplicación de prácticas perjudiciales en la esfera de las TICs y que no permitieran deliberadamente que su territorio fuera utilizado

[172] Periodo 2004/2005, A/RES/58/32,
Periodo 2009/2010, A/RES/60/45,
Periodo 2012/2013, A/RES/66/24,
Periodo 2014/2015, A/RES/68/243 y
Periodo 2016/2017, A/RES/70/237.
[173] Digital Watch Observatory, *UN GGE*, disponible en https://dig.watch/processes/ungge, consultada el 12 de septiembre, 2017.

para que se cometan hechos internacionalmente ilícitos mediante esas tecnologías. También abogó para que se incrementara el intercambio de información y la asistencia para entablar acciones penales por el uso de las TICs con fines terroristas y delictivos, haciendo hincapié en que los estados deberían garantizar el pleno respeto de los derechos humanos, incluido a la privacidad y la libertad de expresión.[174]

Una recomendación importante fue que un estado no debería realizar o apoyar de forma deliberada actividades en la esfera de las TICs que dañaran intencionadamente infraestructuras críticas o medidas apropiadas para proteger sus infraestructuras críticas frente a las amenazas relacionadas con las TICs. Asimismo, los estados no deberían dañar los sistemas de información de los equipos autorizados de respuesta a emergencias de otro Estado ni utilizar esos equipos para participar en una actividad internacional malintencionada. Los estados deberían alentar la divulgación responsable de las vulnerabilidades de las TICs y adoptar las medidas pertinentes para garantizar la integridad de la cadena de suministro y evitar la proliferación de técnicas e instrumentos malintencionados en la esfera de las TICs o funciones ocultas y dañinas.[175]

Destacan los resultados del periodo 2014/2015 por el progreso y éxito que representaron para el grupo, en comparación con los tres periodos que lo precedieron, asimismo, el cuarto periodo tuvo el aval del G20, consiguiendo de esta manera mayor legitimidad; sin embargo, en el último periodo se imposibilitó la entrega de un reporte consensuado de resultados para 2017.

Para lo anterior hay varias explicaciones, podemos empezar por el aumento en el número de miembros, que de los 15 originales se llegó a 25, ocasionando, de esta manera, que la mesa de negociación acogiera un mayor número de intereses y por ende una mayor dificultad para alcanzar acuerdos.[176] Sin embargo, de acuerdo con

[174] Maurer, Tim, *Op. Cit.*
[175] *Ídem.*
[176] Nye, Joseph S., "Controlling Cyber Conflict" en *Project Syndicate. The World´s opinion page*, 8 de Agosto, 2017, disponible en http://prosyn.org/0jHrDb3, consultada el 13 de septiembre, 2017.

Tim Maurer, el grupo se mantiene dividido en dos lados; el primero liderado por China y Rusia, y el segundo, por EE.UU.

A principios del 2017 se generó el borrador de lo que sería el reporte final, el cual buscaba, establecer los pasos que deberían seguir los estados en tiempos de paz. EE.UU y países afines presionaron para que las leyes internacionales de conflictos armados, incluido el derecho a la legítima defensa, se aplicara también al ciberespacio; sin embargo, el grupo presidido por China y Rusia se mostraron renuentes, lo que ocasionó un clima hostil en las negociaciones para el grupo en su conjunto.[177]

No podemos negar que lo anterior representa un freno para el GGE; sin embargo, también invita a replantearse nuevas preguntas para lograr acuerdos más incluyentes. A pesar de no lograr un acuerdo total, las normas previamente acordadas y aceptadas, pueden seguir su curso fuera del marco del GGE, e inclusive, con formatos diferentes como el de *multistakeholders.*

A pesar de que los miembros del GGE son técnicamente asesores del Secretario General de Naciones Unidas, y no negociadores de cada Estado, tienen intereses específicos que pueden mermar los acuerdos, o como en el caso del último grupo de expertos, frenarlos por completo; sin embargo, actores afines pueden establecer un marco normativo más robusto y con mayores acuerdos, que en un futuro y con base en resultados, podrán convencer a otros actores de adherirse.

#### 2.1.1.2. Cumbre Mundial de la Sociedad de la Información (CMSI).

Asimismo, la Cumbre Mundial de la Sociedad de la Información (World Summit on the Information Society, WSIS) y el Foro de la Gobernanza de Internet (Internet Governance Forum, IGF) han recogido en sus trabajos, la importancia de la ciberseguridad como uno de los componentes en la definición de la gobernanza del ciberespacio.

[177] *Ídem*.

Bajo la Resolución 56/183 de la Asamblea General de la ONU en diciembre de 2001, se aprobó llevar a cabo la Cumbre Mundial de la Sociedad de la Información en dos partes. La primera tuvo lugar en Ginebra en diciembre de 2003 y la segunda en Túnez en noviembre de 2005.

Bajo el amparo de Naciones Unidas y el entonces secretario General Kofi Annan, se coordinaron los esfuerzos para llevar a cabo la cumbre, y se designó a la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés) como organismo encargado de la organización.

En ambas fases se reunieron jefes de Estado o Gobierno, representantes de todos los organismos competentes de las Naciones Unidas y otras organizaciones internacionales, organizaciones no gubernamentales, sector privado, sociedad civil y medios de comunicación, lo que se tradujo, en Ginebra, en más de 11,000 participantes de 175 países y, en Túnez, más de 19,000 participantes de 174 países.[178]

La Cumbre aprobó una Declaración de Principios y un Plan de Acción, encaminados a facilitar el crecimiento de la sociedad de la información y lograr el principal propósito de reducir la brecha digital en todo el mundo.[179]

Se rescatan los esfuerzos de la WSIS para posicionar en el centro del debate al ser humano y el desarrollo, y no la tecnología, así como el interés por construir una Sociedad de la Información incluyente, equitativa y que atienda las necesidades humanas, a pesar de no tener muy claro cómo hacerlo.

En el 2013, diez años después de la Cumbre de Ginebra, se llevó a cabo el proceso de revisión de resultados llamado CMSI+10; a partir de ella se buscaba extender la CMSI a sesiones plenarias, conferencias magistrales, reuniones temáticas

[178]International Telecommunication Union, ITU, Cumbre Mundial sobre la Sociedad de la Información, Ginebra 2003 – Túnez 2005, sitio web: http://www.itu.int/net/wsis/basic/about-es.html.
[179]Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, UNESCO, Comunicación e Información, UNESCO y la CMSI, sitio web: http://www.unesco.org/new/es/communication-and-information/unesco-and-wsis/about/.

orientadas hacia el futuro, la creación de un evento especial de alto nivel sobre el Internet dentro del mandato de la UNESCO, mesas redondas de alto nivel, la creación del Foro del Futuro Unesco, reuniones de trabajo y de alto nivel del Grupo de las Naciones Unidas sobre la Sociedad de la Información (United Nations Group on the Information Society, UNGIS), así como otras reuniones que incluyeron 10 reuniones relacionadas con la WSIS por la FIPA (Foundation for Intelligent Physical Agents), Premios de la Cumbre Mundial (PCM), lanzamiento de publicaciones, y la reunión del grupo de Trabajo en la Educación de la Comisión de Banda Ancha.[180]

Como se hizo mención, en los albores del nuevo milenio se llevaron a cabo cumbres sobre diferentes temas relativos a la nueva agenda de seguridad internacional, por ejemplo, los ODM o la Cumbre sobre el cambio climático. Al propio tiempo tuvo lugar la WSIS; sin embargo, aunado a las desigualdades sociales y los problemas de desarrollo que enfrentan gran parte de los pueblos alrededor del mundo, el Internet carecía de medidas claves y específicas, como gobernabilidad, marcos regulatorios y políticas adecuadas, etc., que aún hoy son inexistentes, y que permearon el alcance de resultados; sin embargo, y como en el caso del GGE, las lecciones aprendidas son importantes y las interrogantes que surgen, marcan el camino que deben seguir las negociaciones.

Dar un primer paso y poner sobre la mesa la importancia de las TICs para el desarrollo y seguridad humana es de suma importancia; la WSIS sensibilizó a las partes e indudablemente dio pauta para llevar a cabo procesos nacionales o iniciativas sobre la importancia e impacto de las políticas de las TICs en el progreso y desarrollo de los pueblos. Asimismo, es plausible el formato *multistakeholder* y el trabajo que ha logrado la sociedad civil a partir de la WSIS.

[180] Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, UNESCO, Comunicación e Información, Acerca de la CMSI+10, sitio web: http://www.unesco.org/new/es/communication-and-information/wsis-10-review-event-25-27-february-2013/about-wsis-10/.

Además de los documentos finales, la WSIS también dio lugar al IGF, descrito como un espacio de diálogo de múltiples partes interesadas sobre cuestiones políticas pertenecientes a Internet.[181]

Hasta el momento no existe un documento negociado; sin embargo, es una plataforma de debate entre personas de diferentes grupos, que informa e inspira a aquellos con el poder para influir en el diseño e instrumentación de políticas tanto el sector público como en el privado.[182]

#### 2.1.1.3. Código Internacional de Conducta para la Seguridad de la Información.

Por último, podemos mencionar el Código Internacional de Conducta para la Seguridad de la Información, establecido por el SCO, lo que lo posiciona como un acuerdo regional, pero que ha sido presentado ante Naciones Unidas.

Como se expuso, el Código Internacional de Conducta para la Seguridad de la Información es un acuerdo regional por parte de los estados miembro del SCO, cuya radiografía muestra su interés por crear un consenso internacional sobre ciertas normas de conducta, donde el principal objetivo recae en mantener la noción de soberanía y territorialidad de los espacios físicos, en el ciberespacio; es decir, que cada Estado, tenga la libertad, pero principalmente el derecho, de establecer control y jurisdicción interna sobre el ciberespacio.

El SCO tiene su origen en 2001 como un foro clave de la región, cuya misión es generar un consenso normativo y legal mediante prácticas de cooperación, en lo que para ellos constituye una amenaza. En primer momento, dichas amenazas consistían en el terrorismo, el separatismo y el extremismo; sin embargo, la seguridad de la información se unió a este listado como una amenaza latente a la seguridad nacional y con la creación del código, los países del SCO buscan extender el consenso a nivel internacional.

[181] Internet Governance Forum, IGF 2016, Jalisco, México, sitio web: http://www.igf2016.mx/es/.
[182] *Ídem.*

Es esta esfera, el código ha hecho “ruido” en materia de DD.HH. debido al régimen autoritario focalizado en los países del SCO y por la intención de que la seguridad de la información contempla el control sobre los contenidos y el intercambio de la misma a través de los medios digitales.

### 2.1.2. Esfuerzos internacionales fuera del marco de Naciones Unidas.

#### 2.1.2.1. Convenio sobre la Ciberdelincuencia (Convenio de Budapest).

Las respuestas en otros organismos y mecanismos multilaterales son diversas; todas representan esfuerzos específicos para abordar o segmentos específicos de la seguridad cibernética o campos de acción regionales delimitados.

Sin embargo, también destacan los esfuerzos por diseñar un entramado legal que dé soporte a las acciones que realizan los estados tanto en prevención como en aplicación de la ley. El Convenio 185 del Consejo de Europa sobre Ciberdelincuencia (Convenio de Budapest) es uno de los esfuerzos para establecer estándares y mecanismos de cooperación para actuar ante incidentes que pongan en riesgo la seguridad pública.

En el marco de la nueva agenda internacional y bajo el umbral del multilateralismo del nuevo milenio, la gobernanza del ciberespacio comenzó a perfilarse dentro de las principales preocupaciones para la sociedad internacional.

El 23 de noviembre de 2001, en Budapest, Hungría, se firmó el Convenio sobre la Ciberdelincuencia, único acuerdo internacional en la materia, presidido por el Consejo de Europa y cuyo objetivo recae en la cooperación internacional y la asistencia mutua para el establecimiento de una política penal común en la materia.

El Convenio de Budapest se compone de 48 artículos, siendo los más significativos los referentes a la tipificación del delito informático, el derecho procesal, la cooperación internacional y la asistencia mutua.

#### 2.1.2.2. Conferencia Global sobre el Ciberespacio.

La Conferencia Global sobre Ciberespacio es un mecanismo *multistakeholder,* que busca acercar a los tomadores de decisión con expertos y miembros del sector privado para debatir sobre los retos y oportunidades de un Internet abierto, libre y seguro. Se han celebrado reuniones en Londres (2011), Budapest (2012), Seúl (2013) y La Haya (2015).

Los principales temas abordados por la Conferencia a lo largo de las ediciones se pueden agrupar en tres:

1. Apoyo a la cooperación práctica en el ciberespacio: Se busca desarrollar conjuntamente respuestas prácticas a nivel mundial, a los retos urgentes, tales como delitos cibernéticos y el enjuiciamiento, la mejora de la cooperación CERT y la adopción de medidas técnicas para salvaguardar Internet.

2. Promover la creación de capacidades y el intercambio de conocimientos en el ciberespacio: La Conferencia ha promovido la creación de una Iniciativa Resiliencia Cibernética Global, donde todos los socios pueden compartir su experiencia cibernética y trabajar juntos.

3. Discutir las normas de comportamiento responsable en el ciberespacio: se busca promover el consenso sobre las normas relativas a garantizar la ciberseguridad, la lucha contra la ciberdelincuencia y hacer frente a las amenazas a la estabilidad internacional. Asimismo, se ha incorporado el debate internacional sobre los derechos humanos y la privacidad en Internet.

En el marco de la Conferencia de 2015, celebrada en La Haya, Holanda, se creó el Foro Mundial de Experiencias Cibernéticas (GFCE, por sus siglas en inglés). Dicho foro busca respaldar proyectos específicos en materia de ciberseguridad.

### 2.1.2.3. Organización de Estados Americanos (OEA).

En este último punto, la OEA, a través del Comité Interamericano contra el Terrorismo (CICTE), desarrolla un programa específico sobre el tema que ha permitido a los países de hemisferio desarrollar capacidades y compartir experiencias y buenas prácticas en la materia.

En 2004, los estados miembros aprobaron la Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética en la resolución AG/RES. 2004 (XXXIV-O/04), donde, entre los objetivos más destacables, se encuentra el establecimiento de Equipos de Respuesta a Incidentes (CSIRT) en cada país; una red de alerta Hemisférica capaz de proporcionar asistencia técnica; promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética; y fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el Hemisferio.[183]

Asimismo, el 7 de abril, mediante la Resolución CICTE/RES.1/17, el CICTE estableció el Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio, donde resuelve:

> Establecer un Grupo de Trabajo para que elabore un conjunto de Medidas de Fomento de Cooperación y Confianza en el Ciberespacio, el cual deberá elaborar una serie de proyectos de Medidas de Fomento de la Confianza (MFCs), basadas en los informes consensuados del Grupo de Expertos Gubernamentales de las Naciones Unidas (UN-GGE) para mejorar la cooperación, la transparencia, la previsibilidad y la estabilidad, y para reducir los riesgos de malinterpretación, escalamiento y conflicto que puedan derivarse del uso de las TIC, y mantener informado sobre sus avances y actividades al Comité Interamericano contra el Terrorismo (CICTE) y a la Comisión de Seguridad Hemisférica de la OEA.[184]

Como resultado de dicha resolución, la primera reunión del Grupo de Trabajo se llevó a cabo los días 28 de febrero y 1ro. de marzo de 2018 y se presentó en dicha

[183] Organización de los Estados Americanos, OEA, *Seguridad Cibernética*, disponible en https://www.sites.oas.org/cyber/Es/Paginas/default.aspx, consultada el 14 de agosto, 2017.
[184] Resolución del Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos, CICTE/RES.1/17, 10 de abril 2017.

reunión, el Proyecto de Medidas de Fomento de la Confianza por parte de Canadá, Chile, Colombia, México y Estados Unidos, sin que hasta el momento se haya publicado el documento oficial.

Sin embargo, la Organización para la Seguridad y Cooperación en Europa (OSCE), ya ha establecido una serie de MFC regionales que son una importante referencia para lo que buscan lograr los países americanos. Dentro de las MFCs establecidas por la OSCE a través de la Decisión No. 1202, se destacan las relativas a compartir estrategias y políticas nacionales, identificar puntos de contacto nacionales, llevar a cabo reuniones y debates regulares, así como talleres, seminarios, etc., el intercambio de puntos de vista sobre amenazas e incidentes y desarrollar mecanismos y marcos de consultas para evitar percepciones erróneas y proteger infraestructuras críticas. Es importante señalar el carácter voluntario de estas medidas; nadie está obligado a cumplirlas, sin embargo, se resaltan las ventajas de cooperar y generar confianza en la región para fortalecer la seguridad cibernética y los costos que implicaría no hacerlo.

La ambigüedad legal en el ciberespacio, como resultado de intereses específicos, ha facilitado que las actividades delictivas sean cada vez más comunes y la capacidad para prevenirlas y mitigarlas se vea acortada. Sin embargo, la falta de consenso en la institucionalización de normas no debería de ser un obstáculo para trabajar en los procesos que garanticen la seguridad.

La cooperación internacional a nivel técnico y entre los responsables de la formulación de políticas es esencial para maximizar los beneficios de la tecnología, al mismo tiempo que se previenen y mitigan los riesgos y se mejora la seguridad.

Para llevar a cabo el proceso de gobernanza en el ciberespacio y crear un marco normativo equitativo, los foros internacionales abiertos y de cooperación, así como el establecimiento de medidas de fomento de confianza voluntarias, podrían significar la vía idónea para apalancar el desarrollo de los países en el ciberespacio, así como para aumentar la transparencia, la previsibilidad y la estabilidad.

En un tópico como el ciberespacio donde muchos países aún tienen muy limitadas sus capacidades, establecer otro tipo de acuerdos, como la firma de tratados, puede dar paso a otro tipo de problemas como violaciones de derechos fundamentales; asimismo, los tratados reducen su marco de acción a los estados y, tenemos claro que en el ciberespacio convergen múltiples actores con capacidades, a veces, igual o mayores a la de los estados, por ejemplo, el sector privado.

## CAPÍTULO 3. La adhesión de México al Convenio de Budapest. Escenarios para México en el ciberespacio.

Desde las diferentes formas de hacer frente a los retos internacionales, los tratados internacionales han sido un mecanismo eficiente y determinante; sin embargo, de cara al ciberespacio, como uno de los temas principales en la agenda de seguridad del nuevo milenio, los tratados internacionales son un terreno poco explorado.

El Convenio de Budapest, al ser el único tratado internacional en la materia y punto central de la investigación, resulta relevante para el análisis de una posible adopción por parte de México como escenario viable en la materia.

### 3.1. El Convenio de Budapest.

El Convenio sobre la Ciberdelincuencia del Consejo de Europa (COE) es el único tratado internacional en materia de cibercrimen. En 1997 el Consejo de Ministros de Europa nombró un Comité de Expertos del Ciberespacio para debatir el problema de la delincuencia en Internet. El Comité se conformó por policías, juristas e informáticos y se invitó, además de los países europeos, a EE.UU., Canadá, Japón y Australia, por su relevancia en la sociedad de la información.[185]

Fue firmado el 23 de noviembre de 2001, por 30 países,[186] y entró en vigor el 1ro. de julio del 2004, únicamente en 5 estados.[187] Actualmente, se ha firmado por 50 países y ratificado por 46; asimismo, 9 países están adheridos y solo 4 de los firmantes no lo han ratificado.[188]

---

[185] Salom Clotet, Juan, "El ciberespacio y el crimen organizado", en *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*, Instituto Español de Estudios Estratégicos, España, 2010, p. 136.

[186] (Intra-COE) Albania, Alemania, Armenia, Austria, Bélgica, Bulgaria, Chipre, Croacia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Italia, Macedonia, Moldavia, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, Rumania, Suecia, Suiza, y Ucrania. (Extra-COE) Canadá, Estados Unidos, Japón y Sudáfrica.

[187] Albania, Croacia, Estonia, Hungría y Lituania. Este último firmó el 23 de junio de 2003.

[188] Para ver lista actualizada, visitar: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

En el preámbulo del mismo, se hace un llamado a la intensa cooperación entre las partes involucradas (estados y el sector privado) en lo que se define como prioritario, la aplicación de “una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia”.

Asimismo, se expresa la preocupación por “el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes”.[189]

El Convenio de Budapest se considera “necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, […] y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable”.[190]

Para “garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales”[191] se hace uso de lo consagrado en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) “y otros tratados internacionales aplicables en materia de derechos humanos”, así como la Convención sobre los Derechos del Niño de las Naciones Unidas (1989) y el Convenio sobre las peores formas de trabajo infantil de la Organización Internacional del Trabajo (1999).

[189] Anexo A.
[190] *Ídem.*
[191] *Ídem.*

El Convenio se compone de 48 artículos distribuidos en 4 capítulos. El primero de ellos se refiere a la terminología y definición de sistema informático, datos informáticos, proveedor de servicios y datos relativos al tráfico.[192]

El segundo capítulo lleva por nombre “Medidas que deberán adoptarse a nivel nacional” y comprende del artículo 2 al 22, distribuidos en 3 secciones. La primera de ellas se refiere a la tipificación del delito, es decir, el Derecho penal sustantivo. Incluye los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, por ejemplo, el acceso ilícito, la interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema y el abuso de los dispositivos; los delitos informáticos, por ejemplo, falsificación informática y fraude informático; delitos relacionados con el contenido, como los delitos relacionados con la pornografía infantil; delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines; así como otras formas de responsabilidad y de sanción, como la tentativa y complicidad, responsabilidad de las personas jurídicas y las sanciones y medidas.[193]

La segunda sección se refiere al Derecho procesal. Se divide en 5 títulos y se agrupan los artículos del 14 al 21. El primer título aborda las disposiciones comunes, por ejemplo, el ámbito de aplicación de las disposiciones de procedimiento, así como las condiciones y salvaguardas; el segundo título se refiere a la conservación rápida de datos informáticos almacenados y a la conservación y revelación parcial rápidas de los datos relativos al tráfico; el título tres corresponde a la orden de presentación; el cuarto, al registro y confiscación de datos informáticos almacenados; y el título cinco a la obtención en tiempo real de datos informáticos, como los datos relativos al tráfico o la interceptación de datos relativos al contenido.[194] La sección 3, por su parte, se centra a la jurisdicción.[195]

[192] *Ibídem*, Capítulo I, artículo 1.
[193] *Ibídem*, Capítulo II, Sección 1, Títulos 1-5, artículos 2-13.
[194] *Ibídem*, Capítulo II, Sección 2, Títulos 1-5, artículos 14-21.
[195] *Ibídem*, Capítulo II, Sección 3, artículo 22.

El capítulo 3, en consecuencia, hace énfasis en la cooperación internacional. Se divide en dos secciones y comprende del artículo 23 al artículo 35.

La primera sección se refiere a los principios generales relativos a la cooperación internacional, a la extradición, la asistencia mutua y la información espontánea, y los procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables, así como la confidencialidad y restricciones de uso.[196]

La segunda sección del capítulo 3 comprende disposiciones específicas, como la asistencia mutua en materia de medidas provisionales, por ejemplo la conservación rápida de datos informáticos almacenados y la revelación rápida de datos conservados; la asistencia mutua en relación con los poderes de investigación, por ejemplo en relación con el acceso a datos almacenados, el acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público, para la obtención, en tiempo real, de datos relativos al tráfico y en relación con la interceptación de datos relativos al contenido; y por último a la Red 24/7.[197]

Por último, las cláusulas finales corresponden al capítulo 4 y están comprendidas entre los artículos 36 al 48. Dichos artículos hacen mención a la firma y entrada en vigor, la adhesión al convenio, la aplicación territorial, los efectos del convenio, las declaraciones, cláusula federal, reservas, mantenimiento y retirada de las reservas, enmiendas, solución de controversias, consultas entre las partes, denuncia y notificación.

Cabe mencionar que el Convenio de Budapest, en su Art. 42, permite hacer únicamente reservas sobre el párrafo 2 del artículo 4, el párrafo 3 del artículo 6, el párrafo 4 del artículo 9, el párrafo 3 del artículo 10, el párrafo 3 del artículo 11, el párrafo 3 del artículo 14, el párrafo 2 del artículo 22, el párrafo 4 del artículo 29 y el párrafo 1 del artículo 41.[198]

[196] *Ibídem*, Capítulo III, Sección 1, Títulos 1-4, artículos 23-28.
[197] *Ibídem*, Capítulo III, Sección 2, Títulos 1-3, artículos 29-35.
[198] *Ibídem*, Artículo 42.

Asimismo, el Consejo de Europa aprobó, el 30 de enero de 2003, el Protocolo Adicional relativos a la incriminación de actos de naturaleza xenófoba y racista, cometidos a través de sistemas informáticos en Estrasburgo, así como la de Lanzarote, del 25 de octubre de 2007, en materia de explotación y abuso sexual infantil.[199]

En adición al Convenio de Budapest, los tratados del COE de interés para la seguridad informática y la prevención y el combate de los delitos cibernéticos, además de los ya citados, incluyen el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Estrasburgo, 1981) y el Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos (Estrasburgo, 2001). El Comité contra el Cibercrimen, del Convenio de Budapest, delibera actualmente la posibilidad y conveniencia de un protocolo adicional relativo al acceso transfronterizo a datos informáticos.

En general, el Convenio de Budapest desempeña tres funciones principales: la primera es la de una base sustancial para criminalizar la ciberdelincuencia; la segunda es la de una base para recolectar y usar pruebas electrónicas; y la tercera, la de una base para la asistencia legal mutua formal y requiere que los miembros proporcionen un punto de contacto 24/7 para comunicación internacional rápida e informal.[200] Los últimos dos puntos requieren, para su implementación, de las leyes nacionales de cada país miembro.

[199] Solís, Cynthia, "La Transposición del Convenio de Budapest sobre la ciberdelincuencia en la legislación francesa en la práctica", en *Derecho y TIC. Vertientes Actuales*, UNAM, Instituto de Investigaciones Jurídicas, Serie Doctrina Jurídica, núm. 751, México, 2016. Libro completo disponible en, https://archivos.juridicas.unam.mx/www/bjv/libros/9/4065/18.pdf

[200] Hall, William, *La ciberdelincuencia y pruebas electrónicas en el Continente Americano: la perspectiva de Estados Unidos*, Departamento de Justicia de Estados Unidos, 01 de abril del 2014, disponible en https://rm.coe.int/1680303ed4.

### 3.2. México y el Convenio de Budapest

El 23 de noviembre de 2001, 30 países firmaron el Convenio de Budapest, incluidos cuatro estados no miembros del COE: Canadá, EE.UU., Japón y Sudáfrica. Actualmente, se han adherido 10 estados más Extra-COE: Australia, Chile, Costa Rica, República Dominicana, Israel, Mauricio, Panamá, Senegal, Sri Lanka y Tonga. En total son seis países del continente americano adheridos a Budapest, de los cuales cuatro pertenecen a América Latina.

México fue invitado a adherirse al Convenio de Budapest desde el 31 de enero del 2007,[201] y de acuerdo con una entrevista exclusiva para *Excélsior*, Alexander Seger, responsable de la división de ciberdelincuencia del COE y secretario del Comité del Convenio de Budapest, desde esa fecha México manifestó su interés por cooperar con otros países en la lucha contra en cibercrimen.[202] A partir de entonces, en su participación como observador permanente en el COE, México ha mostrado en reiteradas ocasiones, el interés que tiene por adherirse al Convenio de Budapest.

La posición oficial de México que se encontró al respecto es la siguiente:

> De conformidad con el proceso de consultas sostenido, hasta el momento, a nivel interno, México no tiene contemplado formular reservas al Convenio de Budapest, al momento de formalizar su adhesión al mismo.
>
> El Gobierno de México realiza –en paralelo– la armonización legislativa necesaria, para dar cabal cumplimiento a sus disposiciones.[203]

Por estar en consonancia con los intereses en materia cibernética, así como con los estándares y principios contenidos en el Convenio de Budapest sobre la Ciberdelincuencia, del 31 de marzo al 2 de abril del 2014, tuvo lugar en la Cancillería

---

[201] Gobierno de México y Consejo de Europa, Memoria del "Taller sobre legislación en materia de ciberdelincuencia en América Latina", México, D.F., 31 de marzo al 2 de abril de 2014, disponible en https://rm.coe.int/1680303ece.

[202] Hernández Aura, "Piden a México en Convenio de Budapest, ser más que un observador", en *Excélsior*, 07 de diciembre del 2016, disponible en http://www.excelsior.com.mx/hacker/2016/12/07/1132670, consultada el 03 de octubre, 2017.

[203] Secretaría de Relaciones Exteriores, SRE, *Taller sobre la Legislación en materia de Ciberdelincuencia*, México, p. 23, disponible en, https://rm.coe.int/1680303edd.

mexicana el *Taller sobre Legislación en materia de Ciberdelincuencia en América Latina,* co-auspiciado por el Gobierno de México y el COE, a fin de promover la vinculación a este instrumento de los países del continente que acudieron al evento, así como apoyar la armonización de su legislación.

El Taller consistió en dos partes, la primera, referida al marco nacional, llevada a cabo el 31 de marzo e inaugurada por la subprocuradora Jurídica y de Asuntos Internacionales de la Procuraduría General de la República (PGR), la Mtra. Mariana Benítez Tiburcio, quien manifestó que la adhesión al Convenio, así como la aprobación de las reformas necesarias para llevar a cabo la armonización jurídica en nuestro país, colocaría a México en una posición de vanguardia y liderazgo en la región en el combate a la ciberdelincuencia, con el fin de responder a las necesidades de la región.[204]

La segunda parte se centró en el marco internacional, donde se sumaron representantes de Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú y República Dominicana, así como representantes del COE, la OEA y de EE.UU.

Durante los días 1 y 2 de abril, en que se llevó a cabo esta segunda parte, el embajador Juan Manuel Gómez-Robledo Verduzco, Subsecretario para Asuntos Multilaterales y Derechos Humanos de la Cancillería, señaló que "Para México el Convenio de Budapest representa un referente obligado en los esfuerzos de la comunidad internacional en pro del fortalecimiento del Estado de derecho en el ciberespacio".[205]

Como ejes de acción, se propuso implementar de manera compartida, la actualización del marco jurídico, la adhesión al Convenio, así como el impulso a desarrollo y especialización institucional, y el desarrollo de capacidades de los

[204] Secretaría de Relaciones Internacionales, SRE, *Taller sobre legislación en materia de ciberdelincuencia en América Latina,* Prensa, 03 de abril de 2014, disponible en, https://www.gob.mx/sre/prensa/taller-sobre-legislacion-en-materia-de-ciberdelincuencia-en-america-latina-10694.
[205] *Ídem.*

servidores públicos involucrados en la persecución de tales delitos. En el ámbito nacional, se consideró como un hecho inédito las respectivas participaciones por parte de los tres Poderes de la Unión, el sector privado y la academia donde, de manera conjunta, mostraron preocupación, compromiso y la necesidad de tomar acciones inmediatas y concretas, desde sus diversos ámbitos de acción.[206]

Asimismo, dentro del taller se mencionó que, como parte del compromiso que tiene México por adherirse al Convenio de Budapest, en noviembre de 2013, el presidente Enrique Peña Nieto, presentó la Estrategia Digital Nacional (EDN), iniciativa que busca contribuir a alcanzar los objetivos relacionados al desarrollo de las tecnologías de la información y comunicación establecidas en el Plan Nacional de Desarrollo 2013-2018 (PND).[207]

De acuerdo con la página web oficial, la EDN es el plan de acción que el gobierno está implementando para construir un México Digital, en el que la tecnología y la innovación contribuyan a alcanzar las grandes metas del desarrollo del país; se compone de cinco objetivos, cinco habilitadores y 23 objetivos secundarios.[208]

También se resaltó el trabajo en conjunto que realizan las agencias y oficinas federales, incluyendo la Oficina del Fiscal General y la SRE, sobre una propuesta de borrador para modificar el Código Penal Federal (CPF), que incluya nuevos castigos y conductas relacionadas al cibercrimen. Actualmente, de acuerdo con la última reforma al CPF publicada en el *Diario Oficial de la Federación* (DOF), el 26 de junio del 2017,[209] se encontraron los siguientes artículos relacionados:

- Título Quinto, relativo a los Delitos en Materia de Vías de Comunicación y Correspondencia, por ejemplo, interrumpir o interferir comunicaciones o

[206] Secretaría de Relaciones Internacionales, SRE, *Taller sobre legislación en materia de ciberdelincuencia en América Latina*, Nota de Prensa, 01 de abril de 2014, disponible en https://www.gob.mx/sre/prensa/taller-sobre-legislacion-en-materia-de-ciberdelincuencia-en-america-latina.
[207] Gobierno de la República, *Plan Nacional de Desarrollo 2013-2018*, México.
[208] Gobierno de la República, *Estrategia Digital Nacional*, México, disponible en, https://www.gob.mx/mexicodigital/.
[209] Cámara de Diputados del H. Congreso de la Unión, *Código Penal Federal*, Texto Vigente, Última reforma publicada DOF 26-06-2017, disponible en, http://www.diputados.gob.mx/LeyesBiblio/pdf/9_260617.pdf.

violar correspondencia, así como intervenir comunicaciones privadas sin un mandato de una autoridad judicial competente;

- Título Sexto, Art. 178 Bis. del Capítulo I, relativo a los Delitos Contra la Autoridad, específicamente la desobediencia y resistencia de particulares, por ejemplo, al no "colaborar o aportar información para la localización geográfica, en tiempo real de los dispositivos de comunicación en términos de lo dispuesto por la Ley Federal de Telecomunicaciones y Radiodifusión […]"
- Título Octavo, Capítulo II, Art. 202, relativo a la pornografía infantil;
- Título Noveno, relativo a la revelación de secretos y acceso ilícito a sistemas y equipos de informática, incluido en los dos capítulos que lo comprenden.

En general, los títulos de mayor impacto, en cuanto a las TICs refiere, son el Octavo y Noveno relacionados con la prevención de conductas criminales contra niños y adolescentes mediante las TICs y el acceso ilícito a los sistemas y equipos de informática; sin embargo, en los artículos relativos al terrorismo, no se hace mención alguna acerca del terrorismo cibernético o el uso de las TICs para llevar a cabo terrorismo.

En la memoria del Taller se puede comprobar el esfuerzo, preocupación y compromiso no solo de México, sino de todos los participantes, en los retos y oportunidades que ofrece el ciberespacio, destacando la urgencia de adecuar el marco legal correspondiente de cada país, a la realidad. Sin embargo, posterior a esa fecha, no se han llevado a cabo talleres similares que permitan dar seguimiento y continuidad.

En el caso de México, la postura oficial citada en los primeros párrafos de este apartado se recogió de la misma memoria del Taller; sin embargo, para efectos del presente trabajo, a través de la Plataforma Nacional de Transparencia (PNT), se registraron 12 solicitudes a diferentes dependencias de la Federación, para conocer

"La posición oficial de México respecto a la adhesión al Convenio de Budapest, así como los avances en la materia".[210]

De las 12 solicitudes, 10 fueron canalizadas a la SRE por ser tema de competencia para la dependencia; la PGR solicitó ampliar la solicitud y la SRE mediante la consulta de la Consultoría Jurídica, la Dirección General para Europa y la Dirección General para la Organización de las Naciones Unidas, respondió lo siguiente:

> "[…] el Ejecutivo Federal se encuentra evaluando las disposiciones del Convenio a fin de determinar si el marco jurídico vigente permitiría cumplir con las obligaciones contenidas en el mismo.
>
> Una vez que este análisis concluya, se estará en aptitud de considerar la viabilidad de que el Estado mexicano se adhiera al Convenio, o bien identificar las medidas legislativas que sería menester implementar para poder ser parte de este Instrumento."[211]

Asimismo, en el Taller, México puntualizó que la culminación de la adhesión de nuestro país a dicho tratado se efectuaría en diciembre 2014 o enero 2015,[212] sin que en hasta ahora se haya llevado a cabo la misma ni se tenga actualización alguna.

---

[210] Las solicitudes registradas son: Cámara de Diputados, núm. 0120000174517, 17 de octubre de 2017, (respuesta vía electrónica en formato PDF),
Centro de Investigación y Seguridad Nacional, núm. 0410000026917, 17 de octubre de 2017,
Instituto Mexicano de la Propiedad Industrial, núm. 1026500117817, 10 de noviembre de 2017,
Instituto Federal de Telecomunicaciones, núm. 0912100073517, 7 de octubre de 2017,
PGR-Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia, núm. 1700400028017, 26 de octubre de 2017,
Policía Federal, núm. 0413100106517, 17 de octubre de 2017,
Procuraduría General de la República (PGR), núm. 0001700291717, 29 de noviembre de 2017,
Secretaría de Gobernación (SEGOB), núm. 0000400265817, 17 de octubre de 2017,
Secretaría de la Defensa Nacional (SEDENA), núm. 0000700205717, 06 de noviembre de 2017,
Secretaría de Relaciones Exteriores (SRE), núm. 0000500215217, 19 de octubre de 2017,
SRE-Agencia Mexicana de Cooperación Internacional para el Desarrollo (AMEXCID), núm. 0510000005117, 17 de octubre de 2017,
Universidad Nacional Autónoma de México (UNAM), núm. 6440000173717, 17 de octubre de 2017.

[211] Anexo B. Secretaría de Relaciones Exteriores, SRE, Oficio núm. UDT-6983/2017, Folio: 0000500215217, como respuesta a la solicitud presentada a través del sistema Plataforma Nacional de Transparencia, Ciudad de México, 18 de octubre, 2017.

[212] Consejo de Europa, COE, *Mexico, Status regarding Budapest Convention*, última actualización: 23 de noviembre de 2014, disponible en, http://www.coe.int/fr/web/octopus/-/mexico.

Por otro lado, los cuatro estados pertenecientes a AL, que han sido adheridos al Convenio de Budapest, son los siguientes:

**CHILE**[213]

El 27 de abril de 2017, la presidenta Michelle Bachelet promulgó la primera Política Nacional de Ciberseguridad de Chile,[214] al mismo tiempo que, por medio del Decreto no. 83., se promulgó el Convenio sobre la Ciberdelincuencia el 27 de abril del 2017 que entró en vigor el 01 de agosto del mismo año y se realizaron 5 reservas a los artículos 4, 6, 9, 22 y 29. Chile es el Estado Parte no. 54 de la Convención de Budapest.[215]

**COSTA RICA**[216]

Costa Rica fue invitada a adherirse el 1 de febrero de 2007, y 10 años después, el 3 de julio del 2017, se aprobó la Ley no. 9452 para la adhesión de Costa Rica al Convenio de Budapest[217] y como complemento a la Ley 9048 relativa a los Delitos Informáticos. Asimismo, se realizaron tres reservas relativas a los delitos contra la propiedad intelectual, la extradición de los costarricenses y la obligación de designar un "punto de contacto" para asistencia inmediata.[218] Con esto se convirtió en el

[213] Para más información sobre el perfil del país, referirse a, Organización de los Estados Americanos, OEA, en conjunto con el Banco Interamericano de Desarrollo (BID), *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?*, Informe de Seguridad 2016, Observatorio de la Ciberseguridad en América Latina y el Caribe, pp. 62 y 63.

[214] Gobierno de Chile, *Política Nacional de Ciberseguridad*, 2017-2022, disponible en http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.

[215] Consejo de Europa, "Chile's commitment to fight cybercrime", Cybercrime, News, Strasbourg, France, 27 de abril de 2017, disponible en https://www.coe.int/en/web/cybercrime/-/chile-s-commitment-to-fight-cybercrime.

[216] Para más información sobre el perfil del país, referirse a, OEA y BID, *Ibídem*, pp. 66 y 67.

[217] Hess Araya, Christian, "Aprobado convenio europeo contra la ciberdelincuencia", *La Nación*, Opinión, 04 de agosto de 2017, disponible en, http://www.nacion.com/opinion/foros/Aprobado-convenio-europeo-ciberdelincuencia_0_1650234967.html, consultada el 4 de diciembre, 2017.

[218] *Ídem.*

Estado Parte no. 56.[219] Actualmente, Costa Rica no cuenta con una Estrategia Nacional de Ciberseguridad.[220]

**PANAMÁ**[221]

Fue invitado a adherirse el 15 de noviembre de 2012 y en 2014 se confirmó su acceso, convirtiéndolo en el segundo país latinoamericano adherido al Convenio[222] y el Estado Parte no. 42 del Convenio de Budapest.[223] Asimismo, Panamá cuenta con una Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructura Crítica (ENSC+IC).

**REPÚBLICA DOMINICANA**[224]

Fue el primer país del Caribe y América Latina en ratificar el Convenio de Budapest, el 7 de febrero de 2013 y de acuerdo con la información del Estado en el sitio web del COE, ha participado activamente en el marco de la Estrategia Interamericana para Combatir Amenazas a la Ciberseguridad de la OEA y ha señalado la importancia del Convenio para proveer a las autoridades dominicanas, de herramientas necesarias para compartir información y hacer frente a los problemas relativos a los ciberdelitos y la delincuencia organizada.[225]

---

[219] Consejo de Europa, "Costa Rica joins the Budapest Convention", Cybercrime, T-CY News, Strasbourg, France, 03 de octubre de 2017, disponible en, https://www.coe.int/en/web/cybercrime/t-cy-news/-/asset_publisher/GxUcENEFhivB/content/costa-rica-joins-the-budapest-convention.

[220] Hess Araya, Christian, *Op. Cit.*

[221] Para más información sobre el perfil del país, referirse a, OEA y BID, *Ibídem*, pp. 90 y 91.

[222] Autoridad Nacional para la Innovación Gubernamental, "Panamá ratifica convenio sobre cibercrimen", Gobierno de la República de Panamá, 20 de marzo de 2014, disponible en, http://www.innovacion.gob.pa/noticia/2117.

[223] Consejo de Europa, "Panama joins Budapest Convention", Cybercrime, T-CY News, Strasbourg, France, 5 de marzo de 2014, disponible en, https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/panama-joins-budapest-convention.

[224] Para más información sobre el perfil del país, referirse a, OEA y BID, *Ibídem*, pp. 96 y 97.

[225] Consejo de Europa, "Dominican Republic", Octopus Cybercrime Community, Country Wiki, última actualización 10 de febrero de 2015, disponible en, https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/dominican-republic.

### 3.2.1. Esfuerzos por parte de México para el fortalecimiento de la seguridad cibernética.

A pesar de no haber concluido su adhesión al Convenio de Budapest, México ha avanzado considerablemente en la materia desde diversos organismos tanto nacionales como internacionales.

#### 3.2.1.1. Procesos Nacionales.

México ha impulsado procesos nacionales que permiten la armonización legislativa correspondiente, por ejemplo, como se mencionó, los delitos previstos en el Código Penal Federal como la revelación de secretos, el acceso ilícito a equipos y sistemas de informática, delitos contra derechos de autor, *hacking, cracking* informático, etc., aunque resulte insuficiente.

Igualmente, algunas Entidades Federativas han incluido en sus códigos penales, algún tipo de delito informático, por ejemplo: falsificación, producción, impresión, enajenación, distribución y alteración de documentos, principalmente aquellos referidos al crédito. El caso de Sinaloa es importante, ya que fue la primera entidad en tipificar el "delito informático" como tal y el único que lo denomina así.[226]

En el Plan Nacional de Desarrollo 2013-2018 (PND), se busca fortalecer la Responsabilidad Global del Estado Mexicano y dar cohesión a las metas de protección de datos personales (Objetivo VI.A.),[227] ciberseguridad (Estrategia 1.2.3.)[228] y el establecimiento de una Estrategia Digital Nacional en este contexto, así como el uso de tecnologías apropiadas para un México próspero (Objetivo VI.A.) y para el acceso universal a la cultura (Objetivo 3.3.).[229]

---

[226] Congreso de Sinaloa, *Código Penal para el Estado de Sinaloa*, Capítulo V, Art. 217., Texto Vigente, última reforma publicada en el P.O. No. 158 del 28 de diciembre de 2016, disponible en, http://www.congresosinaloa.gob.mx/images/congreso/leyes/zip/codigo_penal_28-dic-2016.pdf.
[227] *Op. Cit.*, México, PND, p. 104.
[228] *Ibídem*, p. 107.
[229] *Ibídem*, p. 126.

Por otro lado, entre los ejes de la Reforma Constitucional en Materia de Telecomunicaciones, Radiodifusión y Competencia Económica, firmado por el presidente de la República el 10 de junio de 2013, figuran el "fortalecimiento de derechos fundamentales (…), las libertades de expresión y de acceso a la información, así como los derechos de los usuarios de los servicios de telecomunicaciones" y el "impulso a una mayor cobertura en infraestructura".[230]

Asimismo, en la Ley de Instituciones de Crédito se sancionan las alteraciones a los medios de identificación electrónica y el acceso ilegal a los equipos electromagnéticos del sistema bancario.[231]

En el Programa para la Seguridad Nacional 2014-2018, la ciberseguridad ocupa el tercer lugar en riesgos y amenazas para nuestro país, por debajo de los desastres naturales y pandemias y la delincuencia organizada transnacional, y por encima de las fronteras, mares y flujos migratorios irregulares, así como por el terrorismo y las armas de destrucción masiva.[232]

Se considera que "debido al aumento de las amenazas vinculadas con la gestión del ciberespacio, […] el incremento de los ataques en contra de la infraestructura crítica, los intereses económicos, las redes de información y las capacidades de defensa de las naciones", es necesario que México desarrolle una política de Estado y una estrategia en materia de ciberseguridad y ciberdefensa.[233]

El Programa para la Seguridad Nacional 2014-2018, consta de dos objetivos estratégicos; el primero busca "Consolidar el Sistema de Seguridad Nacional

---

[230] Gobierno de México, Diario Oficial de la Federación, *Decreto por el que se reforman y adicionan diversas disposiciones de los artículos 6º., 7º., 27,28, 73, 78, 94 y 105 de la Constitución Política de los Estados Unidos Mexicanos, en materia de telecomunicaciones,* 11 de junio del 2013, disponible en, http://www.dof.gob.mx/nota_detalle.php?codigo=5301941&fecha=11/06/2013.

[231] Cámara de Diputados del H. Congreso de la Unión, *Ley de Instituciones de Crédito*, Capítulo IV, Art. 112 Bis., Texto Vigente, Última reforma publicada DOF 17-6-2016, disponible en, http://www.diputados.gob.mx/LeyesBiblio/pdf/43_170616.pdf.

[232] México, Presidencia de la República, *Programa para la Seguridad Nacional 2014-2018,* Diario Oficial de la Federación, 30 de abril de 2014, disponible en, http://www.presidencia.gob.mx/wp-content/uploads/2014/05/Programa-para-la-Seguridad-Nacional-Versio%CC%81n-Final.pdf.

[233] *Ibídem*, p. 64.

mediante el desarrollo y articulación permanente de los sistemas y procesos de los que dispone el Estado mexicano para asegurar la atención integral de las vulnerabilidades, los riesgos y las amenazas a la Seguridad Nacional",[234] y el segundo, "Asegurar que la política de Seguridad Nacional del Estado mexicano adopte una perspectiva multidimensional mediante la coordinación de las autoridades e instituciones competentes, para favorecer así la consecución de los objetivos e intereses nacionales".[235]

El segundo objetivo consta de tres objetivos específicos y estos, a su vez, contienen diferentes estrategias y líneas de acción. En la estrategia 2.1.2. del objetivo específico 2.1., se establece "Desarrollar una política de Estado en materia de seguridad cibernética y ciberdefensa, para proteger y promover los intereses y objetivos nacionales"[236] y cuenta cinco líneas de acción para ello.

Asimismo, en este sentido y bajo el mismo objetivo, las fuerzas armadas participan en los trabajos del Comité Especializado de Seguridad de la Información, el órgano especializado del Consejo de Seguridad Nacional encargado de la ciberseguridad y buscan fortalecer la generación de inteligencia y capacidad de respuesta, impulsando el empleo de las TICs.[237]

Además, México ha desarrollado una política de seguridad de la información en las TICs, aplicable a todas las agencias y entidades de la Administración Pública Federal, la cual está establecida en el "Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias."[238]

---

[234] *Ibídem*, Objetivo Estratégico 1, p. 71.
[235] *Ibídem*, Objetivo Estratégico 2, p. 73.
[236] *Ibídem*, p. 74.
[237] *Ibídem*, Estrategia 2.2.2., p. 75.
[238] Gobierno de México, "Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias", *Diario Oficial de la Federación*, Primera Sección, 04 de febrero de 2016, disponible en, dof.gob.mx/nota_to_doc.php?codnota=5424367.

Dentro del artículo 89 de la Constitución Política de México, relativo a las facultades y obligaciones que se otorgan al presidente de la República, se encuentra la obligación de preservar la Seguridad Nacional;[239] por lo que, para cumplir con este propósito, se creó el Consejo de Seguridad Nacional con el objetivo de establecer y articular la política en la materia. El CSN está conformado por los titulares del Poder Ejecutivo Federal, de la Secretaría de Gobernación (SEGOB), de la Secretaría de la Defensa Nacional (SEDENA), de la Secretaría de Marina (SEMAR), de la Comisión Nacional de Seguridad (CNS), de la Secretaría de Hacienda y Crédito Público (SHCP), de la Secretaría de la Función Pública (SFP), de la Secretaría de Relaciones Exteriores (SRE), de la Secretaría de Comunicaciones y Transportes (SCT), de la Procuraduría General de la República (PGR) y el director general del Centro de Investigación y Seguridad Nacional (CISEN).[240] Éste último tiene como propósito "generar inteligencia estratégica, táctica y operativa, que permita preservar la integridad, estabilidad y permanencia del Estado Mexicano, así como dar sustento a la gobernabilidad y fortalecer al estado de derecho".[241]

Asimismo, México, como otros países, ha establecido un Centro Nacional de Respuesta a Incidentes Cibernéticos, cuyo nombre oficial es Centro Especializado en Respuesta Tecnológica de México (CERT-MX). El CERT-MX forma parte de los Equipos de Respuestas a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) que existen a nivel mundial y cuya capacitación depende del Foro de Equipos de Seguridad y de Respuesta a Incidentes (FIRST, por sus siglas en inglés).

El FIRST es una asociación mundial creada en 1989, conformada por más de 70 países, cuyo objetivo es proveer a los CSIRT de las herramientas necesarias para poder responder eficazmente a incidentes de seguridad, mediante el acceso a mejores prácticas, organización de eventos y educación.[242]

---

[239] *Constitución Política de los Estados Unidos Mexicanos*, Art. 89, *Op. Cit.*
[240] Secretaría de Gobernación, CISEN, disponible en, http://www.cisen.gob.mx/cisen.htm
[241] *Ibídem*.
[242] OEA y BID, *Op. Cit.*, pp. 14.

El CERT-MX se estableció en junio de 2010 y es un equipo de respuesta a emergencias informáticas, responsable de prevenir, contener y mitigar amenazas y vulnerabilidades que se presentan en los sistemas de información.

El CERT-MX trabaja en conjunto con División Científica de la Policía Federal y se encarga de reforzar y proteger la seguridad, brinda respuestas y elabora planes y estrategias para responder ante cualquier incidente, vulnerabilidad o ataque de terceros. Sus objetivos principales son minimizar los daños ante cualquier ataque o amenaza, proveer asistencia rápida y efectiva, y ayudar a la prevención de futuros incidentes.[243] Asimismo, es la única institución acreditada a nivel federal para el intercambio de información con las policías cibernéticas nacionales e internacionales, además de contar con la capacidad de identificar y atender posibles ataques en agravio de la infraestructura gubernamental o contra la ciudadanía en general.[244]

[243] Consejo de Europa, COE, *Mexico, Status regarding Budapest Convention, Op. Cit.*

[244] Secretaría de Gobernación, Comisión Nacional de Seguridad, *Fortalece CNS estrategias para la protección del ciberespacio mexicano*, 25 de febrero de 2015, disponible en, http://www.denuncia.gob.mx/portalWebApp/wlp.c;jsessionid=n2wmJxvJv1KY2J5cWQLBTfcQrdJ4tcvV11fqhw1JQpvGGvzwLJ2s!-1886721534?__c=f7130.

En los cuadros siguientes, se encontrarán los programas de política pública relacionados con las TICs, que el gobierno federal ha impulsado durante los últimos tres sexenios:

**Cuadro 8. Programas de política pública relacionados con Tecnologías de la Información y Comunicación, 2000 – 2017.[245]**

| SEXENIO | PROGRAMAS | OBJETIVO |
|---|---|---|
| VICENTE FOX QUESADA (2000-2006) | Proyecto e-México Centros Comunitarios Digitales (CCD) | Apoyar la inclusión digital en zonas de difícil acceso. |
| | Enciclomedia | Disminuir la brecha digital en el sector educativo. |
| | RH-net | Facilitar e implementar nuevos mecanismos de organización del Sistema de Servicio Profesional de Carrera (SPC) en las dependencias de la APF.V |
| FELIPE CALDERÓN HINOJOSA (2007-2012) | Red Nacional de Impulso a la Banda Ancha (Red NIBA) | Desplegar una red dorsal de fibra óptica para ofrecer servicios de conectividad a los actores institucionales del país. |
| | Impulso a CCD | Se brindó conectividad a 14,566 CCD para cubrir la falta de disponibilidad de servicios de acceso en áreas remotas. |
| | Programa Habilidades Digitales para Todos (PHDT) | La plataforma del PHDT incluyó el uso de Aulas Telemáticas, con lo que se buscaba integrar el equipamiento de Enciclomedia (computadora, pizarrón electrónico, proyector, mesa e impresora) con un sistema de administración de contenidos educativos,un sistema de administración del portal local, pero sobre todo con una conexión a Internet de alta capacidad. |
| | Programa CompuApoyo | Trabajadores de empresas afiliadas al Instituto del Fondo Nacional para el Consumo de los Trabajadores (INFONACOT) recibían apoyo del gobierno para la adquisición de un equipo de cómputo. Para complementar el programa se otorgaba un apoyo de $500 para la contratación de Internet. |

[245] Elaboración propia

| SEXENIO | PROGRAMAS | OBJETIVO |
|---|---|---|
| ENRIQUE PEÑA NIETO (2013-2018) | Reforma en materia de Telecomunicaciones | Consideró la creación de órganos reguladores autónomos para garantizar el desarrollo eficiente de los sectores de telecomunicaciones y de radiodifusión,además de asegurar condiciones de competencia,inclusión social digital y transparencia. Se centró enla democratización de los medios de comunicación (permitiendo el acceso de la población a las tecnologías de la información y la comunicación, incluida la banda ancha), y en la creación de "reglas claras y abiertas, con una autoridad fortalecida, con límites a laconcentración, con obligaciones bien establecidas en cuanto a calidad, costo y continuidad de los servicios, donde las telecomunicaciones cumplirán mejor su papel dinamizador de la economía y de la participación social en el desarrollo nacional. |
| | Ventanilla Única Nacional | Creación y digitalización de un Catálogo Nacional de Trámites y Servicios (CNTSE); los cuales se encuentran estandarizados en sus procedimientos y normatividad en el portal gob.mx para disposición del ciudadano. |
| ENRIQUE PEÑA NIETO (2013-2018) | México Conectado | Busca garantizar el derecho constitucional de acceso a Internet de banda ancha (artículo 6º de la CPEUM),mediante el despliegue de redes de telecomunicaciones que proveen conectividad en los sitios y espacios públicos en los tres ámbitos de gobierno: federal, estatal y municipal. |
| | Programa de Inclusión Digital (PID) | Desarrollar las habilidades digitales y el pensamiento computacional para el aprendizaje de los estudiantes, contempla proveer de acceso a Internet de banda ancha, recursos digitales y equipamiento a escuelas públicas seleccionadas. |
| | Programa para el Desarrollo de la Industria de Software (PROSOFT) y la innovación | Fomentar la productividad en sectores estratégicos del país mediante la adopción de las TIC y la innovación. |
| | Red Compartida | Optimizar el uso del espectro asignado (banda 700 MHz), reducir costos e incrementar la cobertura en regiones que carecen de servicios, no inhibir las inversiones de operadores, ni generar ventajas o desventajas para alguno. |
| | Estategia Nacional de Ciberseguridad | Identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos, social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano. |

### 3.2.1.2. Procesos Internacionales

En el ámbito internacional, México participa en foros de carácter flexible como complemento a los esfuerzos de regulación, generando sinergia con el sector privado, sociedad civil, academia, etcétera.

Un ejemplo es el pronunciamiento de apoyo a las propuestas en la materia, de la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB). En abril de 2013, la XVIII COMJIB aprobó la Declaración de Viña del Mar, en la cual se acordó que las "Bases para la elaboración de un instrumento internacional en materia de cibercriminalidad",[246] sean el punto de partida hacia un convenio iberoamericano sobre cooperación, prueba, jurisdicción y competencia en esa materia.

El 9 de junio de 2014, en Madrid, el procurador General de la República, Jesús Murillo Karam, firmó la adhesión de México al "Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia",[247] de la COMJIB, y a la "Recomendación de COMJIB relativa a la Tipificación y Sanción de la Ciberdelincuencia", cuyo objeto y ámbito de aplicación se establecen en el artículo primero, siendo éste, como el mismo nombre del Convenio, reforzar la cooperación mutua de las partes para la adopción de medidas de aseguramiento y obtención de pruebas para la lucha contra la ciberdelincuencia.[248]

---

[246] XVIII Conferencia de Ministros de Justicia de los Países Iberoamericanos, *Bases para la elaboración de un instrumento internacional en materia de cibercriminalidad*, Viña del Mar, Chile, 04 y 05 de Abril del 2013, disponible en, http://comjib.org/es/xviii-conferencia-de-ministros-de-justicia-de-los-paises-iberoamericanos/.

[247] Conferencia de Ministros de Justicia de los Países Iberoamericanos, COMJIB, *México se adhiere a Convenio Iberoamericano sobre Ciberdelincuencia*, 10 de junio del 2014, disponible en, http://comjib.org/es/mexico-se-adhiere-a-convenio-iberoamericano-sobre-ciberdelincuencia/.

[248] Conferencia de Ministros de Justicia de los Países Iberoamericanos, COMJIB, Secretaría General, *Convenio Iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia*, Madrid, España, 28 de mayo del 2014, disponible en, http://www.mec.gub.uy/innovaportal/file/52706/1/ciber_convenio.pdf.

Asimismo, México forma parte de la Conferencia Global sobre Ciberespacio, donde incluso se convirtió en el primer país de AL para acoger la V Conferencia Global sobre Ciberespacio; también forma parte del Foro Mundial de Experiencias Cibernéticas (GFCE, por sus siglas en inglés) y del GGE sobre la aplicación del DI en el ciberespacio, así como la creación de medidas de fomento de confianza.

Además, México fue invitado a los debates del Manual de Tallin 2.0 sobre la aplicación del DI en ciberoperaciones en tiempos de paz, coordinado por el Centro de Excelencia de la OTAN para la Ciberseguridad (CCDCOE, por sus siglas en inglés).

Es importante señalar que ambas publicaciones del Manual de Tallin sobre el derecho internacional aplicable a la ciberguerra y a las ciberoperaciones respectivamente, están circunscritas significativamente al ámbito de los Convenios y Protocolos de Ginebra, y sin vinculatoriedad jurídica alguna. El objetivo principal de la primera edición hace referencia a las ciberoperaciones más severas, por ejemplo, las que violan la prohibición del uso de la fuerza en las relaciones internacionales, la autorización a los estados de ejercer el derecho de legítima defensa y/o lo que ocurre durante un conflicto armado. Por su parte, en la segunda edición, se suma el análisis legal de los incidentes cibernéticos a los que los estados se enfrentan día a día y que recaen sobre el umbral del uso de la fuerza y los conflictos armados.[249]

Éste documento reconoce que un ciberataque, ya sea ofensivo o defensivo, tiene el potencial de causar graves daños a las personas y la propiedad sin ajustarse necesariamente a la definición convencional de “violencia”, al tiempo de considerar, por ejemplo, que un miembro de las fuerzas armadas responsable de ciberespionaje contra el enemigo en el contexto de un conflicto armado internacional perdería, en principio, el derecho a los beneficios de ser tratado como prisionero de guerra. Tales

[249] NATO Cooperative Cyber Defense Centre of Excellence, CCDCOE, *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*, Tallin, Estonia, disponible en, https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html.

cuestiones escapan en principio al Convenio de Budapest, pero éste deja expresamente a salvo las actividades estatales de aplicación y verificación de la ley para el mantenimiento del orden público, la seguridad nacional y la investigación de delitos.[250]

En este contexto, conviene señalar que la Conferencia "Octopus" contra el cibercrimen, paralela a las sesiones del Comité del Convenio de Budapest y bajo los auspicios del COE, reúne prácticamente a todos los principales actores multilaterales, gubernamentales, no gubernamentales, académicos, tecnológicos y del sector privado de mayor peso específico en este campo, del que México también forma parte.[251]

En el ámbito de la OEA, se resolvió, a través de la resolución AG/RES,[252] el Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética dada la necesidad de proteger las infraestructuras de información mediante un enfoque integral, internacional y multidisciplinario.

Para ello, se llevaron a cabo la Conferencia Sobre Seguridad Cibernética en Buenos Aires, Argentina, en julio de 2003, y la Conferencia Especial sobre Seguridad, en México, en octubre del mismo año. Asimismo, se encomendó al Comité Interamericano contra el Terrorismo (CICTE) de la OEA, a la Comisión Interamericana de Telecomunicaciones (CITEL) y al Grupo de Expertos Gubernamentales sobre Delito Cibernético de la Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas (REMJA), la creación y desarrollo de dicha estrategia.[253]

---

[250] Leetaru, Kalev, "What Tallinn Manual 2.0 Teaches Us About The New Cyber Order", *Forbes*, 09 de febrero, 2017, disponible en, https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order/#18e068b6928b, consultada el 16 de noviembre, 2017.

[251] Council of Europe, Cybercrime, Octopus Conferences, https://www.coe.int/en/web/cybercrime/octopus-conference.

[252] Asamblea General, AG/RES. 1939 (XXXIII-O/03), *Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética*, 10 de junio de 2003, disponible en, http://www.oas.org/juridico/spanish/agres_1939.pdf.

[253] *Ídem.*

Al CICTE corresponde la "formación de una Red Interamericana de Vigilancia y Alerta para la rápida divulgación de información sobre seguridad cibernética y la respuesta a crisis, incidentes y amenazas a la seguridad informática",[254] en la cual México ha colaborado activamente mediante el CERT-MX. Por otro lado, el CITEL está encargado de la "identificación y adopción de normas técnicas para una arquitectura segura de Internet";[255] y el REMJA de "Asegurar que los Estados Miembros de la OEA cuenten con los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y a las redes de información".[256]

### 3.2.1.3. Estrategia Nacional de Ciberseguridad.

Como parte de los trabajos emprendidos por México en materia de ciberseguridad, se encuentra el desarrollo de la Estrategia Nacional de Ciberseguridad (ENCS).

A través del Programa de Seguridad Cibernética, del Comité Interamericano contra el Terrorismo (CICTE) de la OEA, México presentó, el 13 de noviembre de 2017, la ENC durante la Tercera Semana Nacional de Ciberseguridad en la Ciudad de México.[257]

El objetivo general de la ENCS es:

> Identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos, social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano.[258]

---

[254] Organización de los Estados Americanos, OEA, *Una Estrategia Interamericana Integral de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética*, AG/RES. 2004, Anexo A, disponible en, http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf.

[255] *Ídem.*

[256] *Ídem.*

[257] Organización de los Estados Americanos, OEA, *México presentó Estrategia Nacional de Ciberseguridad desarrollada con apoyo de la OEA*, Centro de Noticias, Comunicados de Prensa, C-082/17, 13 de noviembre de 2017, disponible en, http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-082/17.

[258] Gobierno de México, *Estrategia Nacional de Ciberseguridad*, México 2017, p. 3, disponible en, https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

Se promovió mediante foros abiertos y mesas de discusión, a través de un proceso llamado “Hacia una Estrategia Nacional de Ciberseguridad”, de marzo a octubre de 2017,[259] donde participaron grupos de trabajo *multistakeholder*, com el sector público y privado, industrial, técnico, academia, sociedad civil, entre otros, así como organismos internacionales como la OEA.

Durante este proceso, se llevaron a cabo consultas ciudadanas que, con apoyo de la OEA, se consolidaron en documentos de trabajo; asimismo, la OEA entregó una serie de recomendaciones para acompañar a México en el diseño y desarrollo de la ENCS. En un primer documento, se consolidaron las inquietudes de cada sector para después, enfocarse en temas específicos.

Asimismo, se identificaron las diferentes necesidades que tiene México en temas de ciberseguridad y quedaron sentadas las siguientes:

- Que la ENCS articule el desarrollo de las acciones de ciberseguridad que sirvan a individuos, empresas e instituciones públicas del Estado mexicano.
- Colaboración y cooperación entre los diferentes sectores como pieza clave para el desarrollo, seguimiento y evaluación de la Estrategia.
- Conocer la dimensión de los riesgos y amenazas en el ciberespacio, el estado que guarda la ciberseguridad en el país, la construcción de un diagnóstico nacional, así como obtener evidencia para mejorar la toma de decisiones en materia de ciberseguridad.
- Contemplar el escenario global como parte de la problemática y la diplomacia como vía para entablar diálogos y acuerdos que permitan hacer frente a los riesgos, amenazas y ciberdelitos.
- Desarrollar capital humano especializado en materia de ciberseguridad.
- Promover el uso responsable de las TIC y reforzar una cultura de ciberseguridad que contemple acciones de concientización, educación y formación.[260]

Por otra parte, del objetivo general se desprenden cinco objetivos estratégicos, tres principios rectores y ocho ejes transversales.

[259] *Ibídem,* p. 3.
[260] *Ibídem*, p. 3.

Los objetivos estratégicos son:

1. Sociedad y Derechos,
2. Economía e Innovación,
3. Instituciones Públicas,
4. Seguridad Pública y,
5. Seguridad Nacional.[261]

Para cumplirse, requieren de 8 ejes transversales, que son:

1. Cultura de ciberseguridad,
2. Desarrollo de capacidades,
3. Coordinación y colaboración,
4. Investigación, desarrollo e innovación TIC,
5. Estándares y criterios técnicos,
6. Infraestructuras críticas,
7. Marco jurídico y autorregulación y,
8. Medición y seguimiento.[262]

Asimismo, en un sentido de contribuir al desarrollo sostenido de México, se establecen tres principios rectores, que son:

1. Perspectiva de Derechos Humanos,
2. Enfoque basado en gestión de riesgos y,
3. Colaboración multidisciplinaria y de múltiples actores.[263]

La ENCS es un primer paso de gran importancia para la creación de una cultura general de ciberseguridad en México; asimismo se define como un documento vivo, ya que se encuentra abierta a todas las actualizaciones que la dinámica social requiera, con el objetivo de que, una vez alcanzada su madurez, México pueda contar instituciones consolidadas en la materia y recursos dedicados al tema.[264]

Con esta Estrategia, México ocupa el lugar número 8 de los países que han adoptado una Estrategia Nacional de Ciberseguridad en AL, los cuales son: Colombia (2011 y 2016), Panamá (2013), Trinidad y Tobago (2013), Jamaica (2015), Paraguay (abril 2017), Chile (abril 2017) y Costa Rica (abril 2017).[265]

[261] *Ibídem*, p. 4.
[262] *Ibídem*, p. 4.
[263] *Ibídem*, p. 7.
[264] *Ibídem*, p. 4.
[265] OEA, *Op. Cit.*

Evidentemente, quedan grandes retos a encarar en materia de ciberseguridad para México, muchos de ellos probablemente ni siquiera figuran como tal; algunos factores que alteran la seguridad en el ciberespacio no repercuten de la misma forma e intensidad en todos los países. Por lo anterior conviene preguntarnos qué relación guarda México con el Convenio de Budapest y, si este último acompaña, de manera significativa, la visión y misión que México deposita en el la ENCS.

### 3.3. La adhesión de México al Convenio de Budapest.

A lo largo de la investigación se ha puesto el acento sobre los beneficios, pero sobre todo, en la importancia de cooperar a nivel internacional, así como las desventajas de no hacerlo. Sin embargo, también se ha señalado que, a pesar de ser la ciberseguridad un problema mundial, existen situaciones específicas que nos diferencian por país, región e incluso en el nivel de desarrollo.

Un aspecto relevante que ha obstaculizado la cooperación en la materia y que, a su vez se deriva de esta diferenciación, es la armonización de leyes. Mientras que en los países en desarrollo el correo basura puede significar un problema significativo, en los países desarrollados el ciberespionaje representa un debate de gran importancia. El lento proceso de implementar normas jurídicas internacionales obedece a los diferentes efectos del ciberdelito, así como a la diferencia de distintas estructuras y tradiciones jurídicas.[266]

En lo que concierne al Convenio de Budapest, el COE no puede obligar a sus estados miembros a firmar el Convenio sobre la Ciberdelincuencia, ni forzar a los signatarios a ratificarlo, lo que explicaría que la normalización suele considerarse un proceso lento, en comparación con los procedimientos legislativos nacionales y regionales.[267]

---

[266] International Telecommunication Union, ITU, *El Ciberdelito: Guía para los países en desarrollo*, Ginebra, Suiza, abril, 2009, p. 119, disponible en, www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

[267] *Ídem*.

Un obstáculo adicional es la falta de consenso en la tipificación de delitos cibernéticos entre los países. Es importante recordar que los delitos en Internet pueden llevarse a cabo desde cualquier lugar y los procesos de investigación suelen verse a menudo entorpecidos por el sesgo jurídico de algunos países; por ejemplo, los procesos de extradición.

El 30 de mayo de 2017, en la Comisión Permanente del H. Congreso de la Unión, el diputado Jesús Valencia Guzmán, del Grupo Parlamentario del Partido de la Revolución Democrática (PRD), presentó un punto de acuerdo que exhorta a la Secretaría de Relaciones Exteriores (SRE) a iniciar los trabajos necesarios para la adhesión de México al Convenio de Budapest, a efecto de garantizar mayores instrumentos jurídicos para hacer frente a los delitos cibernéticos.[268]

Lo anterior derivado de diversas notas periodísticas y de lo establecido por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), donde indica que México ocupa el último lugar en materia de ciberseguridad debido al rezago en la tipificación de delitos informáticos y a que no cuenta con los recursos humanos preparados (agentes del MP, policías investigadores y jueces conocedores) para hacer frente a los diversos tipos de delitos informáticos.[269]

Previamente, en julio del 2015, la diputada Lizbeth Rosas Montero, integrante del mismo grupo parlamentario, había presentado una proposición solicitando información respecto a la adhesión al Convenio de Budapest.

En los antecedentes a dicha proposición, se reconoce la necesidad que tiene México de crear leyes específicas al respecto y homologar la tipificación del delito, pero también, resulta apremiante, la adhesión a organismos, convenios, acuerdos

[268] Valencia Guzmán, Jesús, *Gaceta del Senado*, Senado de la República, LXIII/2SPR-9/71861, 30 de mayo de 2017, disponible en http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=71861.
[269] *Ídem.*

y tratados internacionales, ya que nuestro país está imposibilitado para sancionar las acciones ilegales que sean perpetradas desde el exterior.[270]

México ocupa el lugar número dos en ciberataques en AL, siendo el sector manufacturero el más afectado con 27%, seguido por el sector financiero y bancario con 21% cada uno.[271] Asimismo, de acuerdo con el Informe Norton sobre Ciberseguridad 2016, durante ese año, 22.4 millones de mexicanos fueron afectados por el cibercrimen, lo que representa el 45% de los usuarios de Internet en México, y 5,500 MDD en lo que refiere a costos financieros.[272]

El ciberespacio es visto como uno de los grandes temas globales a corto, mediano y largo plazos, por lo que México se vería beneficiado con la articulación de objetivos claros de política exterior en la materia. La culminación del proceso de adhesión de México al Convenio de Budapest habría sido un buen principio en este sentido.

Sin embargo, pareciera que, desde el seno mismo del Convenio de Budapest, se ha generado una proyección al exterior de que ya no es suficiente. Budapest ya no alcanza para el ciberdelito por diferentes razones.

La primera de ellas recae en las jurisdicciones nacionales. El lento proceso de armonizar leyes al interior de un país para estar en consonancia con un marco jurídico más global y sobre un tema multifacético, ha dado tiempo a que se generen nuevas amenazas en el ciberespacio y que el Convenio se quede muy al margen, por ejemplo, la *dark web.*

La creación de protocolos adicionales es una muestra del corto alcance que tiene Budapest para los retos actuales.

---

[270] Rosas Montero, Lizbeth, "Dictamen a la Proposición con punto de acuerdo que solicita información respecto a la adhesión al Convenio de cibercriminalidad de Budapest", Segunda Comisión del Pleno de la Comisión Permanente del Congreso de la Unión, México, 22 de julio del 2015.

[271] HUFFPOST, "Microsoft se alía con la Policía Federal vs cibercrimen", México, Edition MX, 24 de febrero de 2017, disponible en http://www.huffingtonpost.com.mx/2017/02/24/microsoft-se-alia-con-policia-federal-contra-delitos-cibernetico_a_21721341/.

[272] Norton by Symantec, *Informe Norton sobre Ciberseguridad 2016*, Comparaciones Globales, México, disponible en, https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf.

Lo anterior nos introduce en una segunda razón que recae en la idiosincrasia tecnológica, de la que hemos sido rebasados una y otra vez, y que con la creación de Internet nos hemos quedado perplejos en una línea continua.

Por último, la tercera razón, y no menos importante, parte de las limitaciones del Convenio y de los instrumentos jurídicos debido a la falta de pluralidad de actores, o lo que es lo mismo, limitarse únicamente a los estados.

### 3.3.1. Ciberseguridad e Interdependencia Compleja.

Por lo antes señalado, en esta reflexión final parece oportuno hablar de la interdependencia compleja como prueba de la efectividad de los postulados extraídos de las propuestas de Keohane y Nye en el mundo actual y, específicamente, su capacidad para articularlos con el Convenio de Budapest 16 años después de su creación.

La interdependencia compleja caracteriza los tiempos de la globalización mediante un marco conceptual dividido en tres postulados. El primero de ellos, la pluralidad de canales que, en este caso específico, aunque los estados son los únicos actores que harán valer los tratados internacionales, a la luz de la teoría, los problemas del mundo actual no pueden ser vistos desde ni hacia una sola dirección; dentro del ciberespacio hay múltiples canales no solo intergubernamentales, donde existe preminencia de otros actores que juegan un papel igualmente relevante.

Asimismo, dos años después del nacimiento del Convenio, se creó el Protocolo adicional relativo a la criminalización de actos racistas y xenófobos cometidos por medio de sistemas informáticos, lo que nos conduce a la ausencia de jerarquía en los temas. Este segundo postulado de Keohane y Nye podemos dividirlo, a su vez, en dos análisis, por un lado, el del Convenio y, por el otro, el de México.

En lo que concierne al Convenio, además del sinfín de actores que fluyen y confluyen dentro del ciberespacio, éste mismo encierra un gran número de temas que tornan insuficiente a Budapest, no solo por enfocarse en él, sino porque dentro

del cibercrimen, los cibercrímenes tipificados en el Convenio han evolucionado y/o cambiado.

Por su parte, en México, y como se mencionó anteriormente, no todos los cibercrímenes afectan de igual manera a todos los países ni el cibercrimen representa la misma importancia para todos. Por tanto, es aplicable la ausencia de jerarquía en la agenda dentro de los estados y en el exterior.

En un mundo tan cambiante y tan complejo, firmar y ratificar un tratado, y un protocolo adicional que existen desde hace más de una década, resulta para México un paso muy grande y muy osado, dados los retos que mantiene nuestro país hoy en día, así como por la influencia que ejercen otros actores en la materia.

México tiene una agenda de pendientes en materia de seguridad, principalmente pública y, por ello, la armonización de leyes que conjuguen con el Convenio de Budapest requiere cambios estructurales no solo en el ciberespacio. Necesitaríamos preguntarnos cómo repercute el Convenio de Budapest en la seguridad, no solo nacional, sino también pública de nuestro país.

En lo personal, y dada la interpretación que se asume de Budapest al exterior, México puede tomar al Convenio de Budapest como una guía para establecer políticas públicas referentes al cibercrimen, fortalecer la ENCS, conceptualizar y tipificar delitos y entender desde otro punto al ciberespacio; sin embargo, la madurez con la que cuenta México en términos de ciberseguridad no es la misma que sostienen los países miembros del COE y la política exterior que México adopte en el ciberespacio debe estar comprometida con los retos y amenazas propios y actuales.

Sin embargo, también queda claro que cada vez son más importantes estos temas para el gobierno federal y los legisladores, y además, que también es cada vez más importante para los foros y mecanismos internacionales.

En este sentido, es toral abordar el papel de la ENCS como escenario de desarrollo en temas de ciberseguridad y como mecanismo para alcanzar mayor madurez en la materia. A través de la ENCS, México puede abordar una visión integral de las diversas aristas que conforman al espacio virtual, capaces de conjugarse con las mayores preocupaciones del espacio físico y que, al gestarse desde el interior, puedan proyectar una política exterior más uniforme.

Estas aristas incluyen la ciberseguridad y el combate a la ciberdelincuencia, el acceso a los beneficios de la red como un derecho humano emergente, la protección a la privacidad individual, al Estado de derecho, y a la gobernanza de Internet.

Dado que la ENCS es estrictamente nueva y no ha comprobado resultados, México debe seguir echando mano de los mecanismos y foros internacionales para encontrar mejores prácticas y, eventualmente, manteniendo latente la prioridad del tema, detonar en cualquier momento una adhesión de México al Convenio de Budapest, ya que se ve muy difícil que en lo que resta de esta administración México pueda adherirse.

## Conclusiones

La creciente dependencia que mantenemos hacia las TICs, al tiempo que aumentan las amenazas en el ciberespacio, ha tornado urgente la necesidad de establecer medidas que garanticen estabilidad y seguridad dentro del mismo. Para lograrlo, la cooperación internacional juega un rol muy importante, así como la inclusión de todas las partes interesadas en los procesos de negociación.

Esta investigación tuvo como propósito demostrar la poca probabilidad que existe por parte del gobierno mexicano de llevar a cabo la firma del Convenio de Budapest, por razones tales como lo obsoleto del tratado o la dificultad y lentitud del proceso de armonización de leyes a nivel nacional, a pesar de las diversas manifestaciones sobre estar en consonancia con lo estipulado en el tratado, pero principalmente, la poca utilidad que tendría para México firmarlo.

A través de los preceptos desarrollados por Keohane y Nye en la teoría de la interdependencia compleja, pude lograr, en un primer ejercicio, destacar la percepción de un mundo cada vez más interconectado e interdependiente, derivado del proceso de globalización, favorecido, en gran medida, por el Internet y las TICs. A partir de esto, el segundo paso consistió en presentar algunos elementos de una radiografía del ciberespacio desde los dos extremos: las ventajas que nos ha ofrecido y el incremento simultáneo de su uso para fines delictivos.

Gracias a los aportes de la interdependencia compleja a la disciplina de las Relaciones Internacionales, podemos analizar la política internacional con mayor acercamiento al mundo actual, caracterizado por una complejidad intrínseca de las relaciones interdependientes que se desarrollan en múltiples temas y a través de múltiples actores o canales.

Derivado de lo anterior, esta teoría permitió ubicar al ciberespacio como parte de este mundo complejo, pero principalmente explicarlo a través de ella.

Dentro del ciberespacio convergen múltiples actores que han formado una "sociedad transnacional" —como la que describían Keohane y Nye—, que comparte ciertos valores, libertades y derechos, pero, además, ha cambiado la percepción tradicional-militar del poder y lo ha redistribuido en diferentes esferas ocasionando un adelgazamiento de las capacidades del Estado.

La historia nos ha marcado el desplazamiento de la idea realista sobre el Estado como actor preponderante de la política internacional que, durante el periodo entre guerras, definió la seguridad en términos de la seguridad de Estado y bajo el mando del poder militar, para dar paso a lo que —durante la Guerra Fría y posterior a ella, consecuencia de las dos grandes guerras— serían los problemas sociales, como migraciones, epidemias, crisis económicas, etc. y, a partir de ello, la necesidad de redefinir la agenda de seguridad internacional y el debate de lo que hoy conocemos como seguridad humana.

Esta transición del concepto de seguridad no minimiza la seguridad nacional tradicional, por el contrario, la complementa y determina que la seguridad va de la mano con el desarrollo.

Si bien es cierto que no podemos tener libertad absoluta y seguridad al mismo tiempo, tampoco se puede garantizar la seguridad total sin detrimento de los derechos humanos; por ello, considero que el punto de partida es encontrar, a partir de los dos extremos del ciberespacio —seguridad y desarrollo—, el punto de intersección y, si logramos encontrar este punto, seremos capaces de implementar marcos normativos que garanticen seguridad, al mismo tiempo que impulsen el desarrollo, reduzcan la brecha digital y protejan los derechos humanos.

Teniendo claro lo anterior, podemos identificar en qué hemisferio de la ciberseguridad se encuentran los principales trabajos internacionales en la materia, cuya catalogación es muy sencilla: los esfuerzos dentro del marco de Naciones Unidas y los esfuerzos fuera, donde se ubica el Convenio de Budapest.

Una de las principales características de Budapest es su carácter vinculante, a diferencia del resto que son voluntarios y, como tal, ejerce sanciones. La base del establecimiento de normas es el carácter voluntario, que conforme avanzan en la instrumentación, hay una especie de estandarización y, en el futuro, obligatoriedad; pero no podemos comenzar obligando a hacer algo y menos si existen brechas en las capacidades técnicas, políticas, económicas y sociales entre las partes.

Aunado a ello, el Convenio de Budapest data de hace más de 10 años y contempla un protocolo adicional que nos dice mucho en el sentido de que el proyecto inicial no fue suficiente; la tecnología, con el paso del tiempo, es cada vez más rápida y muchas veces nos vemos rebasados por ella, así que firmar un acuerdo de 2001 podría resultar obsoleto en el entendido de que no abarca la totalidad de cibercrímenes actuales.

Siguiendo esta línea, el Convenio se concentra en el cibercrimen y, retomando el primer capítulo: un acuerdo que solo piensa en seguridad no protege derechos humanos.

Por otro lado, en el caso específico de México, los problemas de seguridad nacional y pública son alarmantes, así como los niveles de corrupción y desigualdad, lo que hace aún más lento el proceso de armonización de leyes y, además, no son condiciones que tengamos en común con los países miembros del Consejo de Europa, ni tampoco compartimos las mismas capacidades, por lo que considero que establecer vinculatoriedad jurídica internacional le garantizaría más desventajas que ventajas a México, o al menos, no se percibe que hoy pueda ofrecerle mejora alguna en la materia.

Sin embargo, existen trabajos importantes en diferentes foros multilaterales y de carácter flexible —como el Grupo de Expertos Gubernamentales a nivel internacional o los que se dan a través del CICTE de la OEA a nivel regional— que, aunque no son vinculantes en sentido jurídico, si lo son en sentido político, ya que ningún Estado quiere parecer que no coopera en un tema de ciberseguridad que él aceptó participar.

Hoy día, México cuenta con una gran participación en la región, donde haciendo uso de sus experiencias dentro del GGE, comparte voluntariamente con otros Estados marcos, estrategias y políticas para una conducta responsable, al mismo tiempo que revisan la aplicabilidad del derecho internacional al ciberespacio, la elaboración e implementación de medidas de fomento de cooperación y confianza, etc. Asimismo, con la recién creada Estrategia Nacional de Ciberseguridad —que tomó en cuenta la voz de todos los sectores involucrados—, México busca sensibilizar, generar diálogo y crear confianza entre los actores, pero no solo estableció un compromiso a nivel nacional, también proyectó al exterior lo importante que es cada vez más, para los mexicanos, el ciberespacio y que hay un compromiso generalizado de seguir trabajando en la ciberseguridad, al mismo tiempo que desarrollamos y detonamos beneficios comunes de un Internet abierto, seguro, accesible y pacífico.

Las normas existentes en torno al ciberespacio son evolutivas como el tema mismo. Eventualmente cambiarán y se adaptarán a la realidad; sin embargo, lo importante es saber hacia dónde vamos y qué es lo que queremos obtener del Internet y las TICs. Desde mi punto de vista, como lo he señalado a lo largo de la investigación, no podemos pensar al ciberespacio como un espacio inseguro que requiere un control absoluto, ni debe ser manejado por unos cuantos, por el contrario, deberíamos pensarlo como una plataforma de desarrollo que requiere prevenir, contener y mitigar riesgos y amenazas, ser resiliente y continuar con el proceso evolutivo de los avances tecnológicos para seguir obteniendo grandes ventajas.

Concluyo con la responsabilidad que tenemos como sociedad en el ciberespacio; muchas veces somos víctimas de delitos informáticos por la poca importancia que le damos a la información que compartimos en Internet. No podemos evitar que usen nuestra información para fines diferentes a los que fue destinada, pero si podemos elegir qué información queremos compartir y qué uso le damos a las aplicaciones o páginas que utilizamos; por eso considero que lo más importante no es temerle al ciberespacio, sino conocerlo y ser responsables del uso que le damos,

hay que informarnos, abordar el tema y asumir el papel tan importante que tenemos dentro de él.

En artículos recientes[273] se plantea la preocupación —que sin duda es tema para otra investigación—, de la inteligencia artificial que está suplantando el trabajo humano por robots, lo que ocasionaría indudablemente problemas sociales como la falta de empleos, exclusión, rezago, etc. El uso del Internet y las TICs caracteriza el mundo actual, es nuestra realidad y no hay marcha atrás; sin embargo, el reto está en ser conscientes, usarlo responsablemente y reducir la brecha que existe en torno a él, como los derechos humanos, la protección de datos personales, privacidad, accesibilidad, inclusión y, pienso en este momento, el derecho a ser borrado de la red.

[273] De la Fuente, Juan Ramón, "La inteligencia artificial" e "Inteligencia Artificial (II), en *El Universal*, Opinión, 12 de febrero de 2018 y 19 de marzo de 2018, disponibles en http://www.eluniversal.com.mx/columna/juan-ramon-de-la-fuente/nacion/la-inteligencia-artificial, consultadas el 19 de marzo de 2018.
Cortina, Adela, "Ciudadanía digital y dignidad humana", en *El País*, Opinión, 26 de marzo de 2018, disponible en https://elpais.com/elpais/2018/03/22/opinion/1521737007_854105.html, consultada el 26 de marzo de 2018.

**Bibliografía**


Abolhassan, Ferri, *Cyber Security. Simply. Make it Happen.*, Springer, Germany, 2016.

Aguayo, Sergio (comp.), *En busca de la seguridad perdida. Aproximaciones a la seguridad nacional mexicana*, Siglo XXI Editores, primera edición 1990, México.

Assange, Julian, *Cypherpunks. La libertad y el futuro de Internet*, Temas de Hoy, México, 2013.

Bárcena Coqui, Martha, "La reconceptualización de la seguridad", en *Seguridad Internacional en el siglo XXI: los retos para América Latina y el Caribe*, primera edición 2004, Senado de la República, México.

Beck, Ulrich, *¿Qué es la Globalización?, Falacias del globalismo, respuestas a la globalización*, Paidós, España, 1998.

Borja, Arturo (Compilador), *Interdependencia, cooperación y globalismo. Ensayos escogidos de Robert O. Keohane*, CIDE, México, 2009.

Bull, Hedley, *La Sociedad Anárquica. Un estudio sobre el orden en la política mundial.*, Tercera Edición, Ed. Catarata, España, 2005.

Castells, Manuel, *La Galaxia Internet*, Plaza y Janés, España, 2001.

Chatfield, Tom, *50 cosas que hay que saber sobre el mundo digital*, Ed. Ariel, España, 2012.

*Constitución Política de los Estados Unidos Mexicanos*, Ed. Porrúa, México, 2014.

Fazio Vengoa, Hugo, *La Globalización en su historia*, Universidad de Colombia, Bogotá, 2002.

Hernández-Vela Salgado, Edmundo, *Diccionario de Política Internacional*, Tomo II (Letras J-Z), Sexta Edición, Ed. Porrúa, México.

Kant, Manuel, La paz perpetua, Ed. Porrúa, México, 1998.

Programa de las Naciones Unidas para el Desarrollo (PNUD), *Informe sobre desarrollo humano 1994*, FCE, México, 1994.

Rosas, María Cristina (Coord.), *La seguridad por otros medios. Evolución de la agenda de seguridad internacional en el siglo XXI: lecciones para México, La Seguridad Humana: ¿Nuevo Paradigma para la Seguridad Nacional de*

*México en el Siglo XXI?*, Ed. Centro de Análisis e Investigación sobre Paz, Seguridad y Desarrollo Olof Palme A.C., México, 2011.

Spinello, Richard, *Cyberethics. Morality and Law in Cyberspace*, Jones and Bartlett Publishers, United States of America, 2000.

Tercero, José B., *Sociedad digital: del homo sapiens al hombre digitalis*, Alianza Editorial, España, 1996.

Weber, Max, *Economía y sociedad*, Ed. Fondo de Cultura Económica, 2da. Edición, México, 1979, pág. 43.

**Hemerografía**

Anonymous ataca los sitios del Senado y Gobernación por la ley Döring, *Expasión*, 27 de enero, 2012, https://expansion.mx/tecnologia/2012/01/27/anonymous-ataca-los-sitios-del-senado-y-gobernacion-por-la-ley-doring?internal_source=PLAYLIST.

Arcos, Eduardo, "¿Qué es y cómo funciona la Ley Sinde?", *Hipertextual*, 25 de enero, 2011, https://hipertextual.com/2011/01/que-es-la-ley-sinde

Austria, Xóchitl, "5 travesuras de Anonymous en México", *Alto Nivel*, 17 de enero, 2013, http://www.altonivel.com.mx/33468-los-ataques-de-anonymous-en-mexico.html.

BBC Mundo, "La Unidad 61398, el nuevo enemigo de EE.UU.", *BBC*, 20 de mayo de 2014, www.bbc.com/mundo/.../05/140520_tecnologia_hackers_china_unidad_61398_mz

Cortina, Adela, "Ciudadanía digital y dignidad humana", en *El País*, Opinión, 26 de marzo de 2018, https://elpais.com/elpais/2018/03/22/opinion/1521737007_854105.html.

Cyberwar. War in the fifth domain, *The Economist*, Volume 396, number 8689, July 3rd-9th 2010.

De la Fuente, Juan Ramón, "La inteligencia artificial" e "Inteligencia Artificial (II), en *El Universal*, Opinión, 12 de febrero de 2018 y 19 de marzo de 2018,

http://www.eluniversal.com.mx/columna/juan-ramon-de-la-fuente/nacion/la-inteligencia-artificial.

EFE, “Israel y Estados Unidos son los creadores del virus informático de espionaje Flame”, *El País*, 20 de junio, 2012, http://tecnologia.elpais.com/tecnologia/2012/06/20/actualidad/1340176288_675950.html.

Espinosa, Ángeles, “Irán sufre un ataque informático contra sus instalaciones nucleares”, *El País*, 28 de septiembre, 2010, http://elpais.com/diario/2010/09/28/internacional/1285624808_850215.html.

Gallagher, Ryan, “Goverments turn to hacking techniques for surveillance of citizens” en *The Guardian*, Tech, 01 de noviembre, 2011, https://www.theguardian.com/technology/2011/nov/01/governments-hacking-techniques-surveillance.

Hernández Aura, “Piden a México en Convenio de Budapest, ser más que un observador”, en *Excélsior*, 07 de diciembre del 2016, http://www.excelsior.com.mx/hacker/2016/12/07/1132670.

Hess Araya, Christian, “Aprobado convenio europeo contra la ciberdelincuencia”, *La Nación*, Opinión, 04 de agosto de 2017, http://www.nacion.com/opinion/foros/Aprobado-convenio-europeo-ciberdelincuencia_0_1650234967.html.

Jiménez, Claudia G. “Las teorías de la cooperación internacional dentro de las relaciones internacionales” en, *Polis. Investigación y Análisis Sociopolítico y Psicosocial*, 03 Vol. DOS, UNAM, México.

Leetaru, Kalev, “What Tallinn Manual 2.0 Teaches Us About The New Cyber Order”, *Forbes*, 09 de febrero, 2017, https://www.forbes.com/sites/kalevleetaru/2017/02/09/what-tallinn-manual-2-0-teaches-us-about-the-new-cyber-order/#18e068b6928b.

Maurer, Tim, “The New Norms: Global Cyber-Security Agreements Face Challenges”, en *Carnegie. Endowment for International Peace*, 5 de Febrero, 2016, http://carnegieendowment.org/2016/02/15/new-norms-global-cyber-security-agreements-face-challenges-pub-63031.

McCormick, Ty, “Hacktivism: A Short History”, en *Foreign Policy*, 29 de abril del 2013, http://foreignpolicy.com/2013/04/29/hacktivism-a-short-history/

McKune, Sarah, An Analysis of the International Code of Conduct for Information Security, en *The Citizen Lab*, Septiembre, 2015, https://citizenlab.org/2015/09/international-code-of-conduct/

Microsoft se alía con la Policía Federal vs cibercrimen, *HUFFPOST*, México, Edition MX, 24 de febrero de 2017, http://www.huffingtonpost.com.mx/2017/02/24/microsoft-se-alia-con-policia-federal-contra-delitos-cibernetico_a_21721341/.

Monks, Kieron, “Así se ve el Internet en realidad: cables submarinos que atraviesan la tierra”, *CNN Noticias*, 4 marzo, 2014, http://cnnespanol.cnn.com/2014/03/04/asi-se-ve-el-internet-en-realidad-cables-submarinos-que-surcan-la-tierra/#0

Mullen, Jethro, “El mundo intenta recuperarse del masivo ciberataque que afectó a casi 100 países”, en *CNN*, 13 de mayo 2017, http://cnnespanol.cnn.com/2017/05/13/el-mundo-intenta-recuperarse-del-masivo-ciberataque-que-afecto-a-casi-100-paises/

Nakashima, Ellen, “Chinese hack of federal personnel files included security-clearance database”, *The Washington Post*, National Security, 12 de Junio, 2015, https://www.washingtonpost.com/world/national-security/chinese-hack-of-government-network-compromises-security-clearance-files/2015/06/12/9f91f146-1135-11e5-9726-49d6fa26a8c6_story.html

Nye, Joseph S., “Controlling Cyber Conflict” en *Project Syndicate. The World´s opinion page*, 8 de Agosto, 2017, http://prosyn.org/0jHrDb3.

Nye Jr., Joseph S., “Soft Power”, *Foreign Policy*, No. 80, Twentieth Anniversary, Autumn, 1990.

Oliveira, Joana, “El ataque de “ransomware” se extiende a escala global”, en *El País*, Madrid, 15 de mayo, 2017, https://elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html?rel=mas.

Pérez de Armiño, Karlos, “El concepto y el uso de la seguridad humana: análisis crítico de sus potencialidades y riesgos”, en *Revista CIDOB d’Afers Internacionals,* Núm. 76, Fundación CIDOB, España, p. 59-77.

Peterson, Andrea, “OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought”, *The Washington Post*, 23 de Septiembre, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?utm_term=.68e388af59bc.

Raphael, Ricardo, “Contra el espionaje, el periodismo”, en *El Universal*, 13 de agosto, 2015, http://www.eluniversal.com.mx/entrada-de-opinion/columna/ricardo-raphael/nacion/2015/08/13/contra-el-espionaje-el-periodismo.

Riestra, Laura, “Las claves del caso Wikileaks”, en *ABC.es*, 21 de agosto, 2013, http://www.abc.es/internacional/20130821/abci-claves-caso-manning-201308211907.html

Rosas, María Cristina, “Ciberespacio, crimen organizado y seguridad nacional”, en *ALAI, América Latina en Movimiento*, 09 de mayo del 2011, http://alainet.org/active/46432.

Saiz, Eva, “Los ciberataques sustituyen al terrorismo como primera amenaza para EE.UU.” en *El País*, 13 marzo, 2013, http://internacional.elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html.

Sánchez Onofre, Julio, “Vulneración a Hacking Team confirma abuso de espionaje en México”, en *El Economista*, 06 de Julio del 2015, http://eleconomista.com.mx/tecnociencia/2015/07/06/vulneracion-hacking-team-confirma-abuso-espionaje-mexico.

Stevens, Tim, “A Cyberwar of Ideas? Deterrence and Norms in Cyberspace”, en *Contemporary Security Policy*, Vol. 33, No 1, 2012.

Vargas, Alberto, “Ciberseguridad: el ejército Español busca hackers informáticos para una nueva unidad”, en *Zoom News*, 4 de diciembre, 2013,

http://www.zoomnews.es/152254/actualidad/espana/ciberdefensa-ejercito-espanol-busca-hackers-informaticos-nueva-unidad.

Wikileaks en la jornada, *La jornada*, http://wikileaks.jornada.com.mx/cables/gobierno-felipe-calderon/sugieren-a-valenzuela-pedir-a-mexico-que-respalde-sin-ambiguedades-la-politica-estadunidense-para-honduras-cable-09mexico3423/.

**Otras fuentes**

Asociación de Internet. MX, *13° Estudio sobre los Hábitos de los Usuarios de Internet en México 2017*, 08 de agosto, 2017, https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/13-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2017/lang,es-es/?Itemid.

Autoridad Nacional para la Innovación Gubernamental, “Panamá ratifica convenio sobre cibercrimen”, Gobierno de la República de Panamá, 20 de marzo de 2014, http://www.innovacion.gob.pa/noticia/2117.

Banco Mundial (2016), *Informe sobre el desarrollo mundial 2016: Dividendos Digitales*, Banco Mundial, Washington DC.

Cámara de Diputados del H. Congreso de la Unión, Código Penal Federal, Texto Vigente, Última reforma publicada DOF 26-06-2017, http://www.diputados.gob.mx/LeyesBiblio/pdf/9_260617.pdf.

Cámara de Diputados del H. Congreso de la Unión, *Ley de Instituciones de Crédito*, Capítulo IV, Art. 112 Bis., Texto Vigente, Última reforma publicada DOF 17-6-2016, http://www.diputados.gob.mx/LeyesBiblio/pdf/43_170616.pdf.

Clarke, Richard A., *Securing Cyberspace Through International Norms. Recommendations for Policymakers and the Private Sector*, Good Harbor Security Risk Management, LLC., Washington D.C.

Conferencia de Ministros de Justicia de los Países Iberoamericanos, COMJIB, “Bases para la elaboración de un instrumento internacional en materia de cibercriminalidad”, Viña del Mar, Chile, 04 y 05 de Abril del 2013,

http://comjib.org/es/xviii-conferencia-de-ministros-de-justicia-de-los-paises-iberoamericanos/.

Conferencia de Ministros de Justicia de los Países Iberoamericanos, COMJIB, “México se adhiere a Convenio Iberoamericano sobre Ciberdelincuencia”, 10 de junio del 2014, http://comjib.org/es/mexico-se-adhiere-a-convenio-iberoamericano-sobre-ciberdelincuencia/.

Conferencia de Ministros de Justicia de los Países Iberoamericanos, COMJIB, Secretaría General, “Convenio Iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia”, Madrid, España, 28 de mayo del 2014, http://www.mec.gub.uy/innovaportal/file/52706/1/ciber_convenio.pdf.

Congreso de Sinaloa, Código Penal para el Estado de Sinaloa, Capítulo V, Art. 217., Texto Vigente, última reforma publicada en el P.O. No. 158 del 28 de diciembre de 2016, http://www.congresosinaloa.gob.mx/images/congreso/leyes/zip/codigo_penal_28-dic-2016.pdf.

Consejo de Europa, “Chile’s commitment to fight cybercrime”, Cybercrime, News, Strasbourg, France, 27 de abril de 2017, https://www.coe.int/en/web/cybercrime/-/chile-s-commitment-to-fight-cybercrime.

Consejo de Europa, “Costa Rica joins the Budapest Convention”, Cybercrime, T-CY News, Strasbourg, France, 03 de octubre de 2017, https://www.coe.int/en/web/cybercrime/t-cy-news/-/asset_publisher/GxUcENEFhivB/content/costa-rica-joins-the-budapest-convention.

Consejo de Europa, *Convenio sobre la Ciberdelincuencia*, Serie de Tratados Europeos – n° 185, Budapest, 23 de noviembre, 2001.

Consejo de Europa, “Dominican Republic”, Octopus Cybercrime Community, Country Wiki, última actualización 10 de febrero de 2015, https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/dominican-republic.

Consejo de Europa, COE, Mexico, Status regarding Budapest Convention, última actualización: 23 de noviembre de 2014, disponible en, http://www.coe.int/fr/web/octopus/-/mexico.

Consejo de Europa, “Panama joins Budapest Convention”, Cybercrime, T-CY News, Strasbourg, France, 5 de marzo de 2014, disponible en, https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/panama-joins-budapest-convention.

Council of Europe, Cybercrime, *Octopus Conferences*, https://www.coe.int/en/web/cybercrime/octopus-conference.

Cybersecurity Ventures, *2017 Cybercrime Report*, Herjavec Group, 2017, https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.

Digital Watch Observatory, *UN GGE*, https://dig.watch/processes/ungge.

Finnemore, Martha, “Cultivating International Cyber Norms”, en *America’s Cyber Future: Security and Prosperity in the Information Age*, Vol. II, eds., Kristin M. Lord and Travis Sharp (Center of a New American Security: Washington, 2011).

Foro “Hacia una Estrategia Nacional de Ciberseguridad: Perspectivas de Derechos Humanos” en el Museo Memoria y Tolerancia, co-organizado por la Oficina de la Presidencia de la República y la Organización de Estados Americanos (OEA), 15 de agosto de 2017.

Gobierno de Chile, *Política Nacional de Ciberseguridad*, 2017-2022, http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.

Gobierno de México, “Decreto por el que se reforman y adicionan diversas disposiciones de los artículos 6º., 7º., 27,28, 73, 78, 94 y 105 de la Constitución Política de los Estados Unidos Mexicanos, en materia de telecomunicaciones”, *Diario Oficial de la Federación*, 11 de junio del 2013, http://www.dof.gob.mx/nota_detalle.php?codigo=5301941&fecha=11/06/2013.

Gobierno de México, “Acuerdo por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias”, *Diario Oficial de la Federación*, Primera Sección, 04 de febrero de 2016, dof.gob.mx/nota_to_doc.php?codnota=5424367.

Gobierno de México, *Estrategia Nacional de Ciberseguridad*, México 2017, p. 3, https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Gobierno de México y Consejo de Europa, Memoria del “Taller sobre legislación en materia de ciberdelincuencia en América Latina”, México, D.F., 31 de marzo al 2 de abril de 2014, https://rm.coe.int/1680303ece.

Gobierno de la República, *Plan Nacional de Desarrollo 2013-2018*, México.

Gobierno de la República, *Estrategia Digital Nacional*, México, https://www.gob.mx/mexicodigital/.

Hall, William, *La ciberdelincuencia y pruebas electrónicas en el Continente Americano: la perspectiva de Estados Unidos*, Departamento de Justicia de Estados Unidos, 01 de abril del 2014, https://rm.coe.int/1680303ed4.

INEGI, “Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares 2017”, http://www.beta.inegi.org.mx/proyectos/enchogares/regulares/dutih/2017/

INEGI, “Estadísticas a propósito del Día Mundial de Internet (17 de mayo)…”, 15 de mayo, 2017, http://www.inegi.org.mx/saladeprensa/aproposito/2017/internet2017_Nal.pdf

Instituto Español de Estudios Estratégicos, *Ciberseguridad. Retos y Amenazas a la seguridad nacional en el ciberespacio*, Ministerio de Defensa, Cuadernos de Estrategia 149, diciembre 2010.

International Telecommunication Union, ITU, *ITU releases 2017 global information and communication technology facts and figures*, Ginebra, 31 de julio, 2017, https://www.itu.int/en/mediacentre/Pages/2017-PR37.aspx.

International Telecommunication Union, ITU, *La UIT publica los datos sobre las TIC de 2015*, Ginebra, 26 de mayo, 2015, http://www.itu.int/net/pressoffice/press_releases/2015/17-es.aspx#.V-laZYjhDIU.

International Telecommunication Union, ITU, *Cumbre Mundial sobre la Sociedad de la Información, Ginebra 2003 – Túnez 2005*, sitio web: http://www.itu.int/net/wsis/basic/about-es.html.

International Telecommunication Union, ITU, *El Ciberdelito: Guía para los países en desarrollo*, Ginebra, Suiza, abril, 2009, www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

Internet Governance Forum, IGF 2016, Jalisco, México, sitio web: http://www.igf2016.mx/es/.

Libicki, Martin C, *Cyberdeterrence and Cyberwar*, RAND Corporation, Santa Mónica, 2009, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Naciones Unidas, Asamblea General "Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional", A/RES/58/32 (18 de diciembre de 2003), A/RES/60/45 (6 de enero de 2006), A/RES/66/24 (13 de diciembre de 2011), A/RES/68/243 (9 de enero de 2014) y A/RES/70/237 (30 de diciembre de 2015).

NATO Cooperative Cyber Defense Centre of Excellence, CCDCOE, *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*, Tallin, Estonia, https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html.

Norton by Symantec, *Informe Norton sobre Ciberseguridad 2016, Comparaciones Globales*, México, https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf

Organización de los Estados Americanos, OEA, Seguridad Cibernética, https://www.sites.oas.org/cyber/Es/Paginas/default.aspx.

Organización de los Estados Americanos, OEA, México presentó Estrategia Nacional de Ciberseguridad desarrollada con apoyo de la OEA, Centro de Noticias, Comunicados de Prensa, C-082/17, 13 de noviembre de 2017, http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-082/17.

Organización de los Estados Americanos, OEA, Una Estrategia Interamericana Integral de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética, AG/RES. 2004, Anexo A, http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf.

Organización de las Naciones Unidas, ONU, Declaración Universal de los Derechos Humanos, 10 de diciembre de 1948, http://www.derechoshumanos.net/normativa/normas/1948-DeclaracionUniversal.htm?gclid=COjNgKG9ldECFRuBswodJ8YBgQ.

Organización de las Naciones Unidas, ONU, Asamblea General, “Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética”, AG/RES. 1939 (XXXIII-O/03), 10 de junio de 2003, http://www.oas.org/juridico/spanish/agres_1939.pdf

Organización de las Naciones Unidas, ONU, Asamblea General, “Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General”, Resolución A/69/273 (2015), http://www.un.org/Docs/journal/asp/ws.asp?m=A/69/723.

Organización de las Naciones Unidas, ONU, Asamblea General, “Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo”, Resolución A/HRC/32/L.20 (2012), http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf .

Organización de las Naciones Unidas, ONU, Proyecto de documento final de la cumbre de las Naciones Unidas para la aprobación de la agenda para el desarrollo después de 2015, Asamblea General, 12 de agosto, 2015.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, UNESCO, Comunicación e Información, UNESCO y la CMSI, sitio web: http://www.unesco.org/new/es/communication-and-information/unesco-and-wsis/about/.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, UNESCO, Comunicación e Información, Acerca de la CMSI+10, sitio web: http://www.unesco.org/new/es/communication-and-information/wsis-10-review-event-25-27-february-2013/about-wsis-10/.

Pérez de Acha, Gisela, "Informe: Hacking Team. Malware para la vigilancia en América Latina", *Derechos Digitales*. Derechos Humanos y Tecnología en América Latina, marzo, 2016.

Presidencia de la República, "Programa para la Seguridad Nacional 2014-2018", *Diario Oficial de la Federación*, México, 30 de abril de 2014, http://www.presidencia.gob.mx/wp-content/uploads/2014/05/Programa-para-la-Seguridad-Nacional-Versio%CC%81n-Final.pdf

Resolución del Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos, CICTE/RES.1/17, 10 de abril 2017.

Rosas Montero, Lizbeth, "Dictamen a la Proposición con punto de acuerdo que solicita información respecto a la adhesión al Convenio de cibercriminalidad de Budapest", Segunda Comisión del Pleno de la Comisión Permanente del Congreso de la Unión, México, 22 de julio del 2015.

Secretaría de Gobernación, CISEN, http://www.cisen.gob.mx/cisen.htm.

Secretaría de Gobernación, Comisión Nacional de Seguridad, Fortalece CNS estrategias para la protección del ciberespacio mexicano, 25 de febrero de 2015, http://www.denuncia.gob.mx/portalWebApp/wlp.c;jsessionid=n2wmJxvJv1KY2J5cWQLBTfcQrdJ4tcvV11fqhw1JQpvGGvzwLJ2s!-1886721534?__c=f7130

Secretaría de Relaciones Exteriores, SRE, Taller sobre la Legislación en materia de Ciberdelincuencia, México, https://rm.coe.int/1680303edd.

Secretaría de Relaciones Internacionales, SRE, Taller sobre legislación en materia de ciberdelincuencia en América Latina, Nota de Prensa, 03 de abril de 2014, https://www.gob.mx/sre/prensa/taller-sobre-legislacion-en-materia-de-ciberdelincuencia-en-america-latina-10694

Solís, Cynthia, "La Transposición del Convenio de Budapest sobre la ciberdelincuencia en la legislación francesa en la práctica", en *Derecho y TIC. Vertientes Actuales*, UNAM, Instituto de Investigaciones Jurídicas, Serie Doctrina Jurídica, núm. 751, México, 2016, https://archivos.juridicas.unam.mx/www/bjv/libros/9/4065/18.pdf

Student Conference on the United States Affairs, SCUSA 63, *Thinking Beyond Boundaries: Contemporary Challenges to U.S. Foreign Policy, Governing Cyberspace*, U.S. Military Academy at West Point, New York, 2-5 November 2011.

Valencia Guzmán, Jesús, Gaceta del Senado, Senado de la República, LXIII/2SPR-9/71861, 30 de mayo de 2017, http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=71861.

World Bank, World Development Report 2017: Governance and the Law. Washington, DC, 2017.

World Economic Forum, Global Risk Report 2018, Executive Summary, Spanish, http://reports.weforum.org/global-risks-2018/executive-summary-spanish/

Zavaleta, Sandra, *Más allá de la visión tradicional de la seguridad y del desarrollo. Hacia la consecución de la seguridad humana y el desarrollo humano en las relaciones internacionales contemporáneas*, UNAM, Tesis, México, 2012.

**Anexo A**


*Serie de Tratados Europeos - n °185*

# CONVENIO SOBRE LA CIBERDELINCUENCIA

**Budapest, 23.XI.2001**

Preámbulo

Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio,

Considerando que el objetivo del Consejo de Europa es lograr una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los otros Estados Partes en el presente Convenio;

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

Reconociendo la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información;

Estimando que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal;

Convencidos de que el presente Convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable;

Teniendo presente la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de derechos humanos, que reafirman el derecho a defender la propia opinión sin interferencia, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar información e ideas de toda índole, sin consideración de fronteras, así como el respeto de la vida privada;

Conscientes igualmente del derecho a la protección de los datos personales, tal como se define, por ejemplo, en el Convenio de 1981 del Consejo de Europa para la protección de las personas con respecto al tratamiento informatizado de datos personales;

Teniendo presentes la Convención sobre los Derechos del Nino de las Naciones Unidas (1989) y el Convenio sobre las peores formas de trabajo infantil de la Organización Internacional del Trabajo (1999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el objeto del presente Convenio es completar dichos Convenios con el fin de incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como permitir la obtención de pruebas electrónicas de los delitos;

Congratulándose de las recientes iniciativas destinadas a mejorar el entendimiento y la cooperación internacionales en la lucha contra la delincuencia cibernética, y en particular las acciones organizadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8;

Recordando las Recomendaciones del Comité de Ministros n° R (85) 10 relativa a la aplicación práctica del Convenio Europeo de Asistencia Judicial en Materia Penal en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, n° R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, n° R (87) 15 relativa a la regulación de la utilización de datos de personales por la policía, n° R (95) 4 sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos, n° R (89) 9 sobre la delincuencia relacionada con la informática, que ofrece a los legisladores nacionales directrices para definir ciertos delitos informáticos, y n° R (95) 13 relativa a los problemas de procedimiento penal vinculados a la tecnología de la información;

Teniendo presente la Resolución n° 1, adoptada por los Ministros de Justicia europeos, en su XXI Conferencia (Praga, 10 y 11 de junio de 1997), que recomendaba al Comité de Ministros apoyar las actividades en relación con la ciberdelincuencia organizadas por el Comité Europeo para Problemas Criminales (CDPC) con el fin de aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos, así como la Resolución n° 3, adoptada en la XXIII Conferencia de Ministros de Justicia europeos (Londres, 8 y 9 de junio de 2000), que exhortaba a las partes negociadoras a persistir en sus esfuerzos por encontrar soluciones que permitan al mayor número posible de Estados ser partes en el Convenio, y reconocía la necesidad de disponer de un mecanismo rápido y eficaz de cooperación internacional que tenga debidamente en cuenta las exigencias específicas de la lucha contra la ciberdelincuencia;

Teniendo asimismo en cuenta el plan de acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa, con ocasión de su segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997) con objeto de encontrar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa,

Han convenido en lo siguiente:

## Capítulo I - Terminología

### Artículo 1 - Definiciones

A los efectos del presente Convenio:

a. por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;
b. por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;
c. por "proveedor de servicios" se entenderá:

   i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y
   ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo;

d. por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

## Capítulo II - Medidas que deberán adoptarse a nivel nacional

### Sección 1 - Derecho penal sustantivo

#### *Título 1 - Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos*

### Artículo 2 - Acceso ilícito

Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegitimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

### Artículo 3 - Interceptación ilícita

Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no publicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema

informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

### Artículo 4 - Ataques a la integridad de los datos

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegitimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten danos graves.

### Artículo 5 - Ataques a la integridad del sistema

Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

### Artículo 6 - Abuso de los dispositivos

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:
   i. cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio;
   ii. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático,

   con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y

b. la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del presente artículo.

*Título 2 - delitos informáticos*

### Artículo 7 - Falsificación informática

Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

### Artículo 8 - Fraude informático

Las Partes adoptaran las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a. la introducción, alteración, borrado o supresión de datos informáticos;
b. cualquier interferencia en el funcionamiento de un sistema informático,

con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

*Título 3 - Delitos relacionados con el contenido*

### Artículo 9 - Delitos relacionados con la pornografía infantil

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a. la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
b. la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;
c. la difusión o la transmisión de pornografía infantil a través de un sistema informático;
d. la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;
e. la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 anterior, se entenderá por «pornografía infantil» todo material pornográfico que contenga la representación visual de:

a. un menor adoptando un comportamiento sexualmente explícito;
b. una persona que parezca un menor adoptando un comportamiento sexualmente explícito;
c. imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

3. A los efectos del párrafo 2 anterior, se entenderá por «menor» toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

4. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.

*Título 4 - Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines*

### Artículo 10 - Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de Paris de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3. En circunstancias bien delimitadas, toda Parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

### Artículo 11 - Tentativa y complicidad

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en aplicación de los artículos 2 a 10 del presente Convenio, con la intención de que dicho delito sea cometido.

2. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos previstos en aplicación de los artículos 3 a 5, 7, 8, 9.1.a) y 9.1.c) del presente Convenio.

3. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

### Artículo 12 - Responsabilidad de las personas jurídicas

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del presente Convenio, cuando estos sean cometidos por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:

a. un poder de representación de la persona jurídica;
b. una autorización para tomar decisiones en nombre de la persona jurídica;
c. una autorización para ejercer funciones de control en el seno de la persona jurídica.

2. Además de los casos previstos en el párrafo 1 del presente artículo, Cada Parte adoptara las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito previsto en aplicación del presente Convenio por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad.

3. Dependiendo de los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

### Artículo 13 - Sanciones y medidas

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en aplicación de los artículos 2 a 11 estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2. Las Partes garantizaran la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

## Sección 2 - Derecho procesal

*Título 1 - Disposiciones comunes*

### Artículo 14 - Ámbito de aplicación de las disposiciones de procedimiento

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección a los efectos de investigación o de procedimientos penales específicos.

2. Salvo que se establezca lo contrario en el artículo 21, cada Parte aplicara los poderes y procedimientos mencionados en el párrafo 1 del presente artículo:

a. a los delitos previstos en aplicación de los artículos 2 a 11 del presente Convenio;
b. a cualquier otro delito cometido por medio de un sistema informático; y
c. a la obtención de pruebas electrónicas de cualquier delito.

3. a. Las Partes podrán reservarse el derecho a aplicar las medidas mencionadas en el artículo 20 únicamente a los delitos o categorías de delitos especificados en su reserva, siempre que el repertorio de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que dicha Parte aplique las medidas mencionadas en el artículo 21. Las Partes trataran de limitar tal reserva de modo que sea posible la más amplia aplicación de la medida mencionada en el artículo 20.

b. Cuando, a causa de las restricciones que imponga su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas previstas en los artículos 20 y 21 a las comunicaciones transmitidas dentro de un sistema informático de un proveedor de servicios:

i. que se haya puesto en funcionamiento para un grupo restringido de usuarios, y
ii. que no emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado,

dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Las Partes trataran de limitar este tipo de reservas de modo que de modo que sea posible la más amplia aplicación de las medidas previstas en los artículos 20 y 21.

### Artículo 15 - Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos

derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.

3. Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Parte examinara los efectos de los poderes y procedimientos mencionados en la presente Sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

*Título 2 - Conservación rápida de datos informáticos almacenados*

### Artículo 16 - Conservación rápida de datos informáticos almacenados

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación.

2. Cuando una Parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, la Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y a proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el fin de que las autoridades competentes puedan obtener su revelación. Las Partes podrán prever la renovación de dicha orden.

3. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para obligar a la persona que custodia los datos o a otra persona encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

### Artículo 17 - Conservaci6n y revelaci6n parcial rápidas de los datos relativos al tráfico

1. Con el fin de garantizar la conservación de los datos relativos al tráfico, en aplicación del artículo 16, cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para:

a. garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de dicha comunicación; y
b. asegurar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicha Parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

*Título 3 - Orden de presentación*

### Artículo 18 - Orden de presentación

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a. a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; y
b. a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios;

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

3. A los efectos del presente artículo, se entenderá por «datos relativos a los abonados» cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:

a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;
b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio;
c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

*Título 4 - Registro y confiscación de datos informáticos almacenados*

### Artículo 19 - Registro y confiscación de datos informáticos almacenados

a. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de un

modo similar:

b. a todo sistema informático o a parte del mismo, así como a los datos informáticos en el almacenados; y
c. a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos en su territorio.

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para asegurarse de que, cuando, de conformidad con el apartado 1.a), sus autoridades registren o tengan acceso de un modo similar a un sistema informático específico o a una parte del mismo y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial, puedan extender rápidamente el registro o el acceso de un modo similar al otro sistema.

2. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1 o 2. Estas medidas incluirán las siguientes prerrogativas:

a. confiscar u obtener de un modo similar un sistema informático o una parte del mismo, o un dispositivo de almacenamiento informático;
b. realizar y conservar una copia de esos datos informáticos;
c. preservar la integridad de los datos informáticos almacenados pertinentes; y
d. hacer inaccesibles o suprimir dichos datos informáticos del sistema informático consultado.

3. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

*Título 5 - Obtención en tiempo real de datos informáticos*

## Artículo 20 - Obtención en tiempo real de datos relativos al tráfico

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes:

a. a obtener o grabar con medios técnicos existentes en su territorio, y
b. a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas:

   i. a obtener o a grabar con medios técnicos existentes en su territorio, o
   ii. a ofrecer a las autoridades competentes su colaboración y su asistencia para

obtener o grabar en tiempo real los datos relativos al tráfico asociados a comunicaciones especificas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones especificas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio.

3. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

## Artículo 21 - Interceptación de datos relativos al contenido

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno a:

a. obtener o grabar con medios técnicos existentes en su territorio, y
b. obligar a un proveedor de servicios, en la medida de sus capacidades técnicas, a:

   i. obtener o grabar con medios técnicos existentes en su territorio, o
   ii. prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar,

en tiempo real los datos relativos al contenido de comunicaciones especificas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones especificas transmitidas en su territorio con medios técnicos existentes en ese territorio.

3. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Sección 3 - Jurisdicción

### Artículo 22 - Jurisdicción

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del presente Convenio, cuando el delito se haya cometido:

a. en su territorio; o
b. a bordo de un buque que enarbole su pabellón; o
c. a bordo de una aeronave matriculada según sus leyes; o
d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

2. Las Partes podrán reservarse el derecho a no aplicar, o a aplicar solo en determinados casos o condiciones, las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier parte de dichos apartados.

3. Cada Parte adoptara las medidas que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito mencionado en el párrafo 1 del artículo 24 del presente Convenio cuando el presunto autor del mismo se halle en su territorio y no pueda ser extraditado a otra Parte por razón únicamente de su nacionalidad, previa demanda de extradición.

4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

5. En el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebraran consultas, cuando ello sea oportuno, con el fin de decidir que jurisdicción es más adecuada para entablar la acción penal.

## Capitulo III - Cooperación internacional

### Sección 1 - Principios generales

*Título 1 - Principios generales relativos a la cooperación internacional*

### Artículo 23 - Principios generales relativos a la cooperación internacional

Las Partes cooperaran entre sí en la mayor medida posible de conformidad con las disposiciones del presente Capitulo, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno, a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

*Título 2 - Principios relativos a la extradición*

## Artículo 24 - Extradición

1. a. El presente artículo se aplicará a la extradición entre las Partes por los delitos definidos de conformidad con los artículos 2 a 11 del presente Convenio, siempre que sean castigados por la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración de al menos un ano, o con una pena más grave.

b. Cuando se aplique una pena mínima diferente en virtud de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE n° 24), o de un acuerdo basado en legislación uniforme o recíproca, se aplicará la pena mínima prevista en dicho tratado o acuerdo.

2. Se considerará que los delitos descritos en el párrafo 1 del presente artículo están incluidos entre los delitos que pueden dar lugar a extradición en todos los tratados de extradición concluidos entre o por las Partes. Las Partes se comprometerán a incluir dichos delitos entre los que pueden dar lugar a extradición en todos los tratados de extradición que puedan concluir.

3. Cuando una parte que condicione la extradición a la existencia de un tratado reciba una demanda de extradición de otra Parte con la que no ha concluido ningún tratado de extradición, podrá tomar el presente Convenio como fundamento jurídico de la extradición en relación con cualquiera de los delitos previstos en el párrafo 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el párrafo 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.

5. La extradición estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de extradición vigentes, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6. Si se deniega la extradición por un delito mencionado en el párrafo 1 del presente artículo únicamente por razón de la nacionalidad de la persona reclamada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes a efectos de la acción penal pertinente, e informará, a su debido tiempo, de la conclusión del asunto a la Parte requirente. Dichas autoridades tomaran su decisión y realizaran sus investigaciones y procedimientos del mismo modo que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.

7. a. Cada Parte comunicara al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de las demandas de extradición o de detención provisional, en ausencia de tratado.

b. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizara en todo

momento la exactitud de los datos que figuren en el registro.

*Título 3 - Principios generales relativos a la asistencia mutua*

## Artículo 25 - Principios generales relativos a la asistencia mutua

1. Las Partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.

2. Cada Parte adoptara asimismo las medidas legislativas y de otro tipo que resulten necesarias para cumplir con las obligaciones establecidas en los artículos 27 a 35.

3. Cada Parte podrá, en caso de urgencia, formular una solicitud de asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y de autenticación (incluido el criptado, en caso necesario), con confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación.

4. Salvo en caso de que se disponga expresamente otra cosa en los artículos del presente Capitulo, la asistencia mutua estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de los cuales la Parte requerida puede rechazar la cooperación. La Parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los artículos 2 a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal.

5. Cuando, de conformidad con lo dispuesto en el presente Capitulo, la Parte requerida este autorizada a condicionar la asistencia mutua a la existencia de doble tipificación penal, se considerara que dicha condición se satisface si el acto que constituye delito, y para el que se solicita la asistencia mutua, está tipificado como tal en su derecho interno, independientemente de que dicho derecho interno incluya o no el delito en la misma categoría o lo denomine o no con la misma terminología que la Parte requirente.

## Artículo 26 - Información espontánea

1. Dentro de los límites de su derecho interno y sin que exista demanda previa, una Parte podrá comunicar a otra Parte información obtenida de sus propias investigaciones si considera que ello puede ayudar a la Parte destinataria a iniciar o a concluir investigaciones o procedimientos en relación con delitos previstos de conformidad con el presente Convenio, o cuando dicha información pueda conducir a una petición de cooperación de dicha Parte en virtud del presente Capitulo.

2 Antes de comunicar dicha información, la Parte que la proporciona podrá pedir que sea tratada de forma confidencial o que solo se utilice bajo ciertas condiciones. Si la Parte destinataria no puede atender a dicha petición, deberá informar de ello a la otra Parte, que decidirá a continuación si, no obstante, debe proporcionar la información. Si la Parte destinataria acepta la información bajo las condiciones establecidas, estará obligada a

respetarlas.

*Título 4 - Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables*

## Artículo 27 - Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o reciproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones de los párrafos 2 a 9 del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes implicadas decidan aplicar en su lugar la totalidad o una parte del resto del presente artículo.

2. a. Cada Parte designara una o varias autoridades centrales encargadas de enviar las solicitudes de asistencia mutua o de responder a las mismas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución;

b. las autoridades centrales comunicaran directamente entre sí;

c. en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicara al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en aplicación del presente párrafo.

d. el Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizara en todo momento la exactitud de los datos que figuren en el registro.

3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con el procedimiento especificado por la Parte requirente, salvo cuando dicho procedimiento sea incompatible con la legislación de la Parte requerida.

4. Además de las condiciones o los motivos de denegación previstos en el párrafo 4 del artículo 25, la asistencia mutua puede ser denegada por la Parte requerida:

a. si la solicitud tiene que ver con un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
b. si la Parte requerida estima que acceder a la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

5. La Parte requerida podrá aplazar su actuación en respuesta a una solicitud si dicha actuación puede perjudicar a investigaciones o procedimientos llevados a cabo por sus autoridades.

6. Antes de denegar o aplazar su cooperación, la Parte requerida estudiara, previa consulta con la Parte requirente cuando proceda, si puede atenderse la solicitud parcialmente o bajo las condiciones que considere necesarias.

7. La Parte requerida informara rápidamente a la Parte requirente del curso que prevé

dar a la solicitud de asistencia. Deberá motivar toda denegación o aplazamiento de la misma. La Parte requerida informara asimismo a la Parte requirente de cualquier motivo que imposibilite la ejecución de la asistencia o que pueda retrasarla sustancialmente.

8. La Parte requirente podrá solicitar que la Parte requerida mantenga confidenciales la presentación y el objeto de cualquier solicitud formulada en virtud del presente Capitulo, salvo en la medida en que sea necesario para la ejecución de la misma. Si la Parte requerida no puede acceder a la petición de confidencialidad, deberá informar de ello sin demora a la Parte requirente, quien decidirá a continuación si, no obstante, la solicitud debe ser ejecutada.

9. a. En caso de urgencia, las autoridades judiciales de la Parte requirente podrán dirigir directamente a las autoridades homologas de la Parte requerida las solicitudes de asistencia y las comunicaciones relativas a las mismas. En tales casos, se remitirá simultáneamente una copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente.

b. Toda solicitud o comunicación en virtud del presente párrafo podrá formularse a través de la Organización Internacional de Policía Criminal (Interpol).

c. Cuando se formule una solicitud en aplicación del apartado a) del presente artículo y la autoridad no tenga competencia para tratarla, la remitirá a la autoridad nacional competente e informara directamente de ello a la Parte requirente.

d. Las solicitudes o comunicaciones realizadas en aplicación del presente párrafo que no impliquen medidas coercitivas podrán ser transmitidas directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida.

e. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, las Partes podrán informar al Secretario General del Consejo de Europa de que, en aras de la eficacia, las solicitudes formuladas en virtud del presente párrafo deberán dirigirse a su autoridad central.

## Artículo 28 - Confidencialidad y restricciones de uso

1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o reciproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes interesadas decidan aplicar en su lugar la totalidad o una parte del presente artículo.

2. La Parte requerida podrá supeditar la transmisión de información o de material en respuesta a una solicitud al cumplimiento de las siguientes condiciones:

a. que se preserve su confidencialidad cuando la solicitud de asistencia no pueda ser atendida en ausencia de dicha condición; o
b. que no se utilicen para investigaciones o procedimientos distintos a los indicados en la solicitud.

3. Si la Parte requirente no pudiera satisfacer alguna de las condiciones mencionadas en el párrafo 2, informará de ello sin demora a la Parte requerida, quien determinará a continuación si, no obstante, la información ha de ser proporcionada. Si la Parte requirente acepta esta condición, estará obligada a cumplirla.

4. Toda Parte que proporcione información o material supeditado a alguna de las condiciones mencionadas en el párrafo 2 podrá exigir a la otra Parte precisiones sobre el uso que haya hecho de dicha información o material en relación con dicha condición.

## Sección 2 - Disposiciones específicas

*Título 1 - Asistencia mutua en materia de medidas provisionales*

### Artículo 29 - Conservación rápida de datos informáticos almacenados

1. Una Parte podrá solicitar a otra Parte que ordene o imponga de otro modo la conservación rápida de datos almacenados por medio de sistemas informáticos que se encuentren en el territorio de esa otra Parte, y en relación con los cuales la Parte requirente tenga intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, la confiscación o la obtención por un medio similar, o a la revelación de dichos datos.

2. En toda solicitud de conservación formulada en virtud del párrafo 1 deberá precisarse:

a. la autoridad que solicita la conservación;
b. el delito objeto de la investigación o de procedimientos penales y una breve exposición de los hechos relacionados con el mismo;
c. los datos informáticos almacenados que deben conservarse y su relación con el delito;
d. toda información disponible que permita identificar al responsable de la custodia de los datos informáticos almacenados o el emplazamiento del sistema informático;
e. la necesidad de la medida de conservación; y
f. que la Parte tiene intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar, o a la revelación de los datos informáticos almacenados.

3. Tras recibir la solicitud de otra Parte, la Parte requerida deberá adoptar todas las medidas adecuadas para proceder sin demora a la conservación de los datos solicitados, de conformidad con su derecho interno. A los efectos de responder a solicitudes de este tipo no se requiere la doble tipificación penal como condición para proceder a la conservación.

4. Cuando una Parte exige la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de los datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11 del presente Convenio, podrá reservarse el derecho a denegar la solicitud de conservación en virtud del presente artículo en caso de que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá la condición de la doble tipificación penal.

5. Asimismo, las solicitudes de conservación solo podrán ser denegadas si:

a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

6. Cuando la Parte requerida considere que la conservación por si sola de los datos no bastara para garantizar su disponibilidad futura, o que pondrá en peligro la confidencialidad de la investigación de la Parte requirente, o causara cualquier otro perjuicio a la misma, informara de ello rápidamente a la Parte requirente, quien determinará a continuación la conveniencia, no obstante, de dar curso a la solicitud.

7. Las medidas de conservación adoptadas en respuesta a solicitudes como la prevista en el párrafo 1 serán válidas por un periodo mínimo de 60 días, con el fin de que la Parte requirente pueda presentar una solicitud con vistas al registro o el acceso por un medio similar, la confiscación o la obtención por un medio similar, o la revelación de los datos. Una vez recibida la solicitud, los datos deberán conservarse hasta que se tome una decisión sobre la misma.

### Artículo 30 - Revelación rápida de datos conservados

1. Si, al ejecutar una solicitud formulada de conformidad con el artículo 29 para la conservación de datos relativos al tráfico de una determinada comunicación la Parte requerida descubriera que un proveedor de servicios de otro Estado ha participado en la transmisión de dicha comunicación, dicha Parte revelara rápidamente a la Parte requirente un volumen suficiente de datos relativos al tráfico para que pueda identificarse al proveedor de servicios, así como la vía por la que la comunicación ha sido transmitida.

2. La revelación de datos relativos al tráfico en aplicación del párrafo 1 solo podrá ser denegada si:

a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

*Título 2 - Asistencia mutua en relación con los poderes de investigación*

### Artículo 31 - Asistencia mutua en relación con el acceso a datos almacenados

1. Una Parte podrá solicitar a otra Parte el registro o el acceso de un modo similar, la confiscación o la obtención de un modo similar o la revelación de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, incluidos los datos conservados de conformidad con el artículo 29.

2. La Parte requerida responderá a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con las disposiciones pertinentes del presente Capítulo.

3. La solicitud deberá responderse lo más rápidamente posible en los siguientes casos:

a. cuando existan motivos para creer que los datos pertinentes están particularmente expuestos al riesgo de pérdida o de modificación; o
b. cuando los instrumentos, acuerdos o legislación mencionados en el párrafo 2 prevean una cooperación rápida.

### Artículo 32 - Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público

Una Parte podrá, sin autorización de otra:

a. tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos; o
b. tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos por medio de ese sistema informático.

### Artículo 33 - Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico

1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. A reserva de las disposiciones del párrafo 2, dicha asistencia mutua estará sujeta a las condiciones y procedimientos previstos en el derecho interno.

2. Cada Parte prestara dicha asistencia al menos en relación con los delitos para los cuales sería posible la obtención en tiempo real de datos relativos al tráfico en situaciones análogas a nivel interno.

### Artículo 34 - Asistencia mutua en relación con la interceptación de datos relativos al contenido

Las Partes se prestarán asistencia mutua, en la medida en que lo permitan sus tratados y leyes internas aplicables, para la obtención o el registro en tiempo real de datos relativos al contenido de comunicaciones específicas transmitidas por medio de un sistema informático.

*Titulo 3 - Red 24/7*

### Artículo 35 - Red 24/7

1. Cada Parte designará un punto de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que figuran a continuación, o su aplicación directa si lo permite el derecho y la práctica internos:

a. asesoramiento técnico;
b. conservación de datos, de conformidad con los artículos 29 y 30; y
c. obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos.

2. a. El punto de contacto de una Parte dispondrá de los medios para comunicarse con el punto de contacto de otra Parte siguiendo un procedimiento acelerado.

b. Si el punto de contacto designado por una Parte no depende de la autoridad o autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, dicho punto de contacto se asegurará de poder actuar coordinadamente con esta o estas autoridades por medio de un procedimiento acelerado.

3. Cada Parte garantizará la disponibilidad de personal formado y equipado con objeto de facilitar el funcionamiento de la red.

## Capítulo IV - Cláusulas finales

### Artículo 36 - Firma y entrada en vigor

1. El presente Convenio está abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.

2. El presente Convenio estará sujeto a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario General del Consejo de Europa.

3. El presente Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que cinco Estados, de los cuales al menos tres deberán ser miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio, de conformidad con lo dispuesto en los párrafos 1 y 2.

4. Para todo Estado signatario que exprese ulteriormente su consentimiento para quedar vinculado por el Convenio, este entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado dicho consentimiento, de conformidad con lo dispuesto en los párrafos 1 y 2.

### Artículo 37 - Adhesión al Convenio

1. A partir de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá, previa consulta con los Estados contratantes del Convenio y habiendo obtenido su consentimiento unánime, invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo de Europa y que no haya participado en su elaboración. La decisión se adoptará respetando la mayoría establecida en el artículo 20.d del Estatuto del Consejo de Europa y con el voto unánime de los representantes de los Estados contratantes con derecho a formar parte del Comité de Ministros.

2. Para todo Estado que se adhiera al Convenio de conformidad con el párrafo 1 precedente, el Convenio entrara en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.

### Artículo 38 - Aplicación territorial

1. En el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, todo Estado podrá designar el territorio o los territorios a los que se aplicará el presente Convenio.

2. Posteriormente, todo Estado podrá, en cualquier momento y por medio de una declaración dirigida al Secretario General del Consejo de Europa, hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. El Convenio entrara en vigor respecto de dicho territorio el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.

3. Toda declaración formulada en virtud de los dos párrafos precedentes podrá ser retirada, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

### Artículo 39 - Efectos del Convenio

1. El objeto del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones:

– del Convenio Europeo de Extradición, abierto a la firma el 13 de diciembre de 1957 en Paris (STE nº 24)

– del Convenio Europeo de Asistencia Judicial en Materia Penal, abierto a la firma el 20 de abril de 1959 en Estrasburgo (STE nº 30),

– del Protocolo adicional al Convenio Europeo de Asistencia Judicial en Materia Penal, abierto a la firma el 17 de marzo de 1978 en Estrasburgo (STE nº 99).

2. Si dos o más Partes han celebrado ya un acuerdo o un tratado relativo a las cuestiones contempladas en el presente Convenio, o han regulado de otro modo sus relaciones al respecto, o si lo hacen en el futuro, podrán asimismo aplicar el citado acuerdo o tratado, o regular sus relaciones de conformidad con el mismo, en lugar del presente Convenio. No obstante, cuando las Partes regulen sus relaciones respecto de las cuestiones objeto del presente Convenio de forma distinta a la prevista en el mismo, lo harán de modo que no sea incompatible con los objetivos y principios del Convenio.

3. Nada de lo dispuesto en el presente Convenio afectara a otros derechos, restricciones, obligaciones y responsabilidades de cada Parte.

## Artículo 40 – Declaraciones

Mediante declaración por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir, llegado el caso, uno o varios elementos complementarios previstos en los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e).

## Artículo 41 - Cláusula federal

1. Un Estado federal podrá reservarse el derecho a cumplir las obligaciones especificadas en el Capítulo II del presente Convenio en la medida en que estas sean compatibles con los principios fundamentales por los que se rijan las relaciones entre su gobierno central y los estados que lo constituyen u otras entidades territoriales análogas, a condición de que pueda garantizar la cooperación según lo previsto en el Capítulo III.

2. Cuando formule una reserva en virtud del párrafo 1, un Estado federal no podrá hacer uso de los términos de dicha reserva para excluir o reducir de manera sustancial sus obligaciones en virtud del Capítulo II. En todo caso, se dotará de medios amplios y efectivos para aplicar las medidas previstas en el citado Capitulo.

3. En lo relativo a las disposiciones del presente Convenio cuya aplicación sea competencia legislativa de cada uno de los estados constituyentes u otras entidades territoriales análogas, que no estén obligados por el sistema constitucional de la federación a adoptar medidas legislativas, el gobierno federal pondrá dichas disposiciones en conocimiento de las autoridades competentes de los estados constituyentes junto con su opinión favorable, alentándolas a adoptar las medidas adecuadas para su aplicación.

## Artículo 42 - Reservas

Mediante notificación por escrito dirigida al Secretario del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el párrafo 2 del artículo 4, el párrafo 3 del artículo 6, el párrafo 4 del artículo 9, el párrafo 3 del artículo 10, el párrafo 3 del artículo 11, el párrafo 3 del artículo 14, el párrafo 2 del artículo 22, el párrafo 4 del artículo 29 y el párrafo 1 del artículo 41. No podrá formularse ninguna otra reserva.

## Artículo 43 - Mantenimiento y retirada de las reservas

1. Una Parte que haya formulado una reserva de conformidad con el articulo 42 podrá retirarla total o parcialmente mediante notificación por escrito dirigida al Secretario General del Consejo de Europa. Dicha retirada surtirá efecto en la fecha en que el Secretario General reciba la notificación. Si en la notificación se indica una fecha a partir de la cual ha de hacerse efectiva la retirada de una reserva y esta fecha es posterior a la fecha en la que el Secretario General ha recibido la notificación, la retirada se hará efectiva en dicha fecha posterior.

2. Una Parte que haya formulado una reserva de las mencionadas en el artículo 42 retirará dicha reserva, total o parcialmente, tan pronto como lo permitan las circunstancias.

3. El Secretario General del Consejo de Europa podrá solicitar periódicamente a las Partes que hayan formulado una o varias reservas conforme a lo dispuesto en el artículo 42, información sobre las perspectivas de su retirada.

### Artículo 44 – Enmiendas

1. Cada Parte podrá proponer enmiendas al presente Convenio, que el Secretario General del Consejo de Europa comunicará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado que se haya adherido o que haya sido invitado a adherirse de conformidad con lo dispuesto en el artículo 37.

2. Toda enmienda propuesta por cualquiera de las Partes será comunicada al Comité Europeo para Problemas Criminales (CDPC), quien someterá al Comité de Ministros su opinión sobre la enmienda propuesta.

3. El Comité de Ministros examinará la enmienda propuesta y la opinión presentada por el CDPC y, previa consulta con los Estados no miembros Partes en el presente Convenio, podrá adoptar la enmienda.

4. El texto de cualquier enmienda adoptada por el Comité de Ministros de conformidad con lo dispuesto en el párrafo 3 del presente artículo será remitido a las Partes para su aceptación.

5. Toda enmienda adoptada de conformidad con el párrafo 3 del presente artículo entrara en vigor treinta días después de que todas las Partes hayan informado al Secretario General de su aceptación.

### Artículo 45 - Solución de controversias

1. Se mantendrá informado al Comité Europeo para Problemas Criminales (CDPC) del Consejo de Europa acerca de la interpretación y la aplicación del presente Convenio.

2. En caso de controversia entre las Partes sobre la interpretación o la aplicación del presente Convenio, las Partes intentarán llegar a un acuerdo mediante negociación o por cualquier otro medio pacifico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes en litigio, o a la Corte Internacional de Justicia, según acuerden dichas Partes.

### Artículo 46 - Consultas entre las Partes

1. Las Partes se consultarán periódicamente, según sea necesario, con el fin de facilitar:

a. la utilización y la aplicación efectivas del presente Convenio, incluida la identificación de cualquier problema al respecto, así como las repercusiones de toda declaración o reserva formulada de conformidad con el presente Convenio;
b. el intercambio de información sobre novedades jurídicas, políticas o técnicas

importantes observadas en el ámbito de la delincuencia informática y la obtención de pruebas en formato electrónico;

c. el estudio de la posibilidad de ampliar o enmendar el Convenio.

2. Se informará periódicamente al Comité Europeo para Problemas Criminales (CDPC) del resultado de las consultas mencionadas en el párrafo 1.

3. En caso necesario, el Comité Europeo para Problemas Criminales (CDPC) facilitará las consultas mencionadas en el párrafo 1 y adoptará las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Expirado un plazo de tres años como máximo desde la entrada en vigor del presente Convenio, el CDPC procederá, en cooperación con las Partes, a una revisión de todas las disposiciones de la Convención y propondrá, si procede, las enmiendas pertinentes.

4. Salvo cuando el Consejo de Europa los asuma, los gastos que ocasione la aplicación de las disposiciones del párrafo 1 serán sufragados por las Partes, en la forma que ellas mismas determinen.

5. Las Partes recibirán asistencia del Secretario del Consejo de Europa en el ejercicio de las funciones que dimanan del presente artículo.

### Artículo 47 - Denuncia

1. Las Partes podrán denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.

2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

### Artículo 48 - Notificación

El Secretario General del Consejo de Europa notificara a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio, así como a cualquier Estado que se haya adherido o que haya sido invitado a adherirse al mismo:

a. cualquier firma;
b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;
c. cualquier fecha de entrada en vigor del presente Convenio de conformidad con los artículos 36 y 37;
d. cualquier declaración presentada de conformidad con el articulo 40 o cualquier reserva formulada en virtud del artículo 42;
e. cualquier otro acto, notificación o comunicación relativos al presente Convenio.

En fe de lo cual, los infrascritos, debidamente autorizados a tal efecto, firman el presente Convenio.

Hecho en Budapest, el 23 de noviembre de 2001, en versión francesa e inglesa, ambos textos igualmente auténticos, y en un ejemplar único que se depositara en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copia certificada a cada uno de los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del Convenio y a cualquier Estado invitado a adherirse al mismo.

## Anexo B

SRE

"2017, Año del Centenario de la Promulgación de la Constitución Política de los Estados Unidos Mexicanos"

Unidad de Transparencia

Oficio Núm. UDT-6983/2017
Folio: 0000500215217
Asunto: Solicitud de acceso a la información

**Ciudad de México, a 18 de octubre de 2017**

**C. Solicitante.**
Presente.

Como respuesta a su solicitud presentada a través del sistema PLATAFORMA NACIONAL DE TRANSPARENCIA, folio **0000500215217**, a través de la que requirió:

> **"Solicito la posición oficial de México respecto a la adhesión al Convenio de Budapest, así como los avances en la materia.**
> **Convenio de Budapest"**

Se informa que la misma fue turnada para su atención a la **Consultoría Jurídica**, a la **Dirección General para Europa,** así como a la **Dirección General para la Organización de las Naciones Unidas,** atendiendo lo dispuesto en el artículo 133 de la Ley Federal de Transparencia y Acceso a la Información Pública, en ese sentido se hace de su conocimiento lo siguiente:

El Convenio sobre Ciberdelincuencia fue adoptado en Budapest el 23 de noviembre de 2001, en el marco del Consejo de Europa, y constituye el único tratado internacional de carácter "universal" vigente en materia de combate a los delitos cibernéticos. Actualmente, 55 países son Parte de este Instrumento.

Por lo que respecta a la postura del Estado mexicano ante el tratado referido, debe informársele al solicitante que el Ejecutivo Federal se encuentra evaluando las disposiciones del Convenio a fin de determinar si el marco jurídico vigente permitiría cumplir con las obligaciones contenidas en el mismo.

Una vez que este análisis concluya, se estará en aptitud de considerar la viabilidad de que el Estado mexicano se adhiera al Convenio, o bien identificar las medidas legislativas que sería menester implementar para poder ser parte de este Instrumento.

Se reitera el interés de esta Unidad de Transparencia en atender su solicitud y se hace de su conocimiento el derecho de interponer recurso de revisión ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, de conformidad con los Artículos 147, 148 y 149 de la Ley Federal de Transparencia y Acceso a la Información Pública.

Plaza Juárez núm. 20, Piso PB, Col. Centro, Del. Cuauhtémoc, C.P. 06010, Ciudad de México,
Tels.: (55) 3686 - 5023 unidad.transparencia@sre.gob.mx

**Atentamente**
Titular de la Unidad de Transparencia

**Oscar Sánchez Delgado**

c.c.p.- Comité de Transparencia.- Presente.
Órgano Interno de Control.- Presente.

KHP/jggv*

Plaza Juárez núm. 20, Piso PB, Col. Centro, Del. Cuauhtémoc, C.P. 06010, Ciudad de México,
Tels.: (55) 3686 - 5023 unidad.transparencia@sre.gob.mx

**Glosario Digital**[274]

***Advanced Research Projects Agency* (ARPANET).** Red creada por la Agencia de Proyectos de Investigación Avanzados para estudiar la seguridad de las redes de ordenadores en caso de guerra nuclear.

**Aplicación.** Programa de *software* diseñado para una determinada función, como un procesador de textos o una hoja de cálculo.

**Banda ancha.** Técnica para transmitir una gran cantidad de datos, voz y video a largas distancias.

**Bit.** Acrónimo de *binary digit*. Unidad básica de información en un sistema de numeración binaria (compuesto tan solo de ceros y unos).

***Blog.*** Página web personal, actualizada con regularidad, con el objetivo de compartir ideas personales sobre uno o varios temas.

***Browser*.** Herramienta de *software* que permite al usuario navegar a través de Internet y enlazar desde un sitio a otro.

**Ciberespacio.** Mundo de los ordenadores en red donde se interactúa sin presencia física.

***Cookie*.** Pequeños fragmentos de datos almacenados en un ordenador por un navegador para permitir a un sitio web desempeñar algunas funciones.

**Correo electrónico.** Servicio de intercambio de mensajes entre usuarios, que pueden incluir elementos multimedia.

[274] Chatfield, Tom, *50 cosas que hay que saber sobre el mundo digital*, Ed. Ariel, España, 2012.
Spinello, Richard, *Cyberethics. Morality and Law in Cyberspace*, Jones and Bartlett Publishers, United States of America, 2000.
Tercero, José B., *Sociedad digital: del homo sapiens al hombre digitalis*, Alianza Editorial, España, 1996.

***Dark Web.*** Son sitios a los que ya no se puede acceder en lo absoluto y, por lo tanto, se han “oscurecido” gracias a la interrupción en los procesos por los que se dirige el tráfico.

***Deep Web.*** Sitios subyacentes a la superficie de Internet, que no son visibles para los buscadores y el usuario habitual de la red.

***Domain Name System*****.** Sistema básico que traduce las direcciones web de su forma conocida en palabras a direcciones IP (Protocolo de Internet).

***E-Commerce (Electronic Commerce).*** Modelo de negocios para generar utilidades, tomando ventajas de la funcionalidad de *WWW.*

**Encriptación.** Proceso mediante el cual la información se codifica y se mezcla con el fin de hacerse ilegible para los intrusos; la información es decodificada o convertida a su formato original a través de una clave disponible únicamente para el que recibe el mensaje.

**Fibra óptica.** Cable compuesto de fibra de vidrio que transporta señales ópticas en lugar de eléctricas.

***Fire Wall*****.** Mecanismo de seguridad que controla y protege el acceso entre un ordenador o red de ordenadores e Internet.

***Hacking.*** Proceso de irrumpir en un sistema red o programa informático en contra de los deseos del propietario.

***Hardware*****.** Los componentes físicos de un ordenador, así como sus periféricos. Se distingue del *software*, que son los programas que indican al *hardware* lo que tiene que hacer.

**Hipertexto.** Concepto consistente en vincular varios documentos a través de palabras o frases comunes.

***Hypertext Markup Language (HTML).*** Lenguaje codificado en el que se basa la *World Wide Web*, que indica a los navegadores el aspecto que han de tener y como deben funcionar las páginas web.

**HTTP.** Protocolo de transporte *hipertexto* que permite navegar por la Internet.

**Inteligencia Artificial.** Programas diseñados para que su funcionamiento sea similar a los procesos humanos de toma de decisiones.

**Internet.** Red de ordenadores que usan protocolos *TCP/IP*. // Conjunto de *hardware* y *software* interconectados y que comunica una parte creciente de todos los dispositivos informáticos del mundo.

***Internet Protocol (IP) Address*.** Dirección numérica compuesta de cuatro partes para cualquier sistema conectado a Internet, que define la ubicación de distintos recursos de Internet.

***Local Area Network* (LAN).** Red de área local. Ordenadores conectados entre sí dentro de un área limitada.

***Malware*.** *Software* diseñado con intención maliciosa y a veces delictiva, por parte de su creador.

**Memoria.** Almacenamiento primario de un ordenador, como la *RAM*, distinto de un almacenamiento secundario como el disco duro.

**Módem.** Aparato que convierte las señales digitales en analógicas y viceversa (modular, demodular), y que permite la comunicación de dos ordenadores a través de la línea telefónica.

**Multimedia.** Forma de presentar información, a través de un ordenador, utilizando varios medios, como texto, gráficos o sonido.

**Net.** Apócope de *Internet*.

**Nodo.** Ordenador o cualquier otro dispositivo conectado a una *red*.

***Phising.*** Táctica frecuente por la que los correos de *spam* y las páginas maliciosas intentan obtener detalles personales de usuarios incautos, que pueden ir desde los datos de conexión a una cuenta de correo electrónico, hasta los de una tarjeta de crédito.

**PPP.** *Protocolo* de punto a punto. Método de intercambio de información en *Internet* a través de las líneas telefónicas.

**Protocolo.** Definición del sistema de comunicación de un ordenador. Acuerdo entre diferentes sistemas para trabajar conjuntamente. Conjunto de normas que permiten estandarizar un procedimiento repetitivo.

***Random-access memory* (RAM).** Memoria primaria de un ordenador que contiene instrucciones y datos a los que puede acceder directamente la unidad central de proceso.

**Red.** Interconexión de uno o más ordenadores a través de *hardware* y *software*.

**Redes sociales.** Tendencia definitoria de la actual fase de desarrollo de Internet, cuando la red pasa gradualmente de ser una herramienta para encontrar e identificar información, a otra para encontrar y relacionarse con otras personas. Web 2.0.

**Servidor.** Ordenador que proporciona recursos en una red y que provee de información a los clientes.

**Sistema operativo.** Programa de control que dirige las funciones internas de un ordenador.

***Software*.** Programas de sistemas o aplicaciones escritos en un lenguaje que entiende el ordenador.

***SPAM*.** Correo electrónico no solicitado, enviado de forma masiva por un individuo u organización para hacer publicidad de bienes y servicios a clientes potenciales en Internet.

***Spyware.*** Programa diseñado para grabar y transmitir información sobre hábitos de Internet y usos informáticos.

***Transmision Control Protocol/Internet Protocol* (TCP/IP).** Combinación básica de *protocolos* que rigen la transmisión de información en *Internet*.

**Universal Resource Locator (URL).** Dirección electrónica única para un sitio de Internet.

**Virus y gusanos.** Programas ocultos que se autorreproducen con fines maliciosos dentro de un ordenador o red de ordenadores, como borrar archivos cruciales de un disco duro, hasta la instalación de programas ocultos que permiten controlar remotamente el ordenador.

***WEB 2.0.*** Término usado para hacer una distinción entre la primera década de uso de la web -primariamente utilizada como una herramienta para encontrar y compartir información-, y una segunda década con una cultura digital cada vez más activa y, que dio origen al auge de los *blogs* y redes sociales.

***World Wide Web (WWW).*** Sistema lógico de acceso, navegación y búsqueda de la información disponible en Internet.