¿ES NECESARIO REGULAR LA DARK WEB?

IS IT NECESSARY TO REGULATE THE DARK WEB?

(2021)

Oscar Uribe Benítez

RESUMEN: El objetivo del trabajo es demostrar la necesidad de regular jurídicamente a nivel nacional e internacional el ciberespacio, en especial las plataformas de la *Dark Web*, para brindar protección a los derechos humanos de los usuarios y cooperación con otros estados para combatir el cibercrimen. Para ello se utilizaron los métodos histórico, político, descriptivo, doctrinario y legal extranjero e internacional. La conclusión más importante es que el ciberespacio, es el nuevo *Nomos* planetario que quiere conquistar y dominar el hombre, para satisfacer todo tipo de intereses. Esto implica, quizá, la necesidad de su regulación jurídica.

PALABRAS CLAVE: Ciberespacio, gobernanza de Internet, plataformas *Dark Web*, delito y derechos humanos.

ABSTRACT: The objective of the work is to demonstrate the need to legally regulate cyberspace at the national and international level, especially Dark Web platforms, to provide protection for the human rights of users and cooperation with other states to combat cybercrime. For which the historical, political, descriptive, doctrinal and legal foreign and international methods were used. The most important conclusión is that the cyberspace, is the new *Nomos* planetary that wants to conquer and dominate man, to satisfy all kinds of interests. This implies, maybe, the need for its legal regulation.

KEY WORDS: Cyberspace, Internet governance, Dark Web platforms, crime and human rights

SUMARIO: I. *Introducción*. II. *Del Nomos de la tierra al Nomos del ciberespacio y su relación con el derecho de gentes y el derecho internacional contemporáneo, respectivamente.* III. *Internet y la Dark Web.* IV. *Organizaciones internacionales que luchan contra las actividades delictivas y mercados ilícitos en la Dark Web*. V. *Conclusiones*. VI. *Referencias*.

I

INTRODUCCIÓN

Los elementos naturales tierra, mar y aire han sido para el hombre objeto de sendas revoluciones espaciales planetarias, las que han constituido sus respectivos *nomos* y han configurado el derecho que rige a la comunidad internacional. El hombre en su afán infinito de conquista creó un nuevo elemento de carácter artificial: el ciberespacio, al que podríamos considerarlo como objeto de una cuarta revolución espacial planetaria que tiene su propio *Nomos* y que está en ciernes la determinación de su regulación por un tratado específico o por ciber normas por el derecho internacional público. Es probable que en el futuro las revoluciones espaciales planetarias salten a revoluciones espaciales en el universo, como lo visualiza el físico teórico Michio Kaku con la teoría del hiperespacio (en su versión más avanzada teoría de supercuerdas) que agrega seis dimensiones espaciales a las cuatro ya conocidas (longitud, anchura, altura y tiempo), la cual puede proporcionar un medio para hacer un túnel a través del espacio y tiempo, a lo que los cosmólogos proponen la posibilidad de universos paralelos que pueden conectarse con los agujeros de gusano; por ende, asevera Kaku que cualquier civilización que domine la teoría del ciberespacio se convertirá en el señor del universo.[1] En el contexto de las revoluciones espaciales planetarias, en el apartado II se desarrolla del *Nomos* de la tierra al *Nomos* del ciberespacio y su relación con el derecho de gentes, para exponer lo que consideramos el nuevo *Nomos* del ciberespacio y su relación con el derecho internacional contemporáneo, e inclusive nacional.

[1] KAKU, Michio, *HIPERESPACIO Una odisea científica a través de universos paralelos, distorsiones del tiempo y la décima dimensión,* Traductor Javier García Sanz, España, Crítica-Drakontos, 2017, pp. 7-13.

En el apartado III, realizamos una breve descripción de la internet y la *Dark Web*, que son utilizadas para cometer delitos clandestinamente. En el apartado IV, damos cuenta de los esfuerzos de organizaciones internacionales que combaten las actividades delictivas en la *Dark Web.* En el apartado V expresamos nuestras conclusiones, y en el VI describimos las referencias que utilizamos.

II

DEL *NOMOS* DE LA TIERRA AL *NOMOS* DEL CIBERESPACIO Y SU RELACIÓN CON EL DERECHO DE GENTES Y EL DERECHO INTERNACIONAL CONTEMPORÁNEO, RESPECTIVAMENTE

1. *El Nomos de la tierra y su relación con el derecho de gentes* El jurista y filósofo político alemán Carl Schmitt, en el escenario de la Segunda Guerra Mundial, publicó en 1942 su ensayo *Tierra y mar*, en el que expone lo que denomina revolución espacial planetaria, como un ensanchamiento tan grande, tan sorprendente que cambian no sólo proporciones y medidas, no únicamente el horizonte externo del hombre, sino también la estructura del concepto mismo de espacio.[2] Considera que hubo tres revoluciones espaciales planetarias. La primera, acontecida en los siglos XVI y XVII, en la época del descubrimiento de América y de la primera circunnavegación de la tierra[3] con la conquista inglesa de los mares.[4] La segunda, iniciada en el siglo XIX, con la electricidad, la aeronáutica y la radiotelegrafía que revolucionaron todos los conceptos espaciales,[5] y la tercera, en el siglo XX, con la aparición del aeroplano, irrumpiendo un tercer elemento del espacio, además de la tierra y el mar, el aire (o quizá el fuego que está implicado en los motores de explosión), como un nuevo medio de comunicación, con lo que proporciones y medidas se alteran más aún y las posibilidades de dominio del hombre sobre la naturaleza y sobre otros hombres se extienden a insospechados dominios; por ende, refiere que ya no entendemos por espacio una simple dimensión de profundidad vacía de todo contenido imaginable, ya que se nos ha convertido en

[2] SCHMITT, Carl, *Tierra y mar,* Traductor Rafael Fernández-Quintanilla, España, editorial Trotta, 2007, p. 49.
[3] *Ibidem,* p. 54.
[4] *Ibidem,* p. 70.
[5] *Ibidem,* p. 79.

campo de fuerzas donde el hombre despliega su energía, su actividad y esfuerzo, o en palabras de Heidegger, en “Ser y tiempo”, el mundo no está en el espacio; por el contrario, es el espacio el que está en el mundo[6].

Schmitt sostiene que en cada revolución espacial surgió un nuevo *Nomos*, el cual es un sustantivo griego que deriva del verbo griego *nemein* y posee tres significados: 1. Toma de posesión, conquista de la tierra, más tarde conquista del mar; 2. Dividir y distribuir aquello de lo que se ha tomado posesión, y 3. Uso, cultivo y la explotación del terreno obtenido mediante la división, por tanto, la producción y consumo.[7] Este es el significado del *Nomos* que surgió en la primera revolución espacial planetaria. Schmitt no se aventuró a reflexionar sobre el viaje a la luna, que pudiera constituir el inicio de una cuarta revolución espacial ya no planetaria sino interplanetaria o cósmica, con la que surgiría un nuevo *Nomos* por la toma del universo y sus planetas, quizá por su imposibilidad o por su muy lejana factibilidad.

El mencionado ensayo fue el esbozo de su brillante obra de Schmitt publicada en 1950 titulada *El Nomos de la Tierra en el Derecho de Gentes del Ius Publicum Europaeum,* en la que sostiene que los grandes actos primitivos del derecho, representan asentamientos sujetos a la tierra, como es el caso de las tomas de la tierra, fundaciones de ciudades y establecimientos de colonias.[8] La toma de la tierra como acto primitivo, considera Schmitt, establece un derecho en dos sentidos: hacia dentro y hacia fuera. Hacia dentro, al interior del grupo que ocupa la tierra, se establece la primera ordenación de todas las condiciones de posesión o propiedad, con la primera división y distribución del suelo. La toma de la tierra en forma conjunta, en su sentido interno es una propiedad suprema de la comunidad en su totalidad, aunque posteriormente en su distribución se individualice. Hacia fuera, el grupo que ocupa una tierra se enfrenta con otros grupos que toman o poseen una tierra. La toma de la tierra con efectos hacia dentro y hacia fuera, es el primer título jurídico en el que se apoya todo derecho posterior[9]. La toma de la tierra es un hecho

[6] *Ibidem,* pp. 80 y 81.
[7] *Ibidem,* p. 58, nota 1 a pie de página.
[8] *Cfr.* SCHMITT, Carl, *El Nomos de la Tierra en el Derecho de Gentes del Ius Publicum Europaem*, Traductora Dora Schilling Thou, España, editorial Comares, 2002, p. 6.
[9] *Ibidem*, p. 7.

jurídico histórico, aunque se haya producido de manera tumultuosa o surgido a veces a raíz de migraciones de pueblos y expediciones de conquista o de la defensa de un territorio frente a extraños[10].

En esta etapa primitiva, destaca Schmitt, se tenía una concepción mítica del mundo, limitado por el océano, por la serpiente de Midgard o las Columnas de Hércules. La protección política de esos límites consistía en fortificaciones fronterizas, una muralla, un limes, etc. Los límites tenían el sentido de separar un orden protegido de un desorden sin paz. Cada imperio se consideraba el mundo y la tierra de fuera algo interesante o el caos, pero un espacio libre y sin soberano abierto a la conquista, a la adquisición de tierras y a la colonización [11]. En este contexto, Schmitt advierte que existía un derecho de gentes en la era pre global del mundo y para robustecer su afirmación nos proporciona una definición medieval de Isidoro de Sevilla que se incorporó en el *Decretum Gratiani* que reza así: … *el Derecho de Gentes es ocupación de tierra, edificación y fortificación de ciudades, guerra, cautiverio, servidumbre, regreso del cautiverio, alianzas y tratados de paz, armisticio, inviolabilidad de enviados y prohibiciones de casamiento con persona de raza foránea* [12].

Aclara Schmitt que este derecho de gentes no abarcaba el planeta[13]. Con el descubrimiento de América se produjo el primer *Nomos* de la tierra que consistía en una cierta relación entre la ordenación espacial de la tierra y la ordenación espacial del mar libre, la que durante 400 años fue la base de un Derecho de Gentes cuyo epicentro era Europa; es decir, era el *Ius publicum europaeum* [14]. Este Derecho de Gentes moderno del siglo XVI al XX, surgió de la disolución de la ordenación medieval cristiana del espacio basada en el imperio y el Papado[15]. Pese a esa definición del derecho de gentes, Juan de Zumárraga y Juan Ramírez, teóricos del siglo XVI, sostuvieron que la guerra de la conquista española fue ilícita

[10] *Ibidem*, p. 8.
[11] *Ibidem*, pp. 12-14.
[12] *Ibidem*, p. 6.
[13] *Ibidem*, p. 12.
[14] *Ibidem*, p. 11.
[15] *Ibidem*, p. 19.

e injusta, así como la privación de la libertad y hacienda de los indios.[16] Tal derecho de gentes global, es llamado por algunos internacionalistas como derecho internacional clásico que inició en el siglo XVI y se prolongó hasta 1945, como efecto de la transformación de la sociedad medieval en multiplicidad de estados soberanos, con omnipotencia en su territorio e independencia ante el Papado y el Imperio, cuya consumación se realizó en el siglo XVII con la Paz de Westfalia[17].

El jurista español Diez de Velasco, refiere que suele distinguirse este derecho internacional clásico en tres etapas históricas: en la primera, el estado moderno concentra y seculariza el poder y sustituye la jerarquía por la pluralidad de estados, cuyo carácter soberano es el centro de gravedad del orden internacional establecido después de la Paz de Westfalia, pero circunscrito a Europa, por ello cuando se relaciona con un poder fuera de la sociedad europea tiende a dominarlo; en esta etapa el derecho internacional público se carece de base autoritaria y de instituciones estables; es decir, era descentralizado e inorgánico. En la segunda etapa, al emanciparse las colonias inglesas y españolas en América, al finalizar el siglo XVIII y XIX, se crea un sistema de estados de civilización europea, los cuales ponen en tela de juicio los valores legitimadores del poder europeo, por lo que mediante la doctrina Monroe se colocan las bases del principio de no intervención en la forma de organización política sobre el continente americano, pero después dicho principio se liga a la soberanía estatal. En la última etapa, en el siglo XIX, la sociedad de estados confeccionó un marco jurídico y político en la Conferencia de Berlín, para colonizar África por su insuficiente nivel de civilización. Esta sociedad de estados occidentales respetó en forma absoluta la soberanía nacional, por ello no se prohibió el uso de la fuerza ni de la guerra. Tampoco había instituciones y organismos que moderaran el poder de los estados. Este derecho internacional clásico siguió siendo descentralizado, pero además oligocrático, para posteriormente entrar en crisis después de la Segunda Guerra Mundial.[18]

---

[16] URIBE BENÍTEZ, Oscar, "Desarrollo histórico y legislativo de la autonomía de los pueblos y comunidades indígenas de México"*, Quórum Legislativo,* México, núm. 99, diciembre 2009, pp. 251 y 252.

[17] *Cfr.* DIEZ DE VELASCO, Manuel, *Instituciones de Derecho Internacional Público*, 16ª edición, España, Tecnos, 2007, p. 61.

[18] *Ibidem*, pp. 61-63.

2. *El Nomos del ciberespacio y su relación con el derecho internacional contemporáneo* A continuación, se expondrá una breve historia y tendencias del ciberespacio.

A) Antecedentes del ciberespacio El término ciberespacio tiene sus raíces etimológicas en el mundo griego *Kubernetes*, que significa "dirigir". Sin embargo, el uso moderno del mundo "cibernético" fue recogido por el matemático de la Segunda Guerra Mundial Norbert Wiener en su libro de 1948 *Cybernetics: Or, Control and Communications in the Animal and the Machine*. El uso de Wiener de la palabra "cibernético" está en línea con la definición griega e implica la interfaz y la interacción de la biología y la mecánica. El campo de la cibernética, que fue establecido por Wiener, tenía fuertes defensores en toda la academia y el gobierno; sin embargo, el momento de este movimiento que buscaba integrar al hombre y la máquina no fue igualado por la tecnología entonces disponible y, finalmente, el campo cayó en desgracia. A pesar de ello, la cibernética fue recogida por escritores de ciencia ficción en la década de 1980,[19] como se advierte en los siguientes ejemplos.

En 1983, el presidente Reagan vio el éxito de *WarGames*. Es una película de ciencia ficción de la Guerra Fría acerca de un adolescente David Lightman, que hackea una supercomputadora del Comando de Defensa Aeroespacial de América del Norte, WOPR (Plan de Respuesta de Operaciones de Guerra), y presiona a los Estados Unidos al borde de la guerra. El Armagedón nuclear es frustrado cuando Lightman convence a la computadora a jugar tic-tac-toe. La computadora, aprovecha la inteligencia artificial, aprende que no hay un resultado óptimo entre dos jugadores experimentados y que todas las posibles iniciaciones de conflicto resultan en una destrucción mutuamente asegurada. WOPR entonces desactiva las llamadas del lanzamiento nuclear. La película tuvo un profundo impacto en el presidente, quien, en una reunión con el presidente de la Junta de jefes del personal, cuestionó la verosimilitud de este escenario. El presidente de la Junta no tenía una respuesta inmediata y dijo que lo investigaría. Una semana después en

[19] VAN PUYVELDE, Damien, y F. BRANTLY, Aaron, *CYBERSECURITY Politics, Governance and Conflict in Cyberspace,* United Kingdom, Polity Press, 2019, p. 25.

una reunión de seguimiento, explicó al presidente que no solamente era plausible la trama de la película de ciencia-ficción, sino que la realidad era mucho peor que la ficción.[20]

Este banal evento en la historia y desarrollo del ciberespacio activó un diálogo importante entre la comunidad política en los más altos niveles y la comunidad técnica, acerca de las implicaciones de un mundo conectado en crecimiento. Las discusiones de las posibles ramificaciones de ciberseguridad instigado por el presidente Reagan condujo a una conversación gubernamental extensa dentro de los Estados Unidos culminando en una Decisión Directiva de Seguridad Nacional (NSDD-145) sobre "Política Nacional en Telecomunicaciones y Sistemas de Seguridad de Información Automatizada". La misma conversación que el presidente Reagan comenzó continúa actualmente en un medio ambiente que ha ido de muy por debajo de un millón de usuarios conectados en los principios de 1980, la mayoría de ellos americanos, a más de 4 billones de usuarios en todo el mundo en 2018.[21]

El otro ejemplo es la obra de ficción de William Gibson, de la que se derivó por primera vez el término "ciberespacio", quien en 1984 escribió *Neuromancer*, en la que exploró las interacciones de los individuos dentro de una red global, integralmente con Inteligencia Artificial (IA), hackers y más. A pesar de la naturaleza distópica de la novela, el libro también describe elocuentemente la interconexión de los seres humanos y las máquinas, y califica esta interacción como "ciberespacio". Gibson define el ciberespacio en términos generales como una "alucinación consensuada", es decir, un entorno virtual en el que los humanos se involucran entre sí y las máquinas de forma interactiva; refiriéndose a su capacidad para alterar la realidad percibida de aquellos que se involucran entre sí a través de ella en salas de chat o entornos virtuales como *Second Life.*[22]

En el ciberespacio hay interacciones de individuos, grupos y estados. Las personas interactúan con diferentes dispositivos, cada uno conectado a Internet, formando una red masiva de redes que se ha conocido ampliamente como

[20] *Ibidem,* p. 24.
[21] *Ibidem,* pp. 24 y 25.
[22] *Ibidem,* p. 2.

ciberespacio. Casi todos los aspectos de nuestra vida cotidiana son tocados por chips de computadoras para administrar y gestionar bienes y servicios. El ciberespacio es un entorno (ambiente) único y a menudo desconcertante, al que el Departamento de Defensa de los Estados Unidos se refiere como un dominio de operaciones a la par con los otros dominios de combate de la tierra, el mar, el aire y el espacio. El ciberespacio, a diferencia de sus dominios homólogos, es totalmente hecho por el hombre y depende de las estructuras y organizaciones físicas, lógicas y humanas para operar. Algunos estudiosos incluso se refieren al ciberespacio como un sustrato que forma la base de gran parte de la vida moderna y permea los sectores políticos, sociales, económicos, técnicos y ambientales.[23]

Hoy en día, el ciberespacio es un entorno socio-técnico-económico complejo adoptado por 3 billones de individuos, y millones de grupos y comunidades. Todos estos actores se benefician de las oportunidades, facilitadas por el ciberespacio, de compartir recursos e información. Sin embargo, las redes digitales albergan un número cada vez mayor de amenazas cibernéticas, que pueden interrumpir las actividades humanas, en el mundo digital y físico. El ciberespacio es ahora una cuestión de seguridad global que trasciende las fronteras nacionales, sociales y culturales. Como resultado, la ciberseguridad ha comenzado a emerger como un tema importante en el campo de las Relaciones Internacionales, donde los investigadores y profesionales están empezando a considerar la naturaleza de las amenazas cibernéticas y los marcos más adecuados para mitigarlas.[24] El prefijo *cyber* se ha universalizado, ya que se utiliza desde el *cybercrime* hasta *cyberwar.*

B) Definiciones del ciberespacio. De las muchas definiciones del ciberespacio destacaremos dos. En 2009, en un volumen seminal sobre el ciberpoder, Daniel Kuehl, profesor de la Universidad de Defensa Nacional de los Estados Unidos, definió el ciberespacio como *un dominio operativo enmarcado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de sistemas de información interconectados e internet y sus infraestructuras asociadas*. Esta definición la

[23] *Ibidem,* pp. 1 y 2.
[24] *Ibidem,* p. 7.

analizan Puyvelde y Brantly en los términos siguientes: la definición está llena de términos y conceptos que comienzan a delinear las fronteras de lo que el Departamento de Defensa de los Estados Unidos se refiere como un dominio.[25]

Afirman que Kuehl introduce el concepto de electrónica, una clase de dispositivos físicos que dependen del uso de energía eléctrica para operar. Los dispositivos electrónicos pueden incluir tostadoras, circuitos, teléfonos, computadoras o cualquier otra cosa que requiera electricidad para funcionar. En segundo lugar, identifica el uso del espectro electromagnético, un rango de frecuencias y radiación, longitudes de onda y energías fotónicas. El espectro electromagnético incluye todo, desde Wifi y radio recibidos en un estéreo de automóvil hasta controles remotos infrarrojos para televisores, y mucho más. En tercer lugar, da a entender que el ciberespacio no es el uso de la electrónica ni del espectro electromagnético de forma aislada, sino su capacidad de trabajar en tándem para crear, almacenar, modificar, intercambiar y explotar información. En cuarto lugar, no son simplemente los atributos de la información, la creación, el almacenamiento, la modificación y el intercambio dentro de un único sistema, sino la capacidad de transmitir información a través de sistemas conectados y sus infraestructuras asociadas lo que constituye el ciberespacio. Advierte que la definición de ciberespacio de Kuehl está muy lejos de la alucinación de William Gibson. Hace hincapié en la naturaleza física e informativa del ciberespacio, y no aborda el impacto o el valor de la información que circula en este espacio.[26]

La segunda definición está contenida en la Publicación Conjunta 3-12 del Departamento de Defensa de los Estados Unidos de América, que proporciona un marco estructural simplificado y define el ciberespacio de la siguiente manera:

> El ciberespacio consiste en muchas redes diferentes y a menudo superpuestas, así como los nodos (cualquier dispositivo o ubicación lógica con una dirección de protocolo de Internet u otro identificador análogo) en esas redes, y los datos del sistema (como las tablas de enrutamiento) que los soportan. El ciberespacio se puede describir en términos de tres capas: red física, red lógica y ciber-persona. La capa de red física del ciberespacio está compuesta por el

[25] *Ibidem,* p. 26
[26] *Ibidem,* pp. 26 y 27.

componente geográfico y los componentes de red física. Es el medio por donde viajan los datos. La capa de red lógica consiste en aquellos elementos de la red que están relacionados entre sí de una manera que es un abstraído de la red física, es decir, la forma o relación no están vinculados a un individuo, ruta específica o nodo. Un ejemplo sencillo es cualquier sitio web hospedado en servidores en varias ubicaciones físicas donde se puede tener acceso a todo el contenido a través de un único localizador uniforme de recursos. La capa de ciber-persona representa todavía un muy alto nivel de abstracción de la red lógica en el ciberespacio; usa las reglas que aplican en la capa de red lógica para desarrollar una representación digital de un individuo o identidad de la entidad en el ciberespacio. La capa de ciber-persona consiste en las personas realmente en la red.[27]

C) Declaración de independencia del ciberespaci. En 1996, John Perry Barlow, poeta, ensayista y ciber-libertario estadounidense, escribió la Declaración de independencia del ciberespacio, de la que se transcribe el siguiente extracto: *Gobiernos del mundo industrial, ustedes gigantes cansados de carne y acero, yo vengo del ciberespacio, el nuevo hogar de la mente. En nombre del futuro, les pido al pasado que nos dejen en paz. Usted no es bienvenido entre nosotros. Ustedes no tienen soberanía donde nos reunimos*. En opinión de Puyvelde y Brantly la declaración de Barlow no tiene en cuenta la variedad de cuestiones que han surgido que hacen que la ausencia de soberanía en el ciberespacio sea poco práctica y potencialmente perjudicial para los mismos ideales que su declaración trató de defender. Al escribir sobre el desarrollo y el estado actual de la gobernanza de Internet, la académica Laura DeNardis afirma provocativamente que hay una guerra global por la gobernanza de Internet en curso. Dejando de lado la hipérbole, el conflicto sobre la gobernanza de Internet tiene lugar en múltiples lugares, entre y dentro de las naciones.[28]

D) La gobernanza de internet Desde el punto de vista del usuario de internet, las cuestiones de gobernanza pueden parecer triviales. Sin embargo, los problemas en disputa dentro de Internet no son triviales. Internet, ahora a menudo vista

[27] *Ibidem,* pp. 26 y 27.
[28] *Ibidem,* pp. 46 y 47.

ampliamente como ciberespacio, facilita las acciones sociales, políticas y económicas a nivel mundial. Cuestiones como el control de los dominios genéricos de nivel superior (TLDs) que van desde .com y .org hasta .cn y .ru, y la distribución y asignación de direcciones IP a nivel mundial, son algunos de los desafíos a los que se enfrentan los gobiernos de todo el mundo. A los países se les da el control sobre su TLD, la parte nation de las URL utilizadas para acceder y localizar casi todo en Internet. Pero con la expansión de los TLD a nuevas áreas como .Amazon, .Patagonia, .wine y otros indecibles, ¿quién debería ser capaz de controlar los sitios que surgen de su uso? ¿Deberían los países donde fluye el río Amazonas o la Corporación estadounidense Amazon.com tener el control de un dominio determinado? ¿Cómo deben distribuirse las direcciones IP, los números de ruta fundamentales que hacen funcionar Internet?[29]

La apropiación indebida de estas direcciones o el uso indebido de direcciones IP y nombres de dominio por parte de una nación pueden tener ramificaciones globales. En 2008, en un intento de impedir que los paquistaníes accedieran al sitio para compartir videos *Youtube*, que presentaba videos anti islámicos, se ordenó a un ISP paquistaní que censurara el sitio. El ISP respondió modificando el Protocolo de puerta de enlace fronteriza (BGP) para *YouTube* a Pakistán. El proveedor no pudo lidiar con la cantidad de tráfico que recibió como resultado de este secuestro y muchos usuarios de todo el mundo no pudieron acceder a *YouTube* durante un par de horas. El error de YouTube de Pakistán no es un incidente aislado, sino la punta de un próximo cambio en las leyes nacionales que tienen ramificaciones globales. Las leyes nacionales y regionales, como el *European General Data Protection Regulation* (GPPR), que entró en vigor en mayo de 2018, cambiaron la forma en que las empresas pueden utilizar Internet dentro de jurisdicciones soberanas y afectan a la capacidad del usuario para navegar por la web. El GDPR se centra en los derechos de datos de los ciudadanos europeos, pero sus implicaciones son técnicas, políticas y financieras, y visibles a nivel global debido a la conectividad inherente del ciberespacio y su naturaleza transnacional. Leyes como el GDPR desafían los mecanismos técnicos que fomentan la transmisión

[29] *Ibidem,* p. 47.

eficiente de datos y crean costos para los proveedores de servicios en línea que dependen de servidores de almacenamiento de datos ubicados en naciones que se adhieren al GDPR.[30]

La gobernanza de Internet es expansiva e incluye una variedad de preguntas desafiantes sobre la utilización de la información, la libertad de información y muchas más. Algunas de las preguntas son ¿Las naciones más pequeñas deberían tener que pagar precios más altos de Internet porque no pueden ofrecer acuerdos de *peering* simétrico (transferencia de datos) con grandes proveedores de Internet? ¿Cómo debe administrarse, regularse y almacenarse el tránsito de datos entre las naciones? ¿Debería el tráfico en Internet ser neutral, o es aceptable privilegiar un poco de tráfico a expensas de otros? ¿Se debería exigir a los ISP que monitoreen el tráfico de Internet en busca de comportamientos ilegales o inmorales o incluso las actividades de periodistas o activistas de derechos humanos? Los estados han mantenido durante mucho tiempo la jurisdicción sobre su territorio y la ciudadanía. El derecho internacional reconoce dos formas de soberanía: de jure (control jurídico) y de facto (control físico), sobre lo que se produce dentro de sus fronteras. Internet desafía los derechos soberanos de los estados. Las naciones han buscado aumentos en sus derechos soberanos a través de Internet, por medio de una variedad de programas. La Unión Internacional de Telecomunicaciones (UIT), un organismo especializado de las Naciones Unidas, ha sido uno de los principales vehículos para que los estados presionen por su mayor papel en la administración de Internet.[31]

E) Multilateralismo y multipartes interesadas sobre la gobernanza en el ciberespacio. El enfoque que los estados adoptan hacia la gobernanza en el ciberespacio es a menudo una función de su régimen interno y su posición dentro de la política internacional. Estados como China, Rusia e Irán buscan soluciones multilaterales para los desafíos de la gobernanza, mientras los Estados Unidos y sus aliados buscan soluciones multipartes interesadas (*multistakeholder*). Esta divergencia de enfoque establece el escenario para el conflicto y enfrenta a

[30] *Idem.*
[31] *Ibidem,* p. 48.

organizaciones tales como la UIT (Unión Internacional de Telecomunicaciones de la ONU) contra la ICANN (Corporación de Internet para nombres y números asignados). Mientras el balance sigue favoreciendo en gran medida a las instituciones de multipartes interesadas, esto no podría ser un estatus permanente de asuntos. Algunos estudiosos sostienen que el *statu quo* actual de la gobernanza de internet podría conducir a una fragmentación de internet entre los estados que favorecen el control a través de instituciones multilaterales y los que favorecen a las multipartes interesadas.[32]

F) Principales entidades de gobernanza de internet:

Entidad	Rol	Funciones
Certificate Authority (**CA**) Autoridad de Certificación	Emite certificados digitales y certifica la propiedad de una clave pública por parte del sujeto nombrado de un certificado.	Operaciones, servicios.
Internet Architecture Board (**IAB**) Tablero de Arquitectura de Internet	En ultramar (el extranjero) el desarrollo técnico y de ingeniería del IETF y del IRTF	asesoría, compromiso de la comunidad, políticas, normas, investigación.
Internet Corporation for Assigned Names and Numbers (**ICANN**) Corporación de Internet Asignadora de Nombres y Números.	Coordina los sistemas de internet de identificadores únicos, incluyendo direcciones IP, registros de protocolos y parámetros y espacio TLD.	Compromiso de la comunidad, operaciones, política y servicios.
Internet Engineering Task Force **(IETF)** Fuerza de Tarea de Ingeniería de Internet.	Desarrolla y promueve normas para los protocolos de internet.	Compromiso de la comunidad, política y normas.
Internet Exchange Points **(IXPs)** Puntos de intercambio de Internet	Proporciona la infraestructura física a través de la cual los ISPs, y redes de entrega de contenido (CDNs) intercambian tráfico de internet.	Operaciones, servicios.

[32] *Ibidem,* p. 51.

Internet Governance Forum **(IGF)** Foro de Gobernanza de Internet	Un Foro abierto de multi partes interesadas para el debate sobre cuestiones de gobernanza de internet	Asesoría, compromiso de la comunidad, política.
Internet Network Operators´Group Grupo de Operadores de Redes de Internet.	Discute e influye en asuntos relacionados con las operaciones y la regulación de Internet dentro de los externos informales compuestos por ISPs, IXPs y otras partes interesadas.	Asesoría, operaciones, servicios.
Internet Research Task Force (**IRTF**) Fuerza de Tarea de Investigación de Internet	Promueve la investigación sobre la evolución de la internet, crea grupos de investigación enfocados a largo plazo que trabajan en temas relacionados con protocolos, aplicaciones, arquitectura y tecnología.	Investigación.
Internet Service Providers (**ISPs**) Proveedores de Servicio de Internet.	Una organización, pública o privada, que proporciona servicios para participar, acceder o usar Internet.	Operaciones, servicios.
Internet Society (**ISOC**)	Asegura el desarrollo abierto, la evolución y el uso de internet para el beneficio de todas las personas.	Compromiso de la comunidad, educación, política y servicios.
Regional Internet Registries (**RIRs**)	Cinco registros regionales de Internet gestionan la asignación y el registro de recursos numéricos de Internet dentro de las regiones geográficas	Operaciones, política, servicios.
World Wide Web Consortium (**W3C**) Consorcio	Crea normas para la red mundial que habilita una plataforma de red abierta	Normas.[33]

[33] *Ibidem,* p. 52.

Consorcio de la Red Mundial		

G) El derecho internacional público contemporáneo y el ciberespacio. Los profesores ingleses Chris Reed y Andrew Murray mencionan que es axiomático más o menos en el pensamiento jurisprudencial que las naciones-estados tienen autoridad ilimitada para hacer leyes, sujeto sólo a las restricciones que esos estados aceptan voluntariamente mediante la firma de acuerdos con otros estados. Las únicas dudas surgen con respecto a los estados fallidos o a los estados en transición entre regímenes gobernantes. El ciberespacio nos obliga a desafiar ese axioma. El desafío surge porque múltiples estados afirman que sus leyes son aplicables a las actividades de los usuarios del ciberespacio. Tales afirmaciones no parecen controvertidas si el usuario del ciberespacio es residente o un ciudadano del estado en cuestión. En ese caso, el estado tendrá el poder final para hacer cumplir su reclamo de autoridad contra la persona del usuario del ciberespacio, o contra la propiedad ubicada en el estado. Además, al estar presente en el estado, el usuario del ciberespacio se ha sometido a la autoridad del estado. La autoridad de las leyes de un estado en esta situación es en gran parte indiscutible. Pero es menos obvio que una reclamación de autoridad esté bien fundada si el usuario del ciberespacio es un residente en el extranjero, cuya única conexión con el territorio nacional del estado que reclama resulta de las actividades del usuario en el ciberespacio. Es inevitable, particularmente si varios estados reclaman autoridad sobre la misma actividad, que los usuarios del ciberespacio pregunten cuál de esas leyes, si las hay, debe ser obedecida; o para decirlo en términos jurisprudenciales, si esos legisladores tienen autoridad para reclamar obediencia a sus leyes.[34]

Dichos profesores señalan que los estados afirman jurisdicción sobre sus nacionales en todo el mundo, ninguno más que en la regulación de las actividades de las empresas multinacionales registradas localmente. Por ejemplo, en 1979 el presidente Carter congeló los activos del estado iraní mantenidos en cuentas en sucursales londinenses de bancos estadounidenses. Además, los estados

[34] REED, Chris, y MURRAY, Andrew, *Rethinking the Jurisprudence of Cyberspace,* U.S.A., Edward Elgar Publishing Limited, 2020, p. 2.

reclaman autoridad sobre actividades fuera de su jurisdicción física pero que, sin embargo, tienen efectos, del tipo que pretende la ley, dentro del territorio estatal. Por ejemplo, los acuerdos anticompetitivos entre personas del estado, pero que restringen negativamente la competencia en los estados, la contaminación que cruza las fronteras nacionales, etc. Del tipo de actividad quizás la más conocida es la doctrina del daño en agravios informativos. Esto permite a un individuo difamado dentro de cualquier jurisdicción en la que se produce el daño (daño) para llevar una reclamación a los tribunales locales. Una consecuencia ha sido el aumento del turismo por difamación ante el Tribunal Superior de Inglaterra y Gales.[35]

Por ejemplo, un editor estadounidense cuyo boletín está disponible en línea puede ser demandado en Australia por difamación, incluso si el foco de la publicación era el mercado local, estadounidense (*Gutnick v Dow Jones* [2001] VSC 305, [2002] HCA 56 (Australia), o un servicio de subastas en línea con sede en los Estados Unidos puede ser acusado de delitos en virtud de las leyes antinazis de Francia, como en el caso *Ligue Contre Le Racisme et Lántisémitisme et Union des Étudiants Juifs de France v. Yahoo! Inc et Société Yahoo! France,* ante el Tribunal de *Grande Instance* Paris, *Interim Court Order* No. 00/05308, 00/05309, 22 May 2000.[36]

Es de aplicación general la prueba de efectos, dentro de la jurisdicción de un estado en los que se produjo, independientemente del lugar en donde la conducta los originó, por lo que cualquier ley, incluso anterior al ciberespacio, podría ser exigida por un tribunal nacional para aplicarla a un usuario del ciberespacio. Desde este punto de vista será siempre legítimo que los órganos jurisdiccionales de ese sistema apliquen extraterritorialmente sus leyes. Sin embargo, el rápido aumento de las actividades en el ciberespacio ha demostrado que esta imagen es demasiado simplista, ya que a menudo no tienen autoridad práctica y legítima para un usuario, porque no se lo ha conferido la comunidad legitimadora, el público votante. Cada estado tiene una comunidad extendida en el ciberespacio, y sus leyes tienen autoridad sobre los miembros de esa comunidad que se deriva de sus interacciones

[35] *Ibidem,* p. 3.
[36] *Idem.*

con el estado. Para reclamar autoridad sobre los actores del ciberespacio cambia la naturaleza del problema. El número de personas contra las que se hace el reclamo de autoridad no es simplemente un número mayor, sino tantos órdenes de magnitud mayor que a menudo superará en número a la comunidad en el territorio físico establecido.[37]

La naturaleza a-territorial de las comunicaciones en línea significa que cualquier comunicación a través de un sitio *web* de acceso público es visible para cualquier persona que tenga acceso a Internet, por lo que todas estas comunicaciones son visibles en Francia. Así, la decisión del tribunal de este país pretendía aplicar la legislación francesa a todos los usuarios de Internet. En el año 2000, el número de usuarios se estimaba en unos 400 millones, en comparación con los 60 millones de habitantes de Francia. En 2017 había alrededor de 3,6 billones de usuarios de Internet, mientras que la población de Francia se mantuvo por debajo de los 65 millones. Este reclamo de la autoridad del derecho francés sobre todos los actores del ciberespacio, crea un problema en la identificación de la comunidad legitimadora de ese derecho. Parece absurdo si la ley francesa sólo tiene autoridad legítima si la mayoría (no francesa) de los usuarios del ciberespacio aceptan que la tiene. Pero la alternativa, de que solo los ciudadanos franceses determinen la autoridad de la ley en el ciberespacio con exclusión del grupo numéricamente mayor de actores del ciberespacio, parece igualmente absurda.[38]

Los gobiernos han desarrollado un sólido cuerpo de derecho internacional o se han centrado en el establecimiento de normas (estándares de comportamiento) para gestionar las interacciones entre los estados. Sin embargo, los estados administran sus interacciones dentro de este dominio en evolución que es el ciberespacio. El alcance del derecho internacional es extremadamente amplio y va mucho más allá de los debates sobre la gestión técnica del ciberespacio. Cuestiones tales como el espionaje, extradición criminal y las leyes de conflicto armado son más a menudo tratadas entre naciones en una manera multilateral.[39]

---

[37] *Ibidem,* pp. 4, 25 y 60.
[38] *Ibidem,* p. 61.
[39] VAN PUYVELDE, Damien, y F. BRANTLY, Aaron, *Op. Cit.,* p. 54.

Los profesores Puyvelde y Brantly consideran que el establecimiento de la *Convention on Cybercrime* en 2001, y su subsecuente ratificación por cincuenta y siete naciones, sirve como un buen punto de partida para los debates sobre el derecho internacional y el ciberespacio. Refieren que a finales de la década de 1990, a medida que Internet se expandía, también lo hacían los delitos digitales. La violación de sistemas digitales y el impacto de las actividades criminales en la confidencialidad, integridad y disponibilidad de sistemas informáticos firmemente surgieron dentro de la conciencia internacional. Docenas de naciones reunidas en Budapest comenzaron a idear una estrategia multilateral para abordar el cibercrimen. La Convención de Budapest sobre el cibercrimen trató de armonizar las leyes nacionales dentro de cada uno de los países signatarios, mejorar las técnicas de investigación y facilitar la comunicación y la cooperación. La convención sirve como un ejemplo de uno de los primeros tratados importantes entre las naciones para abordar cuestiones surgidas en el ciberespacio.[40]

La Convención sobre el cibercrimen fue un fuerte primer paso hacia el desarrollo del consenso internacional alrededor de cuestiones que impactan a todos los estados. A principios de 2004 y con una convocatoria periódica hasta 2017, un Grupo de Expertos Gubernamentales de las Naciones Unidas se ha reunido para debatir y desarrollar normas y leyes relacionadas con el ciberespacio. El grupo publica informes periódicos a la Asamblea General de las Naciones Unidas que proporcionan información actualizada sobre los debates y los avances sobre el terreno. Las discusiones de este grupo e informes sirven como el fundamento para el consenso sobre qué leyes o normas potenciales podrían ser establecidas en el futuro. Al trabajar en grupos de discusión multilaterales, las naciones son capaces de mejorar su comprensión de cómo perciben los diversos cambios y acciones en el ciberespacio. Tras los ciberataques coordinados de 2007 contra Estonia, la OTAN estableció el Centro Cooperativo de Excelencia de Ciberdefensa (CCD COE) en Tallin en 2008. Este Centro sirvió como ubicación central para que los miembros de la OTAN trabajaran juntos y abordaran los problemas que surgían en y a través del ciberespacio. Dos de los resultados más impactantes de este esfuerzo han sido

[40] *Ibidem,* p. 54.

los Manuales de Tallin publicados en 2013 y 2017 y producidos a través de un proceso deliberativo entre abogados internacionalistas y académicos jurídicos. Estos manuales interpretan sistemáticamente y aplican el derecho internacional a las acciones que ocurren en y a través del ciberespacio.[41]

Los manuales no son legalmente vinculantes y no establecen formalmente las normas, pero son la colección más sólida de análisis legales sobre los temas relacionados con el conflicto cibernético entre los estados hasta la fecha. Las interacciones internacionales en el ciberespacio en los niveles jurídico y normativo están todavía en flujo (cambiando). A pesar de la falta de reglas concretas del camino para los estados dentro del ciberespacio, las conductas normativas generales y precedentes legales están siendo trabajadas hacia allá. Para países como los Estados Unidos y muchos de sus aliados, las leyes de guerra y muchas de las normas de la conducta internacional ampliamente aplican al ciberespacio.[42]

Es importante mencionar que la *Convention on Cybercrime* es un tratado del Consejo de Europa y referido con el número 185, que lo firmaron y ratificaron los miembros de dicho Consejo, excepto la Federación Rusa e Irlanda que lo firmó, pero no lo ratificó. Sin embargo, el mismo tratado permitió que estados no miembros del mencionado Consejo lo firmaran y ratificaran, como es el caso de países del continente americano, entre los que no se encuentra México.[43] Por nuestra parte, consideramos que la citada Convención y legislaciones nacionales que abordan el cibercrimen o ciberdelincuencia implican la existencia de un desarrollo de ciber-capacidades delictivas que van más allá de ese tratado y leyes. Aseveración que tiene sustento en lo que los profesores Puyvelde y Brantly mencionan acerca de que la *Russian Business Network* y otra gran cantidad de organizaciones criminales que van desde los cárteles mexicanos de la droga hasta los hackers criminales individuales generan nuevas hazañas y utilizan el malware existente a través de bibliotecas disponibles como *Metasploit*. Afirman dichos profesores que los criminales, hacktivistas y terroristas en combinación superan con creces a los

[41] *Ibidem,* pp. 54 y 55.
[42] *Ibidem,* p. 55.
[43] COUNCIL OF EUROPE, *Convention on Cybercrime* (31 de agosto de 2021), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?module=signatures-by-treaty&treatynum=185

estados en volumen y variedad de ataques diarios y robos que ocurren en y a través del ciberespacio. Los actores criminales constituyen la amenaza más grande y sustancial para la ciberseguridad.[44]

Mencionan tales profesores que el Centro de Quejas de Delitos en Internet de la Oficina Federal de Investigación, en su informe de 2017 sobre delitos en Internet, documentó $ 1.4 mil millones en pérdidas basadas en aproximadamente 300,000 informes en el transcurso de un año. La firma de seguridad en Internet *McAfee* estima que el total de delitos cibernéticos globales costó a empresas, individuos y gobiernos entre 445 y 608 mil millones de dólares en 2017. Esto equivale a una pérdida del PIB mundial de entre 0,59 y 0,80 por ciento. El impacto de la ciberdelincuencia varía ampliamente según el país, América del Norte, Europa y Asia central, y Asia oriental y el Pacífico, sufrieron las mayores pérdidas financieras.[45] También explican los delitos *Cyber trespassing*; *Cyber deception/fraud/extortion*; *Cyber theft; Cyber violence* (siendo una de sus formas el *Cyber bullyng y Cyber stalking*); *illicit commerce* (en mercados ilícitos alojados en servicios *Dark Web*, como 12P y Tor, que proporcionan a los clientes acceso a drogas, armas, tarjetas de crédito y débito, herramientas de piratería, pornografía o una gama de productos ilegales) y *a variety of sexual crimes* (transmisión de imágenes de pornografía infantil, violación, mutilación, bestialidad, esclavitud y una variedad de otros crímenes asociados facilitados por el ciberespacio).[46]

H) El nomos del ciberespacio. Con lo anterior, estamos en condiciones de intentar esbozar lo que podría ser el *Nomos* del ciberespacio. Partiendo del carácter polisémico y de su derivación del verbo griego *nemein*, el *Nomos* del ciberespacio significa un espacio virtual sin fronteras y a-territorial, creado por el hombre, que abarca el planeta tierra, con libre acceso para los usuarios del mismo, que comprenden personas físicas (estudiantes, periodistas, académicos, etc.) y personas jurídicas (estados, corporaciones empresariales, financieras. etc.), las cuales están en constante tensión por la disputa de aquellos por ocupar, poseer, distribuirse y usar una ciberfranja del espacio virtual que les permita interactuar con

[44] VAN PUYVELDE, Damien, y F. BRANTLY, Aaron, *Op. Cit.,* pp. 64, 65 y 105.
[45] *Ibidem,* p. 106.
[46] *Ibidem,* pp. 107-112.

privacidad y seguridad, en tanto que estos últimos pretenden también ocupar, poseer, dividirse, usar y explotar completamente el espacio virtual. Es un espacio artificial abierto a la conquista para su apropiación y dominio, con cierta gobernanza por sus operadores y un incipiente sistema de regulación normativa nacional e internacional, en el que se replica en un segundo nivel la tensión, pero entre el derecho nacional y el derecho internacional; inclusive, en un tercer nivel la tensión se replica entre estados y operadores y usuarios; es decir, entre el multilateralismo (que pretende crear un instrumento internacional para regular el ciberespacio) y el multistakeholder (actores privados y públicos que pretenden regular el ciberespacio con cibernormas).

III

INTERNET Y LA *DARK WEB*

La internet y la *Dark Web* no son lo mismo, pero esta última no existiría sin la infraestructura de aquella. Uno no puede entender cómo la *Dark Web* trabaja sin entender (sobre un nivel básico) como la internet trabaja; y no se puede entender como las redes individuales de la *Dark Web* trabajan (Tor, Freenet, 12P) sin primero entender cómo las redes *Dark Web* trabajan en general, lo que implica comenzar la exposición desde los fundamentos de la ciencia informática, teoría de la información y comunicación e ingeniería eléctrica, hasta las redes de la *Dark Web* disponibles actualmente.[47]

1. *Algunos antecedentes de la ciencia informática* Las tres figuras consideradas importantes en la ciencia informática y redes de la información, como la *Dark Web*, para el desarrollo eventual de la internet (y consecuentemente para la *Dark Web*) son Alan Turing, Vannevar Bush, y Claude Shannon, entre otras más.

A) Máquina de computación. Alan Turing, considerado el padre de la ciencia informática, describió a mediados de 1936 a una máquina de computación como una simple máquina que puede ser usada para calcular cualquier secuencia computable y tal máquina sería capaz de memorizar y reconocer patrones de datos. Después diseñó una máquina multiplicadora lógica booleana que jugó un papel

[47] BECKSTROM, Matthew & LUND, Brady, *Casting Light on the Dark Web A Guide for Safe Exploration,* United Kingdom, Rowman & Littlefield, 2019, p. 11.

crucial en los esfuerzos militares en la Segunda Guerra Mundial. Aunque las máquinas de Turing no eran prácticas en comparación con las capacidades de memoria de las computadoras modernas que utilizan memoria de acceso aleatorio para el almacenamiento de datos (su memoria secuencial es el meta-equivalente de la cinta de casete frente al formato MP3 para el almacenamiento de audio), las matemáticas de Turing delineadas en *On Computable Numbers, with an Application to the Entscheidungsproblem* y su disertación, *Systems of Logic Based on Ordinals*, son la base teórica del campo de la ciencia informática o informática.[48]

B) Almacenamiento de datos electrónicos. Vannevar Busch, inspiró a los profesionales de la información con su trabajo *As We May Think* en 1945, relativo al almacenamiento de datos electrónicos, en los campos bibliotecario y de la ciencia informática, ya que describió el sistema *Memex* que predijo el sistema de información con el que se trabaja hoy en día: *Integrated Library System* (ILS). Estos sistemas tienen el objetivo de capturar grandes franjas de conocimiento humano y catalogarlo para un acceso conveniente. A medida que la tecnología mejora, más recursos están vinculados al catálogo de acceso, por lo que los usuarios tienen la funcionalidad de guardar preferencias y notas en sus teléfonos inteligentes. Sus ideas inspiraron el diseño de bibliotecas digitales, agregadores y motores de búsqueda.[49]

C) Canal de comunicación. Claude Shannon, transformó el estudio de la información con su *Mathematical Theory of Communication* en 1948, aunque algo simple, pero se replicó en las ciencias duras y sociales. Introdujo un modelo matemático del ruido en un canal de comunicación. Como en el juego del teléfono, el error y la mala interpretación pueden conducir a una distorsión completa de un mensaje, los mismos problemas son relevantes con los teléfonos reales y demás redes que implican que un mensaje se pase a través de un medio de comunicación verbal de cara a cara a conexiones de internet. Al proporcionar los conceptos de

[48] *Ibidem,* p. 12.
[49] *Idem.*

entropía de la información y el *bit*, Shannon allanó el camino para toda la tecnología de comunicación que disfrutamos.[50]

2. *Historia básica de la internet.* El Departamento de Defensa del gobierno de los Estados Unidos desarrolló e implementó la Red de Agencias de Proyectos de Investigación Avanzada, conocida con el acrónimo ARPANET, cuyo concepto fue propuesto en 1960 por científicos informáticos para crear un nuevo tipo de red informática que permitiera comunicación más eficiente. Una de las ideas fue la conmutación de paquetes en lugar de circuitos que eran utilizados desde la invención del teléfono, que al marcar una serie de números se está creando un circuito. La conmutación de paquetes es más eficaz porque puede usar la misma conexión física para múltiples comunicaciones simultáneas. Utiliza una serie de paquetes de datos, o pequeños paquetes de información que son enviados entre dispositivos de la red. Se enrutan alrededor de la red utilizando diferentes tipos de direcciones. En la parte superior de cada paquete hay un poco de información sobre quién está enviando ese paquete y a quién se está enviando, como sobres digitales. En el exterior hay una dirección de retorno que dice quién está enviando la carta, y también una dirección de destinatario que dice a dónde se dirige. En la red, los paquetes son enviados a varios dispositivos de enrutamiento que utilizan la dirección del destinatario para enviarla a otro dispositivo de la red hasta que finalmente se entregue al destinatario correcto.[51]

El Departamento de Defensa se vio forzado a crear sus propias conexiones entre las oficinas que estaban usando ARPANET; es decir, construir la infraestructura de información (comunicación), la cual no solamente fue para proteger las comunicaciones del Departamento de Defensa en el caso de una guerra nuclear, sino para que las comunicaciones enrutadas pudieran rápidamente ser re-enrutadas en caso de que una porción de la red se inhabilite. En 1970 ARPANET se expandió de California a la Costa Este, agregándose más sitios y universidades, lo cual no constituyó la internet sino instalaciones del gobierno y de algunas universidades cuya información era accesible y disponible para los

[50] *Ibidem,* p. 13.
[51] *Ibidem,* p. 14.

usuarios. Con el tiempo más usuarios no gubernamentales se conectaron a ARPANET. A mediados de 1980 fue restructurada para mover los nodos militares a su propia red llamada red de Datos de Defensa, con lo que ARPANET se dividió en dos redes: militar y civil, que estaban conectadas, pero con puerta de entrada entre ellas.[52]

En los años de 1980 fueron creadas redes similares a ARPANET, ya que grupos, agencias y gobiernos querían aprovechar esta tecnología, al grado de cientos de redes separadas a través de los Estados Unidos, cada una con un propósito específico. La red que movió la tecnología hacia adelante fue la *National Science Foundation Network* (NSFNET), creada en 1985 para promover red de educación e investigación avanzada, usando un nuevo tipo de protocolo de comunicación llamado TCP/IP (*Transmission Control Protocol/Internet Protocol*) que fue más eficaz en enrutar paquetes alrededor de la red y se convertiría en el principal protocolo de comunicación para la internet. Con la explosión de redes de comunicación en los Estados Unidos surgió la idea de conectarlas, por lo que a medida que se conectaban necesitaban estandarizar sus protocolos de comunicación. La NSFNET creó otra tecnología básica de internet: *backbone*, cuya idea era crear un concentrador central que conectara todas las diferentes redes. Con esta red troncal se crearon vínculos internacionales con Canadá, México y diversos países de Europa. Hasta ese punto de avance, esta internet solamente eran redes educativas, científicas y gubernamentales, no la internet que conocemos ahora, pues permanecían en sus propias redes locales y ocasionalmente enviaban información a usuarios de otras redes utilizando las conexiones entre ellos. Había poca preocupación por la privacidad.[53]

En 1990 ARPANET fue dada de baja y aparecieron proveedores de servicios comerciales de internet (ISPs), por lo que ahora por vez primera el usuario medio del equipo sin intereses educativos o científicos podría conectarse a la red. Después en 1995 NSFNET también fue dada de baja y el resto del troncal de internet fue conectado, creándose así la internet actual. La gente descubrió los beneficios de

[52] *Idem.*

[53] *Ibidem,* pp. 14 y 15.

comunicación rápida usando correos electrónicos y charlas por internet; los archivos se compartían y comercializaron. Cuando el inglés Tim Berners-Lee creó la *World Wide Web* y los estándares de comunicación que usamos en navegadores de internet como internet *Explorer*, *Chrome* y *Firefox*, la gente pudo navegar y ver todo tipo de material de todo el mundo. En la medida que incrementaba la velocidad y el acceso los usuarios de internet aprendían, se entretenían y compraban. Las entidades comerciales apreciaron que las ventas por internet proporcionaban experiencias más rápidas y eficientes para sus clientes; y las agencias del gobierno comenzaron a publicar información para las comunidades de la internet.[54]

Este progreso fue acompañado con la interrupción de comunicación en la internet con virus, gusanos y malware (software: programa, documentos, discos, películas, cintas, para dañar o tener control parcial de un dispositivo), lo que forzó a los usuarios a protegerse con el software antivirus que emergió, colocándose en las redes firewalls entre ellos mismos y la internet para inspeccionar el tráfico y determinar si es perjudicial o peligroso. Surgió el cibercrimen en la internet para robar o destruir información, por lo que los ataques ya no eran generales sino focalizados, incluso en contra de compañías competidoras, lo que orilló a crear industrias para frenar o bloquear los ataques. Eventualmente, los gobiernos fueron forzados para ayudar a protegerse y al comercio en general, pero también hubo mayor intrusión en la comunicación por internet, ya que los proveedores del servicio de internet comenzaron a monitorear a sus usuarios para mantener la integridad de sus redes de ataques a sus redes. La adopción de la internet a través del mundo vino a ser una red global, aunque algunos países no aceptaron ideas y creencias de otros países por lo que la bloquearon. La internet fue diseñada para estar abierta, pero nos han forzado a estar protegidos para impedir esa apertura y no siempre funciona, pues los virus siguen infectando, los malware engañan a la gente y entidades intentan irrumpir en lugares que no deberían.[55]

Esta internet es llamada *Surface Web* o Internet de superficie, para distinguirla de la *Deep Web* y la *Dark Web o Darknet*. *La Deep Web* existió en los principios de

[54] *Ibidem,* pp. 15 y 16.
[55] *Ibidem,* p. 16.

la internet con los bloqueos de nombre de usuario/contraseña, cuyo mecanismo básico para proteger información fue colocado atrás en un muro de autenticación, o en un muro de pago. Como la red se hizo más grande, más sitios e información fueron ubicados detrás de los muros de autenticación, como los sitios comerciales que comenzaron a poner información en lugares donde no podrían ser alcanzados por motores de búsqueda. El término *Deep Web* lo acuño en 2001 el científico informático Michael K. Bergman en su trabajo que publicó sobre buscar en la internet con el título *The Deep Web: Surfacing Hidden Value*. Bergman estimó que en el año 2000 la *Surface Web* contenía alrededor de un billón de documentos individuales y páginas, mientras que la *Deep Web* alrededor de 550 billones.[56]

La gente estuvo usando la internet para comunicaciones privadas, así como aquellos miembros de la sociedad americana que querían o necesitaban un nivel mayor de protección de aquellos quienes querían silenciarlos. Las corporaciones y gobiernos comenzaron a monitorear y buscar qué estaba haciendo la gente en la internet, y en algunos casos, los bloqueaban. Por ejemplo, en China en el año 2000 el gobierno utilizó el *Golden Shield Project* para controlar el flujo de información con el fin de proteger a los ciudadanos de lo que consideraba inapropiado, con lo que se creó una cultura de censura.[57]

También el gobierno de los Estados Unidos estaba rastreando y grabando lo que la gente hacía en Internet. Antes de internet, la Agencia de Seguridad Nacional estaba en ARPANET y continuó rastreando a los usuarios a través de la red y, finalmente, creó formas de recopilar, almacenar y usar el tráfico en Internet. Después de los ataques en el *World Trade Center* en 2001, el gobierno de los Estados Unidos aprobó nuevas regulaciones que permitieron crear nuevos programas de vigilancia para monitorear el uso de la internet de extranjeros y ciudadanos norteamericanos. La Ley PATRIOT de los Estados Unidos de América fue aprobada por el Congreso en 2001 y para tener un impacto en la internet. Concedieron a las agencias gubernamentales más poder para reunir y almacenar

[56] *Ibidem,* p. 18.
[57] *Ibidem,* p. 19.

más tráfico de internet de lo que podrían antes. Negociaron la privacidad con la promesa de aumentar la seguridad para los ciudadanos americanos.[58]

En 2013 un contratista para la CIA y la NSA llamado Edward Snowden reveló una riqueza de documentos internos de la NSA que expuso las tecnologías que usó la agencia para monitorear internet. Entre ellas fue PRISM, un programa de vigilancia diseñado por la NSA que reúne y almacena tráfico de internet de las compañías de internet de los Estados Unidos como *Google*, *Yahoo*, y *Verizon*. Snowden también liberó detalles de otros gobiernos involucrados en el rastreo y vigilancia en internet. Por ejemplo, *Tempora* es un programa usado por el gobierno británico para reunir, almacenar, y utilizar tráfico de internet. Él también expuso un sistema de pagos gubernamentales para comprar información de proveedores de internet, intentos del gobierno para reclutar informantes de las comunidades en línea, y que el gobierno de los Estados Unidos estaba vigilando otros países: Brasil, Francia, México, Gran Bretaña, China, Alemania y España.[59]

La seguridad comenzó a ser una cuestión en la internet. Algunas veces, la gente, organizaciones, o gobiernos usaron la internet para buscar otros individuos u organizaciones para robar o atacar. Muchos ataques son dirigidos a ciudadanos para ganar acceso a información financiera, o en negocios para ganar acceso a información corporativa. Internet se convirtió en un punto de acceso para la manipulación por motivos políticos como resultado de su ubicuidad en el mundo desarrollado. Los grupos extremistas podrían usarlo para manipular a las personas y unirlas a una causa y los gobiernos podrían distribuir información falsa e influenciar la percepción pública como en las elecciones de 2016 en los Estados Unidos.[60]

3. *La Dark Web.* La internet como plataforma de comunicación que abarca todo el mundo es objeto del deseo de controlarla. Los gobiernos buscaron impedir que sus ciudadanos aprendieran sobre el mundo e impedir que el resto del mundo conociera acerca de ellos. Las compañías buscaron encontrar nuevos flujos de ingresos de la riqueza de la información acerca de la gente en internet. Los individuos buscaron

[58] *Ibidem,* pp. 20 y 21.
[59] *Ibidem,* pp. 21 y 22.
[60] *Ibidem,* p. 22.

robar o interrumpir la comunicación que ocurría. La gente buscó y necesitó maneras para usar la internet que no fuera monitoreada o rastreada. Ellos desearon maneras para explorar y descubrir fuera el temor de filtrar o vigilar. Entrar a la *Dark Web*.[61]

El Laboratorio de Investigación Naval de los Estados Unidos de América, en la mitad de 1990 creó un proyecto al que denominó enrutador *Onion* y más tarde lo redujo al nombre de *Tor*. El nombre *Onion* fue debido a la forma en que la red enruta el tráfico, creando capas de cifrado sobre los paquetes de transmisión de manera similar a la forma en que las cebollas tienen capas. El Laboratorio estaba intentando encontrar una manera para crear comunicaciones protegidas en la internet para actividades gubernamentales de inteligencia. En 1997 la Agencia de Defensa de Investigación Avanzada (DARPA) desarrolló el proyecto Tor para crear el primer lanzamiento en 2002. En 2004 el Laboratorio lanzó el código para el proyecto *Tor* para el público de manera gratis. La Fundación Frontera Electrónica (EFF) continuó fondeando a los creadores del proyecto original, Roger Dingledine y Nick Mathewson. Ellos más tarde fundaron el proyecto *Tor*, una organización de investigación educativa 501 (c) (3) responsable de mantener *Tor*. Inicialmente, el principal partidario financiero del proyecto *Tor* fue el gobierno de los Estados Unidos, al lado de otras muchas otras organizaciones interesadas en crear privacidad en internet.[62]

En la liberación de información de Snowden, reveló los planes de la NSA para exponer usuarios *Tor* e infiltrar sus comunicaciones. La agencia intentó identificar a los usuarios de la red *Tor* y entonces usó un tipo especial de redirección para señalar su comunicación a los servidores de la NSA. Una vez que la NSA estuvo investigando el tráfico, podría infectar una computadora de usuario con una aplicación especial que le quitó lo anónimo de su comunicación. Desde esta revelación, la NSA supuso haber detenido esta infección. *Tor* había crecido desde su comienzo para ser una de las más frecuentemente usadas herramientas de la *Dark Web*. Estudios recientes han calculado que el número de personas que usan *Tor* diariamente es de alrededor de seis millones. Ha reunido una gran cantidad de

[61] *Idem*.
[62] *Ibidem,* pp. 22 y 23.

prensa con riesgos ilegales como *Silk Road*, que ofertó una variedad de productos ilegales para su venta, pero también ha sido promovida como una herramienta privada que es usada por una larga variedad de gente. Snowden mismo es sabedor del uso de la red *Tor* para sus comunicaciones. Por necesidad, una *Dark Web* comenzó a crecer que ofreció una manera de combatir la pérdida de privacidad, falta de anonimato, y pérdida de control. La *Dark Web* había nacido.[63]

Otra plataforma de la *Dark Web* surgió en 1999, cuando un estudiante en la Universidad de Edinburgh llamado Clarke publicó un artículo de graduación titulado *Un Sistema Descentralizado Distribuido de Almacenamiento y Recuperación de Información*. Como resultado de ese artículo, un grupo de investigadores, incluido Clarke, publicó en 2001 un artículo llamado *Freenet* (un Sistema Distribuido de Almacenamiento y Recuperación de Información Anónima). Ellos establecieron cinco objetivos de diseño para Freenet:

- Anonimato para productores y consumidores de información.
- Negación para almacenadores de información
- Resistencia para intentar, por terceras partes, negar acceso para información.
- Eficiente dinámica de almacenamiento y enrutamiento de información.
- Descentralización de todas las funciones de la red.[64]

La tercera plataforma de la *Dark Web* es 12P o proyecto de internet invisible. Comenzó en 2003 cuando un grupo de voluntarios buscaban crear un camino encriptado a través de la internet para el propósito de comunicación resistente de censura. La red 12P fue diseñada para ofrecer la opción de anonimato para activistas, gente oprimida, periodistas, denunciantes, y usuarios de internet promedio. Aunque fue la última de las tres principales plataformas *Dark Web*, ayudó a impulsar la investigación sobre redes anónimas, llevando la *Dark Web* al frente y al centro de la esfera pública.[65]

4. *El caso paradigmático de la Dark Web: Silk Road* El Gran Jurado presentó *Indictment* (acusación) el 4 de febrero de 2014 en la Corte de Distrito de los Estados

[63] *Ibidem,* pp. 23 y 24.
[64] *Ibidem,* p. 24.
[65] *Ibidem,* p. 25.

Unidos del Distrito Sur de Nueva York, identificada como *United States of America v. Ross William Ulbricht*, también conocido como *Dread Pirate Roberts* (Terrible Pirata Roberts), DPR (*Dread Pirate Roberts*) y *Silk Road* (Ruta de la Seda), en su calidad de acusado; el documento está firmado por el presidente del Gran Jurado, cuyo nombre está oculto con franja negra, y por Preet Bharara, Abogado de los Estados Unidos[66]. En dicha declaración el Gran Jurado expuso cuatro cargos.

El primer cargo, se trata del delito de Conspiración de Tráfico de Narcóticos (*Narcotics Trafficking Conspiracy*), constituido por un apartado de antecedentes; otro de alegatos estatutarios; y uno más de actos manifiestos.

En los antecedentes se menciona que en enero de 2011 el acusado creó un sitio *web* clandestino conocido como *Silk Road*, diseñado para posibilitar anónimamente a los usuarios, a través de todo el mundo, comprar y vender drogas ilegales, así como otros ilícitos y servicios fuera del alcance de la aplicación de la ley. Desde 2011 a octubre de 2013, cuando el sitio *web Silk Road* fue cerrado por las autoridades que hacen cumplir la ley, el acusado se apropió y operó la Ruta de la Seda. Durante ese tiempo, *Silk Road* emergió como el mercado criminal más sofisticado y extenso en la Internet. El sitio *web* fue usado por miles de narcotraficantes y otros vendedores ilegales para distribuir cientos de kilogramos de drogas ilegales y otros bienes y servicios ilícitos, además de cientos de miles de compradores de todo el mundo, y para lavar cientos de millones de dólares derivados de estas transacciones ilegales. El acusado controló todos los aspectos de la Ruta de la Seda, con la asistencia de varios empleados pagados a los que él dirigió y supervisó. A través de su propiedad y operación de la Ruta de la Seda, el acusado ganó comisiones con valor de decenas de millones de dólares, generadas por las ventas ilícitas realizadas a través del sitio *web*. En la búsqueda de proteger su empresa criminal y ganancias ilícitas generadas, persiguió medios violentos, incluyendo la solicitud de un asesinato por contrato de diversos individuos que él creyó representaban una amenaza para esa empresa.

[66] Véase *indictment* en THE UNITED STATES DEPARTMENT OF JUSTICE (16 de julio de 2021), https://www.justice.gov/sited/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf.

En el apartado de alegaciones estatutarias, se señala que de enero de 2011 a octubre de 2013, en el Distrito Sur de Nueva York y en otra parte, el acusado y otros conocidos y desconocidos, intencionalmente y a sabiendas se asoció, conspiró, confederó y acordó junto y con cada otro violar las leyes de narcóticos de los Estados Unidos. Fue una parte y objeto de la conspiración que el acusado y otros conocidos y desconocidos distribuirían y distribuyeron y poseían con el intento de distribuir sustancias controladas, con violación del Título 21, del Código de los Estados Unidos, sección 841 (a) (1). Fue más adelante una parte y un objeto de la conspiración que el acusado y otros conocidos y desconocidos harían e hicieron entrega, distribución y despacho de sustancias controladas por medio de la Internet, en una manera no autorizada por la ley, y ayudaron y conspiraron en tal actividad, con violación al Título 21, del Código de los Estados Unidos, sección 841 (h). Fue más adelante una parte y un objeto de la conspiración que el acusado a sabiendas e intencionalmente usaría y usó una comunicación que facilitaría en cometer y en causar y facilitaría la comisión de actos constitutivos de un delito grave bajo el Título 21, del Código de los Estados Unidos, secciones 841, 846, 952, 960 y 963, con violación del Título 21, del Código de los Estados Unidos, sección 843 (b).

Las sustancias controladas que el acusado conspiró para distribuir y poseer con la intención de distribuir incluyó, entre otros, 1 kilogramo y más de mezclas y sustancias conteniendo una cantidad detectable de heroína, 5 kilogramos y más de mezclas y sustancias conteniendo una cantidad detectable de cocaína, 10 gramos y más de mezclas y sustancias conteniendo una cantidad detectable de Dietilamida de Ácido Lisérgico (LSD), y 500 gramos y más de mezclas y sustancias conteniendo una cantidad detectable de metanfetamina, sus sales, isómeros, y sales de sus isómeros, con violación del Título 21, del Código de los Estados Unidos, sección 812, 841 (a) (1), y 841 (b) (1) (A).

Respecto del apartado de los actos manifiestos, refiere, en la promoción de la conspiración y para el efecto de sus objetos ilegales, los siguientes actos manifiestos, entre otros, los cometidos en el Distrito Sur de Nueva York y en otra parte: en enero de 2011, el acusado creó el sitio web *Silk Road*, proporcionando una plataforma para narcotraficantes alrededor del mundo para vender una amplia

variedad de sustancias controladas vía la Internet. El 29 de marzo de 2013, el acusado en conexión con la operación del sitio web *Silk Road*, solicitó a un usuario de la Ruta de la Seda ejecutar un asesinato por contrato de otro usuario de la Ruta de la Seda, quien amenazaba con liberar las identidades de miles de usuarios del sitio. El 1 de octubre de 2013, el acusado conectó como administrador del sitio al servidor de la web almacenando el sitio web de *Silk Road*.

El segundo cargo, como continuación de la empresa criminal, advierte que las alegaciones contenidas en los parágrafos 1 al 4 de esta acusación son repetidas y vueltas a alegar como si estuvieran establecidas completamente de aquí en adelante; es decir, las alegaciones contenidas en el apartado de los antecedentes del primer cargo. Además, de enero de 2011 a octubre de 2013, en el Distrito Sur de Nueva York y en otra parte, el acusado participó en la continuación de la empresa criminal, en la que él a sabiendas e intencionalmente violó el Título 21, del Código de los Estados Unidos, secciones 841, 843 y 846, cuyas violaciones fueron parte de una continuación de series de violaciones de la Ley de sustancias Controladas; y Título 21, del Código de los Estados Unidos, sección 801, y siguiente, emprendidas por el acusado, en concierto con al menos cinco personas más con respecto a quienes el acusado ocupó una posición de organizador, una posición de supervisor y una posición de gestor, con las cuales continuó la serie de violaciones el acusado, quien obtuvo un ingreso sustancial y recursos, en violación al Título 21, del Código de los Estados Unidos, sección 848 (a).

En el tercer cargo, relativo al delito de conspiración de piratería informática (*Computer Hacking Conspiracy*), se repitió la frase de que las alegaciones contenidas en los parágrafos 1 al 4 de esta acusación son repetidas y vueltas a alegar como si estuvieran completamente establecidas de aquí en adelante; es decir, tiene por reproducidas las alegaciones de los antecedentes. Adicionalmente, al suministro de una plataforma para la compra y venta de narcóticos ilegales, el sitio *web* Ruta de la Seda también proporcionó una plataforma para la compra y venta de *software* maliciosos diseñados para la piratería informática, tales como robo de contraseñas, claves de registros, y herramientas de acceso remoto. Mientras estuvo en operación, el sitio *web* Ruta de la Seda regularmente ofreció

cientos de anuncios para tales productos. En este cargo se realizaron también alegaciones estatutarias, en el sentido de que de enero de 2011 a octubre de 2013, en el Distrito Sur de Nueva York y en otra parte, el acusado y otros conocidos y desconocidos, intencionalmente y a sabiendas se asociaron, conspiraron, confederaron y acordaron juntos y con cada otro cometer piratería informática con violación del Título 18, del Código de los Estados Unidos, sección 1030 (a) (2); y que fue parte y objeto de la conspiración que el acusado y otros conocidos y desconocidos, harían e hicieron el acceso intencional a computadoras sin autorización, y de este modo obtendrían y obtuvieron información de computadoras protegidas, para propósitos de ventaja comercial y ganancia financiera privada, y en el fomento de actos delictivos e ilícitos con violación a la Constitución y a las leyes de los Estados Unidos, así como del Título 18, del Código de los Estados Unidos, sección 1030 (a) (2) y sección 1030 (b).

El cuarto cargo, consistió en el delito de conspiración de lavado de dinero (*Money Laundering Conspiracy*), señalando que se tienen por reproducidas las alegaciones del parágrafo 1 al 4 de los antecedentes del primer cargo, agregando que el acusado diseñó el sitio *web* Ruta de la Seda para incluir un sistema de pago basado en moneda digital o virtual (*Bitcoin*) que sirvió para facilitar el comercio ilegal realizado en el sitio *web*, incluyendo la ocultación de las identidades y localización de los usuarios que transmiten y reciben fondos a través del sitio.

Contiene alegaciones estatutarias en los términos siguientes: de enero de 2011 a octubre de 2013, en el Distrito Sur de Nueva York y en otra parte, el acusado y otros conocidos y desconocidos, intencionalmente y a sabiendas se unieron, conspiraron, confederaron y acordaron juntos y con cada otro cometer lavado de dinero, con violación del Título 18, del Código de los Estados Unidos, secciones 1956 (a) (1) (i) y 1956 (a) (1) (B) (i). Siendo una parte y objeto de la conspiración que el acusado y otros conocidos y desconocidos, ofensas que involucran y afectan el comercio interestatal y extranjero, sabiendo que la propiedad involucrada en ciertas transacciones financieras representaron ganancias de alguna forma de actividades ilícitas, que realizarían y realizaron e intentarían e intentaron conducir tales transacciones financieras, las cuales en realidad involucraron las ganancias

de actividades especificadas como ilícitas, por tráfico de narcóticos y piratería informática, con violación del Título 21, del Código de los Estados Unidos, sección 846, y Título 18 del mismo Código, sección 1030, respectivamente.

La intención de promover la realización de la actividad ilícita, fue con violación del Título 18, del Código de los Estados Unidos, sección 1956 (a) (A) (i). Más adelante una parte y un objeto de la conspiración fue que el acusado y otros conocidos y desconocidos, en ofensas que involucran y afectan el comercio interestatal y extranjero, sabiendo que la propiedad involucrada en ciertas transacciones financieras representaron ganancias de alguna forma de actividades ilícitas, realizarían y realizaron e intentarían e intentaron realizar tales transacciones financieras, las cuales involucraron las ganancias de la actividad ilícita especificada, por tráfico de narcóticos y piratería informática, con violación del Título 21, del Código de los Estados Unidos, sección 846, y Título 18, del mismo código, sección 1030, respectivamente, sabiendo que las transacciones fueron diseñadas en todo y en parte para ocultar y disfrazar la naturaleza, la localización, la fuente, la propiedad y el control de las ganancias de la actividad ilícita especificada, con violación del Título 18, del Código de los Estados Unidos, sección 1956 (a) (1) (B) (i); y Título 18, del Código mencionado, sección 1956 (h).

En este cargo se adicionaron alegaciones de decomiso, que estriban en que como resultado de la comisión de las ofensas de las sustancias controladas en los cargos 1 y 2 de esta acusación, el acusado perderá para los Estados Unidos, de conformidad con el Título 21, del Código de los Estados Unidos, sección 853, cualquier propiedad constitutiva, o derivada de, cualquier ganancia que el acusado obtuvo, directa o indirectamente, como resultado de la ofensa y cualquier propiedad usada, o intentada para ser usada, en cualquier forma o parte, para cometer, o para facilitar la comisión de las ofensas.

Por nuestra parte, advertimos que este caso alcanzó dimensiones inesperadas, ya que la acusación fue adicionada con tres cargos más por el Gran Jurado del Distrito de Maryland ante la Corte de Distrito de los Estados Unidos del Distrito de Maryland, el 1 de octubre de 2013; el abogado defensor presentó mociones antes y después del juicio por no cumplir la acusación con los requisitos

de la ley, ni el Fiscal con la solicitud del acusado sobre el descubrimiento probatorio; el jurado lo declaró culpable y también fue sentenciado por la Corte del Distrito Sur de Nueva York a cadena perpetua; apeló la sentencia y fue confirmada; el sentenciado sigue luchando con sus abogados para encontrar salida a la pena, incluso cuenta con una página *web* para que sea apoyado económica y socialmente en dicha lucha; tiene 2 cadenas perpetuas y 40 años más, sin libertad condicional.[67]

Como resultado de cometer la ofensa de piratería informática alegada en los tres cargos de la acusación expuesta, el acusado perderá en favor de los Estados Unidos, de conformidad con el Título 18, del Código de los Estados Unidos, sección 982 (a) (2) (B), cualquier propiedad constitutiva, o derivada de, las ganancias obtenidas directa o indirectamente como resultado de la ofensa; y como resultado de cometer la ofensa de lavado de dinero alegado en el cargo cuatro de esta acusación, el acusado, perderá en favor de los Estados Unidos, de conformidad al Título 18, del Código de los Estados Unidos, sección 982 (a) (1), cualquier propiedad, real o personal, involucrada en la ofensa, o cualquier propiedad rastreable para tal propiedad.

Finalmente, respecto al suministro de activos sustitutos, en la acusación se mencionó que si alguna de las propiedades perdibles descritas arriba, como resultado de cualquier acto u omisión del acusado, no se puede localizar en el ejercicio de la debida diligencia; ha sido transferida o vendida a, o depositada con, una tercera persona; ha sido ubicada más allá de la jurisdicción de la Corte; ha sido sustancialmente disminuida en valor; o ha sido mezclada con otra propiedad que no puede ser subdividida sin dificultad, es la intención de los Estados Unidos, de conformidad con el Título 18, del Código de los Estados Unidos, sección 982 (b) y Título 21, del mismo Código, sección 853 (p), buscar el decomiso de cualquier otra propiedad del acusado hasta el valor de las propiedades perdibles descritas arriba; además con el apoyo del Título 18, secciones 981 y 982; Título 21, sección 853; y Título 28, sección 2461, del Código de los Estados Unidos.

5. *Criptomoneda Bitcoin* El 31 de octubre de 2008, un programador de computadoras con el pseudónimo de Satoshi Nakamoto envió un correo electrónico

[67] FREE ROSS ULBRICHT (16 de julio de 2021), https://freeross.org/

a una lista de correo de criptografía para anunciar que había producido un nuevo sistema de efectivo electrónico que es totalmente *peer-to-peer*, sin ningún tercero de confianza.[68] El 9 de enero de 2009, Nakamoto liberó la versión 0.1 del cliente de *Bitcoin* (hoy conocido como *Bitcoin Core*), un *software* de código abierto que conectaba varias computadoras entre sí, y esto dio origen a la red que soportaría la criptomoneda. Las tareas de la red eran, en apariencia, sencillas: permitir transacciones entre usuarios, hacer una lista de todas las transacciones, verificar que no se gaste dos veces la misma moneda y emitir nuevas unidades monetarias. Ese mismo día, a las 00:54, se abrió el primer bloque de *Bitcoin* y con él se crearon las primeras unidades. Tres días más tarde, el 12 de enero de 2009, Hal Finney, uno de los miembros más destacados de la lista de correo *Cryptography,* recibió la primera transacción de *Bitcoin* de la historia. El 26 de abril de 2011, Nakamoto desapareció y nunca más se supo nada de él. El precio máximo alcanzado a la fecha del *Bitcoin* está por encima de los $60,000 dólares americanos.[69]

En la *web* todavía se puede encontrar el documento de Satoshi Nakamoto que lleva por título *Bitcoin: A Peer-to-Peer Electronic Cash System*[70] (*Bitcoin*: Un Sistema en Efectivo Electrónico de Par a Par [o entre pares o iguales]). El Diccionario Merriam-Webster define *peer-to-peer* como una red mediante la cual los equipos operados por individuos pueden compartir información y recursos directamente sin depender de un servidor central. En informática significa punto a punto, cada cliente puede ser un servidor. Se encadenan dos o más equipos, y todo el mundo puede compartir archivos, programas, unidades, impresoras y cualquier otra cosa que esté adjunta. Otra definición es lo existente o hecho entre pares.[71]

En el documento de Satoshi Nakamoto, en su introducción, menciona que el comercio en internet ha venido dependiendo de instituciones financieras como

---

[68] AMMOUS, Saifedean, *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, U.S.A. y Canadá, John Wiley & Sons, Inc., 2018, p. i.

[69] FORBES, artículo publicado el 27 de abril de 2021 (31 de agosto de 2021), https://forbes.co/2021/04/27/editors-picks/por-que-no-se-sabe-nada-del-creador-del-bitcoin-satoshi-nakamoto/

[70] bitcoin.org/bitcoin.pdf (31 de agosto de 2021), https://bitcoin.org

[71] MERRIAM WEBSTER (31 de agosto de 2021), https://www.merriam-webster.com/dictionary/peer-to-peer

terceros confiables para el procesamiento de pagos electrónicos. El costo de la mediación incrementa los costos de transacción. Los costos e incertidumbres de pagos pueden ser evitados, pero no existe un mecanismo para hacer pagos por un canal de comunicación sin un tercero confiable. Por ende, se necesita un sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiendo a dos partes interesadas realizar transacciones directamente, por lo que propone un servidor de marcas de tiempo usuario-a-usuario distribuido para generar una prueba computacional del orden cronológico de las transacciones. En lo relativo a las transacciones, define la moneda electrónica como una cadena de firmas digitales. Cada dueño transfiere la moneda al próximo al firmar digitalmente un *hash*[72] de la transacción previa y la clave pública del próximo dueño y agregando estos al final de la moneda. Un beneficiario puede verificar las firmas para comprobar la cadena de propiedad. Los demás apartados versan sobre el servidor de marcas de tiempo; prueba de trabajo; red; incentivo; espacio en disco; verificación de pagos simplificada; combinación y división de valor; privacidad, cálculos, y conclusión.

6. *El oscurecimiento de la Web* El profesor Alexander Klimburg refiere que el término cyber antes era utilizado para significar sexo, pero ahora significa guerra.[73] Considera que las aspiraciones de los estados en el ciberespacio, junto con las realidades técnicas de este nuevo mundo artificial, están creando riesgos significativos para el bienestar humano. Estos riesgos están asociados con nuevos medios para no solamente infligir destrucción a gran escala en conflictos interestatales y guerra, sino también para hacer daños catastróficos a sociedades democráticas liberales a través de una reformulación sutil de información en general como un arma. En un futuro no muy lejano internet, un fabuloso artificio de la

[72] Significa función criptográfica; función que asigna cadenas de bits a cadenas de bits de longitud fija que satisface dos propiedades: es inviable computacionalmente encontrar para una cierta salida una entrada que se acote a esa salida y es inviable computacionalmente encontrar para una cierta entrada una segunda entrada que se acote a la misma salida; y la salida de una función hash, resumen de mensaje, resumen hash o valor hash, según NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE, INFORMATION TECHONOLOGY LABORATORY, COMPUTER SECURITY RESOURCE CENTER, (1 de septiembre de 2021), https://csrc.nist.gov/glossary/term/hash

[73] KLIMBURG, Alexander, *THE DARKENING WEB The War for Cyberspace,* U.S.A., Penguin Books, 2018, p. 23.

civilización humana percibido hoy como un dominio para promover las libertades y la prosperidad, podría convertirse en cambio en una *Dark Web* de subyugación.[74]

Sostiene que muchos gobiernos han facilitado la formación de un "mundo dragón" encubierto en el ciberespacio, en el que por falta de transparencia en cuanto al alcance y el tipo de capacidades cibernéticas ofensivas no solo aumenta la posibilidad de que los malentendidos conduzcan a un conflicto total, sino que amenaza con legitimar un tipo de conflicto completamente nuevo, un mundo de guerra de la información en el que el objetivo no es lograr un efecto físico, sino uno psicológico mucho más sutil. Es la conversión de un bien no cualificado en una *Dark Web* que sólo puede ser percibida como una herramienta de dominación, opresión y control. Es la perversión del ciberespacio, de un vehículo que empodera profundamente a los humanos a uno que amenaza con lo contrario.[75]

Nos recuerda que William Gibson en su obra *Neuromancer* describió un mundo en el que las megacorporaciones han reemplazado en gran medida a los estados como potencias dominantes del mundo, y el ciberespacio es el término utilizado para referirse a la cuadrícula de información global conocida como *Matrix*, un espacio artificial poblado de representaciones físicas de datos que forman ciudades y montañas enteras y donde criminales, estados y corporaciones luchan entre sí usando virus y otras armas cibernéticas. Los usuarios, la gente común, son sólo engranajes en el sistema, en el mejor de los casos. Apunta que *Neuromancer* generó la literatura *cyberpunk* en la que el ciberespacio a menudo tiene una sensación ominosa, dominando las vidas de las personas promedio que son esclavos virtuales del control completo de la información de los poderosos: estados, corporaciones y hackers. En estos mundos, internet se ha transformado en algo que abarca todo, íntimo y bastante siniestro: *Matrix*. La idea de *Matrix* pasó a tener una larga vida cultural con la exitosa película de 1999 del mismo nombre, protagonizada por Keanu Reeves. A menudo representa la distopía hecha digital, un sistema panóptico que emplea deliberadamente los datos para un solo propósito: la subyugación del individuo.[76]

---

[74] *Ibidem,* pp. 2 y 3.
[75] *Ibidem,* pp. 11 y 12.
[76] *Ibidem,* pp. 315 y 316.

Advierte que el sueño de los estados de ejercer el poder en y a través de los ciberespacios muestra que hay poderosos incentivos para empujar a Internet a convertirse en algo similar a la *Matrix* de la *Dark Web*. Las sociedades occidentales han definido la seguridad nacional en lo que se refiere al ciberespacio principalmente como una cuestión de efectos *kinetic* (cinéticos), es decir, daños físicos o destrucción de la infraestructura física, pero los estados autoritarios han considerado desde hace mucho tiempo que la principal amenaza a la seguridad surge de los efectos informativos; es decir, la infiltración de mensajes políticos problemáticos. El peligro es que los gobiernos occidentales puedan adoptar lentamente, inadvertidamente, esta línea de pensamiento por sí mismos. Por ejemplo, se lanza un ataque terrorista cibernético importante en los próximos diez años más o menos, los gobiernos occidentales podrían cambiar radicalmente su posición actual al apoyar el enfoque de múltiples partes interesadas para la gobernanza de Internet y presionar para facilitar el desarrollo de un nuevo tipo de arquitectura de Internet muy diferente de lo que tenemos hoy en día. En 2015, un grupo de personas prominentes, entre ellas Bill Gates, Elon Musk, Steve Wozniak y Stephen Hawking, firmaron una carta con cientos de personas más para advertir de un peligro: el auge de la inteligencia artificial (IA). Concluye Klimburg que el poder potencial de la IA, que se ejecuta fuera de la infraestructura de computación cuántica aún por implementar, pero inmensamente poderosa, podría ser una amenaza inmediata de que Internet se convierta en la *Matrix de la Dark Web*.[77]

IV

ORGANIZACIONES INTERNACIONALES QUE LUCHAN CONTRA LAS ACTIVIDADES DELICTIVAS Y MERCADOS ILÍCITOS EN LA *DARK WEB*

1. *ONU* La Oficina de Drogas y Crimen, refiere que el Programa Mundial sobre Delitos Cibernéticos, conforme a la resolución 65/230 de la Asamblea General y las resoluciones 22/7 y 22/8 de la Comisión de Prevención del Delito y Justicia Penal, tiene el mandado de ayudar a los estados miembros en su lucha contra los delitos cibernéticos mediante la creación de capacidad y asistencia técnica, con el financiamiento de los gobiernos de Australia, Canadá, Japón, Noruega, Reino Unido

[77] *Ibidem,* pp. 316-318.

y Estados Unidos. El delito cibernético lo clasifica en ciberdependiente, cibernéticos y, explotación y abuso sexual infantil en línea, los cuales explica y ubica la compra de drogas en línea en el delito cibernético. Refiere que lo que la mayoría de la gente ve en línea es solo una pequeña parte de los datos que se encuentran en la *clearnet*. La mayoría de los motores de búsqueda, por ejemplo, solo indexan el 4% de Internet. La *Deep Web*, que se define como una parte de la *World Wide Web*, no la pueden descubrir los motores de búsqueda, incluye información protegida por contraseña, desde las redes sociales hasta los servidores de correo electrónico. Considera que *Darknet* es una colección de miles de sitios *web* que utilizan herramientas de anonimato como *TOR* para cifrar su tráfico y ocultar sus direcciones IP. El alto nivel de anonimato en el espacio digital permite a los delincuentes actuar sin ser detectados fácilmente. La *darknet* es más conocida por la venta de armas en el mercado negro, la venta de drogas y la transmisión de abuso infantil. Sin embargo, la *darknet* también se utiliza para el bien, incluida la habilitación de la libertad de expresión de activistas de derechos humanos y periodistas.[78]

Para el propósito del Programa Mundial, cuenta con un repositorio de delitos informáticos (base de datos de legislación, base de datos de jurisprudencia y base de datos de lecciones aprendidas).[79] Asimismo, opera un Comité Intergubernamental Especial de Expertos para elaborar una convención internacional sobre la lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos.[80]

2. *INTERPOL* Expertos del Complejo Mundial para la Innovación de INTERPOL, en diciembre de 2016 y abril de 2017, encontraron pruebas de que los delincuentes utilizan la *Darknet* para vender productos ilícitos de vida silvestre de especies en

[78] ONU, OFICINA DE DROGAS Y CRIMEN, *Cybercrime* (30 de agosto de 2021), https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

[79] ONU, OFICINA DE DROGAS Y CRIMEN, *Cybercrime* (30 de agosto de 2021), https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html

[80] ONU, OFICINA DE DROGAS Y CRIMEN, *Cybercrime* (30 de agosto de 2021), https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

peligro crítico, como el cuerno de rinoceronte, el marfil de elefante y las partes y productos de tigre. En el informe del Departamento de Estado de los Estados Unidos y de la *African Wildlife Foundation*, se demostró que la mayoría del comercio fue en criptomonedas como *Bitcoin*. Refiere que el crecimiento del comercio electrónico y el interés potencial en esta área delictiva demuestran la necesidad de que los funcionarios encargados de hacer cumplir la ley analicen la *Darknet* al investigar a los delincuentes de la vida silvestre. INTERPOL mantiene una asociación de largo tiempo con el Fondo Internacional para el Bienestar Animal (IFAW) para combatir los delitos contra la vida silvestre en todo el mundo.[81]

Asimismo, publicó en julio de 2019 y puso a disposición un Manual Operativo sobre la investigación del terrorismo biológico y químico en la *Darknet*, que contiene las mejores prácticas internacionales, las técnicas y procedimientos para investigadores y analistas al realizar investigaciones en la *Darknet* relacionadas con la adquisición de agentes biológicos y químicos.[82] Interpol, la Organización de los Países Bajos para la Investigación Científica Aplicada y con apoyo de expertos del Laboratorio Kaspersky y de SECOM de Japón, realizaron capacitación del 15 al 19 de agosto de 2016, para identificar delincuentes y redes de delincuencia organizada dentro de la *Darknet* y su *modus operandi,* cuyo objetivo fue desarrollar capacidades en áreas clave relacionadas con el uso de *Darknet* y las criptomonedas, incluida la investigación en línea, el análisis forense digital, el análisis, la colaboración internacional, los desafíos legales y la criminología.[83]

3. *EUROPOL* Ejemplo de la lucha contra los mercados ilícitos en la *Dark Web* es la eliminación de los llamados *Wall Street Market* y *Silkkitie* (conocido como *Valhalla Marketplace*). Respecto del primero de ellos, la Policía Criminal Federal de Alemania lo cerró bajo la autoridad del Fiscal de ese país, apoyados por la Policía Nacional Holandesa, Europol, Eurojust y varias agencias de los Estados Unidos

[81] INTERPOL, *Research identifies ilegal wildlife trade on the Darknet, 14 june 2017* (1 de septiembre de 2021), https://www.interpol.int/News-and-Events/News/2017/Research-identifies-illegal-wildlife-trade-on-the-Darknet

[82] INTERPOL, *INTERPOL Operational Manual on Investigating Biological and Chemical Terrorismo on the Darknet* (1 de septiembre de 2021), interpol.int/Crimes/Terrorism/Bioterrorism

[83] INTERPOL, *INTERPOL Training on Darknet and cryptocurrencies targets organized crime,* 19 August 2016 (1 de septiembre de 2021), interpol.int/News-and-Events/News/2016/INTERPOL-training-on-Darknet-and-cryptocurrencies-targets-organized-crime

(Administración de Control de Drogas, Oficina Federal de Investigación, Servicio de Impuestos Internos, Investigaciones de Seguridad Nacional, Servicio de Inspección Postal y el Departamento de Justicia). El mercado comerciaba drogas (cocaína, heroína, cannabis y anfetaminas), datos robados, documentos falsos y *software* malicioso. La plataforma ilegal era accesible exclusivamente a través de la red *Tor* en la *Dark Web*. Contaba con 63,000 ofertas de venta en línea y el registro de 1,150,000 cuentas de clientes y 5,400 vendedores, cuyos pagos de los usuarios fue a través de criptomonedas *Bitcoin* y *Monero*. Se detuvo a 3 sospechosos, se aseguró 550,000 € en efectivo, criptomonedas *Bitcoin y Monero* en montos de 6 dígitos, etc. En los Estados Unidos se arrestaron a dos de los proveedores de narcóticos.[84]

En cuanto al segundo mercado, participó la Aduana Finlandesa, con la cooperación de la Policía Nacional francesa y Europol, quien contó con la asistencia de *Bitdefender*, empresa de seguridad de internet que asesora al Centro Europeo de Ciberdelincuencia (EC3) de Europol. Dicho mercado operaba en la red *Tor* desde 2013, al que se le aseguró moneda digital *Bitcoin*, producto de la venta de estupefacientes y otros productos ilícitos. Europol ha establecido un equipo dedicado a la *Dark Web* para trabajar con los socios de la Unión Europea y las fuerzas del orden en todo el mundo para reducir la economía ilegal clandestina.[85]

Debe resaltarse que La *Dark Web* es utilizada por ciudadanos y empresas, así como por los que hacen cumplir la ley, militares y comunidades de inteligencia.[86]

V

CONCLUSIONES

Primera. El ciberespacio, como realidad virtual, es el nuevo *Nomos* en nuestro planeta que pretenden conquistar y dominar las personas físicas y jurídicas (corporaciones y estados) con sus propias reglas, a fin de salvaguardar sus

[84] EUROPOL, *Double Blow to Dark Web Marketplaces,* 3 May 2019, (2 de septiembre de 2021), https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces

[85] *Idem.*

[86] FINKLEA, Kristin, *Dark Web,* p. 13, Congressional Research Service, March 19, 2017, (2 de septiembre de 2021), https://sgp.fas.org/crs/misc/R44101.pdf

intereses, incluso para cometer delitos en forma clandestina a través de las plataformas de la *Dark Web*.

Segunda. El fenómeno del cibercrimen en la *Dark Web* amerita esfuerzos de cooperación internacional para combatirlo, lo que implica, quizá, una convención específica, garantizando los derechos de terceros; por consiguiente, leyes específicas en nuestro país y otros para evitar conflictos de leyes.

Tercera. Las instituciones de investigación de delitos en México no mencionan el cibercrimen en la *Dark Web*, lo que no significa que no exista, sino que tal vez no lo abordan.

VI

REFERENCIAS

AMMOUS, Saifedean, *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, U.S.A. y Canadá, John Wiley & Sons, Inc., 2018.

BECKSTROM, Matthew & LUND, Brady, *Casting Light on the Dark Web A Guide for Safe Exploration,* United Kingdom, Rowman & Littlefield, 2019.

DIEZ DE VELASCO, Manuel, *Instituciones de Derecho Internacional Público*, 16ª edición, España, Tecnos, 2007.

FINKLEA, Kristin, *Dark Web,* Congressional Research Service, March 19, 2017, (2 de septiembre de 2021), https://sgp.fas.org/crs/misc/R44101.pdf

KAKU, Michio, *HIPERESPACIO Una odisea científica a través de universos paralelos, distorsiones del tiempo y la décima dimensión,* Traductor Javier García Sanz, España, Crítica-Drakontos, 2017.

KLIMBURG, Alexander, *THE DARKENING WEB The War for Cyberspace,* U.S.A., Penguin Books, 2018.

MERRIAM WEBSTER (31 de agosto de 2021), https://www.merriam-webster.com/dictionary/peer-to-peer

REED, Chris, y MURRAY, Andrew, *Rethinking the Jurisprudence of Cyberspace,* U.S.A., Edward Elgar Publishing Limited, 2020.

SCHMITT, Carl, *Tierra y mar,* Traductor Rafael Fernández-Quintanilla, España, editorial Trotta, 2007.

SCHMITT, Carl, *El Nomos de la Tierra en el Derecho de Gentes del Ius publicum europaem*, Traductora Dora Schilling Thou, España, editorial Comares, 2002.

URIBE BENÍTEZ, Oscar, *Desarrollo histórico y legislativo de la autonomía de los pueblos y comunidades indígenas de México, Quórum Legislativo,* núm. 99, diciembre 2009.

VAN PUYVELDE, Damien, y F. BRANTLY, Aaron, *CYBERSECURITY Politics, Governance and Conflict in Cyberspace,* United Kingdom, Polity Press, 2019.

INTERNET

BITCOIN.ORG/bitcoin.pdf (31 de agosto de 2021), https://bitcoin.org

COUNCIL OF EUROPE, *Convention on Cybercrime* (31 de agosto de 2021), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?

EUROPOL, *Double Blow to Dark Web Marketplaces,* 3 May 2019, (2 de septiembre de 2021), https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces

FORBES, artículo publicado el 27 de abril de 2021 (31 de agosto de 2021), https://forbes.co/2021/04/27/editors-picks/por-que-no-se-sabe-nada-del-creador-del-bitcoin-satoshi-nakamoto/

FREE ROSS ULBRICHT (16 de julio de 2021), disponible en: https://freeross.org/

INTERPOL, (1 de septiembre de 2021), https://www.interpol.int/

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE, INFORMATION TECHONOLOGY LABORATORY, COMPUTER SECURITY RESOURCE CENTER, (1 de septiembre de 2021), https://csrc.nist.gov/glossary/term/hash

ORGANIZACIÓN DE LAS NACIONES UNIDAS, OFICINA DE DROGAS Y CRIMEN, *Cybercrime* (30 de agosto de 2021), https://www.unodc.org/unodc/en/cybercrime

UNITED STATES DEPARTMENT OF JUSTICE (16 de julio de 2021), https://www.justice.gov/sited/default/files/usaosdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf.