UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, LEÓN

UNAN-LEÓN

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

PROGRAMA DE MAESTRÍA PROFESIONAL EN DERECHO PENAL Y DERECHO PROCESAL PENAL

PRIMERA EDICIÓN

Tesis de investigación para optar al grado académico de Magíster en Derecho con énfasis en Derecho Penal y Derecho Procesal Penal

LA LEY ESPECIAL DE CIBERDELITOS DE NICARAGUA: ANÁLISIS SOBRE SU ÁMBITO DE APLICACIÓN ESPACIAL

Autor: José Alfredo Herradora Pérez

Tutor: Prof. Dr. Marcelo Antonio Castillo Monterrey

León, noviembre 2021.

"A la Libertad por la Universidad"

UNIVERSIDAD
NACIONAL
AUTÓNOMA DE
NICARAGUA - LEÓN

Facultad de Ciencias Jurídicas y Sociales
Departamento de Derecho Público
Programa de Maestría Profesional en Derecho penal y Derecho procesal penal
Primera Edición (Bienio 2017/2019)

CARTA DE AUTORIZACIÓN DEL TUTOR DE LA TESIS DE INVESTIGACIÓN COMO FORMA DE CULMINACIÓN DE ESTUDIOS DE MAESTRÍA

El suscrito Profesor **Marcelo A. Castillo Monterrey**, Tutor del discente **José Alfredo Herradora Pérez,** informa favorablemente de la investigación titulada **"La Ley Especial de Ciberdelitos de Nicaragua: Análisis Sobre su Ámbito de Aplicación Espacial",** realizada durante periodo extraordinario de investigación y elaboración de los Trabajos de Fin de Maestría (TFM) de la primera edición del Programa de Maestría Profesional en Derecho penal y Derecho procesal penal (Bienio 2017/2019) de la Universidad Nacional Autónoma de Nicaragua, León (UNAN-León), por cumplir con la aptitud, pertinencia y calidad científicas mínimas requeridas y la estructura académica básica como forma de culminación de estudios para optar al **Título de Magister en Derecho con énfasis en Derecho penal y Derecho procesal penal** por la misma Universidad.

Asimismo, hago constar que la tesis de investigación cumple con lo estipulado en los anexos: Área, líneas y temáticas específicas de investigación 2018/2023; Instructivo para la formulación de artículos científicos como Trabajos de Fin de Especialidad y Fin de Maestría y; Modelo de citas de referencia de fuentes de conocimiento para elaboración de Trabajos de Fin de Especialidad y Fin de Maestría, todos del programa de postgrado referido.

Por todo lo anterior y de conformidad con los Artículos 14, 21 y 38 del Reglamento de Estudios de Postgrado de la UNAN-León aprobado en Sesión No. 260 del Consejo Universitario, del día 21 de julio del año 2014 y; del numeral XIV del Programa de Postgrado y Reglamento Interno del Programa de Postgrado: Maestría Profesional en Derecho penal y Derecho procesal penal, en mi calidad de Tutor, expreso mediante este informe mi debida AUTORIZACIÓN para la presentación de la aludida tesis de investigación ante la Comisión Académica del Programa de Postgrado para que sea sometida a consideración de dicha instancia la aprobación de su disertación y defesa pública ante Tribunal Examinador especialmente constituido.

Autorizado en la ciudad de León, a los tres días del mes de noviembre del año dos mil veintiuno.

Fdo. _____

Dr. Marcelo A. Castillo Monterrey

Tutor

RESUMEN

En este trabajo se analiza el ámbito de aplicación espacial de la Ley Especial de Ciberdelitos de Nicaragua, con el propósito de establecer las bases para una aplicación espacial razonable de la legislación penal nicaragüense, ante posibles conflictos de jurisdicción. Con tal fin, primeramente, se expusieron los conceptos informáticos generalmente empleados en materia de ciberdelincuencia. Sucesivamente, se analizó el postulado del lugar de comisión del cibercrimen. A continuación, se analizaron los criterios adoptados por los países miembros del Sistema de Integración Centroamericana para aplicar su legislación frente al cibercrimen. Tras la revisión documental se concluyó que el conocimiento de los conceptos informáticos básicos permite una adecuada comprensión y aplicación de la ley; que los componentes físicos del cibercrimen permiten identificar el lugar material de comisión del hecho y que el ámbito espacial de la Ley Especial de Ciberdelitos de Nicaragua no cumple con los estándares internacionales.

Palabras claves: cibercrimen, lugar de comisión, ley, ámbito espacial, jurisdicción

ABSTRACT

This paper analyzes the spatial scope of application of the Nicaraguan Special Cybercrime Law, in order to establish the bases for a reasonable spatial application of Nicaraguan criminal law, in the face of possible conflicts of jurisdiction. To this end, firstly, the computer concepts generally used in the field of cybercrime were exposed. Subsequently, the postulate of the place of commission of the cybercrime was analyzed. Next, the criteria adopted by the member countries of the Central American Integration System to apply their legislation against cybercrime were analyzed. After the documentary review, it was concluded that the knowledge of the basic computer concepts allows an adequate understanding and application of the law; that the physical components of cybercrime make it possible to identify the material place of commission of the act and that the spatial scope of the Special Cybercrime Law of Nicaragua does not comply with international standards.

Keywords: *cybercrime, place of commission, law, spatial scope, jurisdiction*

SUMARIO

I. INTRODUCCIÓN

La intromisión de las tecnologías de la comunicación e información en la vida cotidiana de la sociedad moderna ha facilitado la inmediatez de las comunicaciones, así como el procesamiento expedito y preciso de gran cantidad de información. Como consecuencia de ello, esta sociedad se vuelve cada día dependiente de estas tecnologías, a tal punto que las estructuras informáticas o el denominado ciberespacio se representan como bienes de vital importancia para su correcto funcionamiento.

En ese sentido, el "ciberespacio" se ha erigido como una comunidad virtual, donde las personas socializan, comercializan, laboran y se desarrollan personal y profesionalmente. Por otro lado, en ese mismo espacio virtual han surgido actividades delictivas que se benefician de las ventajas de esas tecnologías. Tras esa preocupación, los Estados han tomado medidas legislativas para regular esas conductas en la red, no obstante, su capacidad jurisdiccional se ha visto mermada por la naturaleza transnacional de estos delitos. Esa incapacidad se traduce en las dificultades de identificar el lugar de comisión del hecho y, además, en los óbices de su investigación, persecución y sanción, que se acentúan ante la colisión con la soberanía territorial de otros Estados. A partir de ello, han surgido posturas que llaman a repensar el postulado del lugar de comisión del hecho para concebirlo como un lugar indeterminado[1].

Ciertamente, esa cosmovisión entra en contienda con **el principio de territorialidad**, bajo el cual los distintos Estados aplican, en primera instancia, su legislación penal en el espacio. Así pues, la idea de que el cibercrimen acontece en un espacio inmaterial ha provocado una creciente preocupación por las situaciones de impunidad que esto podría generar. Y en ese afán, algunos países han optado por establecer criterios de aplicación espacial de la ley penal muy amplios para atraer su **jurisdicción**, como ha pasado en el caso

[1] Véase MAYA, Ricardo Posada, "El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual", *Nuevo Foro Penal*, vol. 13, no 88, [en línea], 2017, 72-112, p. 72 y ss. Consultado el 19 de junio del 2021. Disponible en: https://publicaciones.eafit.edu.co/index.php/nuevo-foro-penal/article/download/4751/pdf/.

nicaragüense, en el cual la **Ley Especial de Ciberdelitos** (en adelante, LECD)[2] establece que ésta se aplicará a quienes cometan los delitos contenidos ella, **independientemente del lugar donde se realicen**. Por consiguiente, en este trabajo tratamos de responder a las interrogantes ¿en qué lugar se cometen los cibercrímenes? ¿Es necesario abandonar los postulados tradicionales de aplicación espacial de la ley penal*?* ¿El ámbito de aplicación espacial de la LECD cumple con los estándares internacionales? Subsidiariamente, aparte de la LECD ¿Contiene la legislación penal nicaragüense criterios concretos para resolver posibles conflictos de jurisdicción frente a los cibercrímenes*?*

Para dilucidar esa problemática nos propusimos como objetivo general: analizar el ámbito de aplicación espacial de la LECD a través la doctrina y la legislación penal comparada para proponer una adecuada aplicación de la legislación en casos de conflictos de jurisdicción. En esa línea, nos trazamos tres objetivos específicos, consistentes: en exponer los conceptos esenciales del funcionamiento de las TIC como compontes del cibercrimen; examinar el postulado dogmático del lugar de comisión del hecho frente al cibercrimen tanto a nivel doctrinal como legislativo, y, por último, analizar el ámbito de aplicación espacial de la LECD adoptado por el legislador nicaragüense. Conforme a lo anterior, esta investigación es de tipo documental, puesto que se analiza la problemática desde el campo teórico-conceptual. Se consultó la literatura especializada, la legislación comparada, instrumentos internacionales y sentencias de órganos internacionales, los cuales, en su conjunto, nos permitieron enmarcar la problemática teórica del tema de estudio y, consecuentemente, proponer una solución al respecto.

En esa labor metodológica, se utilizaron tres métodos de investigación, a saber: el método análisis-síntesis, conforme al cual diseccionamos el análisis de la problemática en cuatro fases; en la primera, se expuso la terminología técnica y se profundizó en la noción del denominado ciberespacio; en la segunda, se analizó el postulado del lugar del hecho en el cibercrimen; en la tercera, se analizó brevemente la legislación comparada y, por último, se conjugaron todos esos elementos estudiados en el análisis del ámbito de aplicación espacial de la LECD. Paralelamente, se utilizó el método deductivo, en el cual se partió de los

[2] Ley Nº. 1042**, "**Ley Especial de Ciberdelitos**".** En la Gaceta, Diario Oficial, del 30 de octubre de 2020, Nº. 201, pp. 9319-9316.

aspectos generales, desde los conceptos básicos, el desarrollo doctrinal de la problemática en general, el abordaje a través del Convenio de Budapest, la legislación comparada, hasta arribar a lo particular, que fue el análisis del ámbito de aplicación de la referida ley. Por lo referido, se empleó como recurso auxiliar el método de derecho comparado.

II. PRECISIONES CONCEPTUALES

El estudio de la ciberdelincuencia requiere no solamente del saber de la Ciencia Penal, sino, también, del conocimiento técnico de la informática. En ese sentido, en este título esbozaremos un marco conceptual sobre los términos que nos ayudarán a comprender dicho fenómeno.

1. DATO E INFORMACIÓN

El **dato** es definido como una representación de hechos, conceptos o instrucciones en una manera formalizada, apta para la comunicación, la interpretación o el procesamiento[3]. Los datos suelen ser representaciones aisladas que, por sí mismos, no tienen un significado mayor que aquel que ellos representan, pero cuando esos datos son recopilados y pasan por un sistema o medio que los procesa, generan una información útil para tomar una decisión.

En ese sentido, la información es definida por PAOLI como "…un conjunto de mecanismos que permiten al individuo retomar los datos de su ambiente y estructurarlos de una manera determinada, de modo que le sirvan como guía de su acción. …"[4]. Así las cosas, los datos serán los hechos, conceptos e instrucciones sin procesar, que una vez que se agrupan, organizan, analizan, terminan en convertirse en información[5].

---

[3] RIGDON, John C. *Data*, en *Dictionary of computer and internet terms*,1. a ed., Catersville, Eastern Digital Resources. 2016, [en línea], Consultado el 1 de julio del 2021. Disponible en: http://www.damanhour.edu.eg/pdf/738/dictionaries/[Dictionary of Computer and Internet TermsWords.pdf.

[4] PAOLI, J. Antonio, "Comunicación e información", *Perspectivas teóricas*, México, *Trillas*, UAM, 1983, p. 15.

[5] FLORES SALGADO, Lucerito, *Derecho informático*, México, Grupo Editorial Patria, 2014, p. 7.

Debido a que el cerebro humano dispone de una capacidad limitada para procesar los datos, surge la idea de crear dispositivos que faciliten y agilicen la capacidad de almacenamiento y procesamiento de los datos, *verbi gratia:* la computadora, entendiéndola acá como un sistema de procesamiento de datos (en el siguiente apartado se profundizará sobre el concepto).

Así pues, cuando esos datos se digitalizan (en código binario) para ser tratados por una computadora, son denominados **datos informáticos.** A nivel internacional el concepto normativo de dato informático se recoge en el Convenio de Budapest sobre la Cibercriminalidad (en adelante: el Convenio de Budapest), el cual los define como "…toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función[6]". Aparentemente el Convenio equipara al **dato** con el término de información, no obstante, a nuestro parecer, se refiere a que el dato es una representación de la información.

En el año dos mil veintiuno, con la entrada en vigor de la LECD se incorporó a la legislación nacional un concepto de dato informático, el cual consiste en "*cualquier representación de hechos, información o conceptos en formato digital o analógico**,** que puedan ser generados, almacenados, procesados o transmitidos a través de las Tecnologías de la Información y la Comunicación"*[7]. Esta definición tiene cierta similitud con la brindada por la Convención de Budapest, con la excepción de que incorpora una variante**:** que el dato puede encontrarse en **formato digital** o **analógico,** lo cual puede resultar incompatible, puesto que ambos formatos tienen distinta naturaleza[8].

[6] Véase el art. 1 inc. b, Consejo de Europa, "Convenio sobre Cibercriminalidad", Budapest, abierto a la firma el 23 de noviembre de 2001, Serie de Tratados Europeos, No. 185, p. 4.

[7] Art. 3, numeral 5.

[8] HARTWIG, Robert. L, *Basic TV Technology: Digital and Analog*, 4ta ed., EE. UU, ELSEVIER, *p. 26 y 168.* Para dilucidar esta distinción el referido autor lo ejemplifica con la voz de una persona emulada a través de un altavoz tradicional. En este supuesto, las ondas sonoras son captadas por un diafragma dentro de un micrófono, el cual reacciona a dichas ondas y vibra, creando un voltaje eléctrico (señal analógica); este

2. COMPUTADORA

La computadora es definida como "cualquier dispositivo capaz de procesar la información para producir un resultado deseado. No importa cuán largas o pequeñas sean las computadoras, típicamente se desempeñan en tres pasos bien definidos: (1) aceptar la entrada de información, (2) procesar la información de acuerdo con las reglas predefinidas (programas) y (3) producir la información procesada[9]".

Para que la computadora pueda cumplir con esos tres pasos, precisa, por lo tanto, de un dispositivo físico en el cual se introduzcan los datos y de un programa o dispositivo inmaterial que se encargue de procesar la información para obtener la respuesta deseada. Es decir, requiere de la conjunción de un *hardware* y *software*, respectivamente.

En una concepción amplia, el *hardware* comprende los componentes físicos de un sistema informático, incluyendo cualquier equipamiento periférico como una impresora, módems, y el dispositivo conocido como *mouse*[10]. Por otro lado, concretamente, por *software* se entiende al conjunto de instrucciones que le dice al sistema cómo funcionar, permitiendo a los usuarios usar los recursos del ordenador directamente, como, por ejemplo, los sistemas operativos: *Windows*, *Mac* o *Linux*, entre otros[11]. En resumen, podríamos decir que el *hardware* es el que permite la introducción y salida material de datos, del usuario al equipo y viceversa, mientras que el *software* permite a los usuarios la interacción virtual con el ordenador.

---

voltaje es transmitido a la ingeniería del altavoz y, sucesivamente, este se encarga de emular las ondas sonoras recibidas. Mientras que, para que la señal analógica sea digital, debe convertirse en ceros y uno.

[9] RIGDON, John C., *Computer,* en *op., cit.,* Cuando se hace mención al tamaño de la computadora, se refiere a que los dispositivos como los celulares podrían incluirse dentro de ese concepto, siempre y cuando cumplan con las funcionalidades descritas.

[10] RIGDON, John C. *Hardware, en op., cit.*

[11] LABORATORIO NACIONAL DE CALIDAD DEL SOFTWARE, *Ingeniería del software: metodologías y ciclos de vida*, España, Instituto Nacional de Tecnologías de la Comunicación, 2009, p. 11.

3. SISTEMA DE INFORMACIÓN Y SISTEMA INFORMÁTICO

El **sistema de información** es conocido como "un sistema ya sea automatizado o manual, que comprende a las personas, máquinas y/o métodos organizados para recolectar, procesar, transmitir y diseminar los datos que representan la información del usuario"[12]. Mientras tanto, el **sistema informático** es definido como "todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa"[13].

De estas definiciones se desprende que el término "**sistema de información"** puede utilizarse para referirse –genéricamente– al procesamiento de datos tanto manuales como automatizados, que puede comprender el elemento humano y de máquinas, mientras que el sistema informático hace alusión específicamente al tratamiento automatizado de los datos por medio de computadoras.

4. TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC[14])

Para ZUPPO, la problemática en la definición de las TIC radica en que son un cuerpo común de muchas áreas del conocimiento, las cuales, en muchos casos, se basan de alguna manera en una definición tácita del término y las diversas aplicaciones en las que son

---

[12] THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION. *Telcom Glossarry: informatiom system*, [en línea]. Consultado el 15 de julio del 2021. Disponible en http://standards.tiaonline.org/market_intelligence_/glossary/index.cfm?term=%26%23%24%3B%5BR%227G%0A.

[13] Convenio de Budapest, art. 1, inciso a.

[14] Si bien es cierto, es común en el ámbito periodístico, incluso académico, encontrar la abreviación de las Tecnologías de la información y comunicación como TICS o TICs para denotar el plural, sin embargo, la *FUNDÉU*, asesorada por la RAE, sugiere que lo correcto es que el plural se indique a través de los determinantes "Las", puesto que al ser las TIC un acrónimo, agregarle la S, implicaría hacer referencia a un acrónimo distinto o confundirlo con otro. Véase *FUNDÉU* RAE, "*las TIC*, mejor que *las TICs* o *las TICS"*, [en línea]. Consultado el 15 de julio del 2021. Disponible en https://www.fundeu.es/recomendacion/las-tic-mejor-que-las-tics-o-las-tics/. En el mismo sentido coincide MIRÓ LLINARES, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012, p. 25.

empleadas[15]. Ello quiere decir que generalmente se emplea este término sin que exista hasta el momento un consenso sobre su definición, de manera tal que su definición se ha asumido implícitamente. Por consiguiente, su concepción variará en correspondencia al área del conocimiento en la que se emplee el término.

Pese a la disyuntiva que existe en cada disciplina, el referido autor encontró que sí puede sintetizarse los puntos en común de cada una de ellas y de esa manera puede establecerse una noción básica o primaria de las TIC, la cual gira en torno a los dispositivos e infraestructuras que facilitan la transferencia de información a través de medios digitales[16]

A partir de esta concepción se extrae que las TIC están configuradas por una serie de dispositivos e infraestructuras que, a criterio de BENÍTEZ y QUINTANA, se pueden agrupar en cuatro categorías, a saber: **redes**, **terminales**, **aplicativos/*software*** y **servicios**[17]. En cuanto al primer criterio, se incluyen la telefonía móvil, banda ancha, internet, en general sistemas de conexión digital alámbrica o inalámbrica, entre otros.

Dentro de las **terminales** se cuenta con los dispositivos electrónicos propiamente dichos, como *smartphones, Smart T. V,* impresoras, videocámaras digitales, discos duros, entre otros. En lo que respecta al ***software*** se incluye a los sistemas operativos y sus aplicativos, por ejemplo, *Windows 10 y Microsoft Word*, respectivamente. Por último, la categoría de **servicios** contiene el correo electrónico, buscadores como *Google*, banca en línea; en general páginas web que brinden servicios como almacenamiento en la nube, por ejemplo[18].

---

[15] ZUPPO, Colrain M., "Defining ICT in a boundaryless world: the development of a working hierarchy", *International Journal of Managing Information Technology*, vol. 4, No.32, [en línea], 2012, 13-22, p. 13. Consultado el 22 de julio del 2021. Disponible en: http://www.airccse.org/journal/ijmit/papers/4312ijmit02.pdf

[16] Véase *ídem*, p. 13 y ss.

[17] BENÍTEZ, William Guillermo Jiménez, y QUINTANA, Orlando Meneses. "La investigación y práctica jurídicas", *Revista Prolegómenos Derechos y Valores*, vol. 20, no. 40, Colombia, Universidad Militar Nueva Granada, 2017, 43-61, p. 45. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6091041.

[18] *Ídem*, p. 45 y ss.

Por su parte, el art. 3 de la LECD define a las TIC como el **"**Conjunto de medios de comunicación y las aplicaciones de información que permiten la captura, producción, reproducción, transmisión, almacenamiento, procesamiento, tratamiento, y presentación de información, en forma de imágenes, voz, textos, códigos o datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros, por medio de protocolos de comunicación, transmisión y recepción". De esta definición se colige que el legislador nicaragüense ha optado también por prever una definición lo suficientemente amplia que abarque no solamente los dispositivos actuales, sino, también los futuros.

De esta manera, la definición amplia desarrollada en la LECD sobre las TIC, efectivamente, abarca los elementos desarrollados por BENÍTEZ y QUINTANA, tales como las: **redes**, **terminales**, **aplicativos/*software*** y **servicios.** No obstante, opinamos que en la LECD se incurrió en ciertos pleonasmos en el uso de este término, como, por ejemplo, en la tipificación del **acceso indebido a sistemas informáticos** (art. 4), en el cual se sanciona, *inter alias,* al que acceda sin autorización a un sistema informático "…que utilice las Tecnologías de la Información y la Comunicación… A como se estudió líneas arriba, el sistema informático va integrado en el funcionamiento de la computadora, al igual que en la definición de las TIC. En consecuencia, es un pleonasmo exigir que el sistema informático deba utilizar las TIC.

5. APROXIMACIÓN CONCEPTUAL A LA CIBERDELINCUENCIA

Desde el Derecho Penal y la Criminología se ha buscado establecer un término omnicomprensivo de todas aquellas conductas ilícitas que se cometen mediante los sistemas informáticos o en contra de éstos; en ese afán se usan los términos: ciberdelitos, ciberdelincuencia, delincuencia informática, cibercrimen, delitos informáticos o delitos de alta tecnología, sin encontrar, hasta el momento, un consenso al respecto[19]. Así, en las siguientes líneas nos proponemos acercarnos a una definición del cibercrimen para delimitar nuestro tema de estudio.

[19] Por nuestra parte, optaremos por la expresión de cibercrimen o ciberdelincuencia (esta última como categoría que engloba el conjunto de cibercrímenes), elección que justificaremos con posterioridad.

Se debe tomar en consideración, *ab initio*, que las primeras acciones estatales encaminadas a perseguir y sancionar las infracciones penales relacionadas con el uso de los sistemas informáticos aparecieron en los Estados Unidos de Norte América (en adelante: EEUU) al final de la década de 1970, hasta formalizar su tratamiento a través de la sección 1030 de la *Comprehensive Crime Control Act* de 1984[20], la cual regulaba, entre otros aspectos, el acceso ilegítimo a la información almacenada en las computadoras[21]. EEUU fue, entonces, el primer país en regular este tipo de delito y, por ello, en estudiar el fenómeno.

De ahí que, las primeras denominaciones para este tipo de conductas criminales fueran en el idioma inglés, empleándose los términos, en un principio: *crime by computer*[22], posteriormente, *computer crime*[23] *o computer-related crime*[24] y por último *cybercrime*[25], aunque con menos frecuencia, también se ha denominado *Information Technology Crime* (*IT crime*), *Information and Communication Technology Crime* (*ICT crime*) *o high tech*

[20] Véase GUTIÉRREZ FRANCÉS, María Luz, *Fraude informático y estafa*, Madrid, Ministerio de Justicia de España, 1991, p. 23, quien recoge una breve memoria de estas conductas y de las acciones judiciales que se realizaron; por su parte, MATA Y MARTÍN, Ricardo M, *Delincuencia informática y Derecho Penal*, Managua, Hispamer, 2003, p. 23, confirma que fue en EEUU donde por primera vez se reguló el fenómeno a través de la *Crime Control Act* de 1984.

[21] DEPARTMENT OF JUSTICE, *Prosecuting Computer Crime*, 2da. ed., Washington D.C, Office of Legal Education Executive Office for United States Attorneys, 2007, p.1. Disponible en: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

[22] Véase PARKER, D. B., *Crime by Computer*, New York, Charles Scribner's Sons, 1976, p. 1 y ss.

[23] La conducta delictiva va mostrando una evolución no solamente fenomenológica, también en su denominación, lo cual se refleja en el segundo libro de PARKER, D. B., *Fighting Computer Crime*, New York, Charles Scribner's Sons, 1983, p. 1 y ss.

[24] En 1986 se usaban indistintamente las denominaciones: *computer crime o computer related crimen*, véase TOMPKINS JR., Joseph B., y MAR, Linda A., "*The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem", The John Marshall Journal of Information Technology & Privacy Law*, no. 6, [en línea], 1986, 459-483, p. 460. Consultado el 23 de julio del 2021. Disponible en: https://repository.jmls.edu/cgi/viewcontent.cgi?article=1512&context=jitpl.

[25] Según MIRÓ LLINARES, F., *op., cit.*, p. 33, el primer uso de este término se le atribuye a John Perry Barlow, teórico de la sociedad de la información.

crime [26]. En Alemania, en el año 1980, se abordó por SIEBER como *Computerkriminalität*[27]. Como reflejo de esa falta de uniformidad, se podría explicar el motivo por el cual en los académicos de habla hispana no exista un consenso sobre el término que englobe estas conductas.

Las TIC han revolucionado el comercio, la forma de gobernar y las relaciones sociales, sin embargo, las bondades de esas tecnologías se han empleado en la comisión de conductas ilícitas tradicionales y se ha concebido, inclusive, la privación de una vida haciendo uso de éstas. Por ejemplo, se reporta que personas se han infiltrado en computadoras de un hospital y alteraron las prescripciones médicas y en su lugar prescribieron fármacos potencialmente letales para un niño de nueve años que padecía meningitis[28].

En este escenario, cabe preguntarse ¿puede incluirse esa conducta dentro de los llamados delitos informáticos? ¿No estaríamos estrictamente ante un asesinato en grado de tentativa cometido mediante las TIC? Para BRENNER, de haberse producido el resultado, se trataría de un asesinato, ergo, de la migración de un delito tradicional a la red[29]. Este supuesto nos obliga a preguntarnos ¿qué es el cibercrimen? Para el Diccionario Jurídico de la RAE se entiende como la infracción penal cometida utilizando un medio o instrumento informático[30].

---

[26] KLEVE, P., De Mulder, R., y VAN NOORTWIJK, K, "The definition of ICT Crime", *Computer Law & Security Review, vol. 27, no. 2,* [en línea], 2011, 162–167, p. 163. Consultado el 22 de julio del 2021. Disponible en: www.sciencedirect.com.

[27] Para MIRÓ LLINARES, *op. cit.,* p. 34, SIEBER fue el pionero en introducir el tema con su monografía *Computerkriminalität und Strafrecht*.

[28] BRENNER, Susan W., "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare", *Journal of Criminal Law and Criminology*, no. 97, United States of América, Northwestern University School of Law Scholarly Commons, 2007, 379-476, p. 384.

[29] *Ídem.* En el mismo sentido coincide DE LA MATA BARRANCO, Norberto, "Los delitos vinculados a la tecnología de la información y comunicación", en ECHANO BASULDA (Dir.), *Delito e informática: algunos aspectos, Cuadernos Penales José María Lidón,* no. 4, Bilbao, Publicaciones de la Universidad de Deusto, 2007, 13-41, p. 42.

[30] Muñoz Machado, Santiago (Dir.), *delito informático*, en *Diccionario Panhispánico del Español Jurídico,* Madrid, RAE/ Cumbre Judicial Iberoamericana, Consejo General del Poder Judicial-Santillana, [en línea],

Esa breve definición permite *per se* poner en contexto la problemática conceptual del asunto, porque al tenor de ella podemos incluir la tentativa de asesinato arriba descrita como cibercrimen, en la cual la computadora figuraría como **un medio** para cometer **la infracción penal**. Así pues, si el cibercrimen fuera todo delito tradicional cometido por medio de las TIC su concepto desde ya carecería de autonomía y especialidad en el ámbito jurídico.

A. CRITERIO DELIMITADOR

En el año 1991 Gutiérrez Francés propuso como criterio delimitador de la delincuencia informática, atender a la **especialidad** o **especificidad** del ordenador, respecto a su **operatividad y funciones** propias más importantes, es decir: el procesamiento y transmisión automatizada de datos y la confección y/o utilización de programas para tales fines[31]. Operatividad que se desempeña en cinco fases y que puede ser objeto de diversos ataques: "la fase de entrada de datos *(input)*, programación *(programming)*, procesamiento de datos *(data processing)*, la fase de salida de datos *(output)* y la comunicación electrónica"[32], entre los ataques que se pueden presentar, está la manipulación de los datos, supresión de los existentes y extracción de información.

En ese sentido, concordamos con la autora primeramente en la necesidad de delimitar el ámbito de estudio de la delincuencia informática; en segundo lugar, en usar la operatividad del sistema informático como criterio delimitador de esta delincuencia, porque a través de dicho criterio podemos excluir muchas conductas que no merecen un tratamiento penal –ni criminológico– diferenciado. En ese sentido, podemos afirmar que la delincuencia informática se circunscribe a aquellas infracciones penales que se cometen operando un

---

© 2020. Consultado el 23 de julio del 2021. Disponible en: https://dpej.rae.es/lema/delito-informático. Cabe aclarar que La RAE usa indistintamente los términos ciberdelito y delito informático.

[31] GUTIÉRREZ FRANCÉS, María Luz, *Fraude informático y estafa*, p. 57 y 58.

[32] Ibidem, p. 64. Esta misma operatividad del sistema informático se describirá en el apartado B de nuestra investigación.

sistema informático, ya sea que la acción recaiga sobre el mismo sistema o sirva solamente como medio para lesionar otro bien jurídico.

B. DENOMINACIÓN

Después de delimitar el ámbito de estudio de este tipo de delincuencia, surge la necesidad de encontrar un término que logre englobar estas conductas. Las primeras discusiones doctrinales en torno a su denominación encontraban su primer óbice en el uso del término **delito**, debido a que éste hace referencia a una realidad jurídica positiva[33], realidad que no existía a principios de los años noventa. Los argumentos versaban en que, para hablar de la existencia de **delitos informáticos,** *prima facie*, se tenían que limitar estrictamente a aquellas conductas que se encontraban tipificadas en la legislación penal vinculadas a las computadoras, de conformidad con el **principio de legalidad penal** y por la propia definición de delito establecida en los códigos penales o leyes especiales, es decir, que la acción fuese típica, antijurídica y culpable.

En segundo término, se tenía que buscar el denominativo "**delitos informáticos o ciberdelitos**", denominación que no existía en los ordenamientos jurídicos, como por ejemplo en el nicaragüense, pues tampoco existía ningún título relativo a los **delitos informáticos** como grupo de tipos penales sistematizados[34]. Por tanto, no existía tal denominación en sentido normativo, empero, sí existía esta delincuencia como realidad criminológica.

Con mucha certeza se razonaba que si a nivel doctrinal se hablase de delitos informáticos estrictamente como realidad jurídico-positiva, se dejaría a fuera la realidad social, en la cual existen conductas delictivas vinculadas a los sistemas informáticos que no se encontraban aún tipificadas pero merecían su penalización de *lege ferenda*; de tal modo que, para

[33] Véase HERNÁNDEZ DÍAZ, Leyre, "El delito informático", *EGUZKILORE: Cuaderno del Instituto Vasco de Criminología*, Número, no. 23, Fundación Dialnet [en línea], 2009, 227-243, p.235. Consultado el 24 de julio del 2021. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3343365.

[34] Principalmente porque los códigos penales sistematizan los delitos según el bien jurídico protegido.

abarcar las conductas típicas y las merecedoras de penalización, GUTIÉRREZ FRANCÉS propuso utilizar un término menos rígido como el de **criminalidad informática,** para que resaltara, además, el carácter criminológico del fenómeno[35]**.**

En ese orden de ideas, para HERNÁNDEZ DÍAZ, la doctrina hoy mayoritaria, al internar eludir el término **delito** por la problemática señalada, ha recurrido a las expresiones de delincuencia informática o criminalidad informática, "para incluir en ellas todos los comportamientos en los que un sistema informático sea el medio para lesionar un bien jurídico, cualquiera, y todos aquéllos en que dicho sistema sea él mismo el propio objeto sobre el que recae la acción delictiva"[36].

Estas denominaciones "delincuencia informática o criminalidad informática", representan una primera generación del fenómeno criminológico en la que, en palabras de MIRÓ LLINARES, lo característico era el uso de los ordenadores para la comisión de delitos, a la cual le ha sucedido una segunda generación cuya característica central es que el delito se comete a través de Internet y, concuerda con WALL en que existe, una tercera en la que los delitos están absolutamente determinados por el uso del internet y las TIC[37]. Y de ella deviene la denominación **cibercrimen o cibercriminalidad.**

En las primeras líneas del presente apartado 5, título II, se mencionó la evolución fenomenológica y nominal de estas conductas en EEUU, hasta asentarse el término *cybercrime;* de la misma manera, ello ha migrado al idioma español, razón por la cual actualmente se expande el uso del prefijo ciber proveniente del anglicismo *cyber* para crear, bajo la propia recomendación de la RAE, nuevos términos pertenecientes al ámbito de las

[35] GUTIÉRREZ FRANCÉS, María Luz, *Fraude informático y estafa*, p. 52-53.

[36] Hernández Díaz, Leyre, "El delito informático…*", op., cit.,* p. 237.

[37] Véase Miró Llinares, F., *op., cit.*, p. 37 y ss., citando a Wall, D., *Cybercrime: the transformation of crime in the information age*, Cambridge, Polity Press, 2007, pp. 44 y ss. Conviene mencionar que el Internet es entendido acá como un sistema global de información y comunicación basado en un protocolo que une ordenadores de todo el mundo y permite el acceso a cualquiera de ellos para obtener e intercambiar información de manera sencilla.

comunicaciones por Internet[38]. A partir de ello se justifica nuestra preferencia por el uso de la denominación de cibercrimen.

El criterio de que en el cibercrimen solo se incluirían las conductas cometidas a través del Internet, hace excluir aquellas conductas en las que el acceso no autorizado al sistema informático se podría presentar sin el uso de internet, acción que es claramente posible[39]. Si esa conducta fuera excluible del cibercrimen como realidad normativa, en nuestra opinión, dicho criterio no sería funcional para analizar la realidad jurídica del fenómeno[40].

El motivo por el cual MIRÓ LLINARES considera que el uso de Internet debe ser el elemento delimitador de la cibercriminalidad, en primer lugar, estriba en que el uso de este espacio digital se ha popularizado a escala planetaria que potencia el riesgo respecto a la afectación de bienes jurídicos tradicionales por medios más complejos, que hace dudosa la capacidad de los tipos penales existentes para combatir esta criminalidad, pero también -y en segundo término- porque ha propiciado la aparición de nuevos comportamientos nocivos que solamente pueden realizarse en este espacio digital[41], como, por ejemplo, el ataque informático distribuido de denegación de servicios (en inglés *distributed denial of service o DDos*, por sus siglas)[42].

---

[38] RAE, *Ciber*, en *Diccionario panhispánico de dudas*, [en línea], 2005. Consultado el 5 de julio del año 2021, disponible en: http://lema.rae.es/dpd/srv/search?id=tb7u92tGpD6zzdh481. En el mismo sentido se ha sugerido en el idioma inglés por OXFORD UNIVERSITY, *Cyber*, en "*Oxford English and Spanish Dictionary, Synonyms, and Spanish to English"*, [en línea], 2021. Consultado el 5 de julio del 2021, disponible en https://www.lexico.com/en/definition/cyber-.

[39] Ello se puede extraer de la afirmación que hace MIRÓ LLINARES en cuanto a que el acceso al sistema que tenga un *insider* no puede ser considerado un cibercrimen, ya sea en sentido amplio o restringido, sino es cometido a través de internet, véase MIRÓ LLINARES, *op., cit.*, p. 42.

[40] Sin embargo, debe tomarse en consideración, como el mismo autor señala, que su estudio sobre el cibercrimen es propiamente desde una perspectiva criminológica, no normativa.

[41] *Ibídem*, *op., cit.*, p. 26 y ss.

[42] Una forma de ataque (usualmente) a un servicio de internet que tiene como propósito evitar que el servicio opere correctamente, a menudo bombardeándolo con más información de la que este puede procesar, según RIGDON, John C., *DDos*, en *op., cit.*

Aunque discrepemos de MIRÓ LLINARES respecto la exigencia del uso del internet como criterio delimitador, consideramos importante su perspectiva, en tanto que este criterio pone de manifiesto un elemento que cada día más está presente en estos delitos, y que, por su transnacionalidad plantea los conflictos de aplicación espacial de las normas[43].

Llegados a este punto, vale plantearse lo siguiente ¿Si A amenaza con matar a B vía *Facebook Messenger*, estaremos frente a un cibercrimen? De acuerdo, con los criterios expuestos de GUTIÉRREZ FRANCÉS y MIRÓ LLINARES, dicha conducta sería considerada dentro de la categoría de criminalidad informática o cibercriminalidad. Por ese motivo, BRENNER insiste en que se tratan de simples conductas tradicionales que únicamente han emigrado a internet[44]. Sin embargo, hay que recordar que existen algunas conductas que pueden concebirse únicamente por la aparición de las TIC.

Ante esa circunstancia, para MIRÓ LLINARES el término cibercrimen puede emplearse en sentido amplio y restringido[45], en el primero se incluirían cualquiera de esos tipos penales que permitan cometerse a través del uso de las TIC y, el segundo, se refiere a conductas que solo pueden cometerse en la Red.

Por su parte, la LECD define al ciberdelito como las "Acciones u omisiones, típicas, antijurídicas, continuas o aisladas, de carácter penal, cometidas en contra de personas naturales y/o jurídicas, utilizando como método, como medio o como fin, los datos, sistemas informáticos, Tecnologías de la Información y la Comunicación y que tienen por objeto lesionar bienes jurídicos personales, patrimoniales o informáticos de la víctima".

---

[43] Este criterio también podría tomarse como una circunstancia agravante, de *lege ferenda*, cuando la conducta tradicional o novedosa a la luz de la ciberdelincuencia, sea cometida valiéndose de las ventajas del uso de las redes telemáticas.

[44] BRENNER, Susan W., *loc. cit.*, "At Light Speed: Attribution and Response…", p. 383.

[45] Véase MIRÓ LLINARES, *op., cit., p. 42. Confr.*, MAYA, Ricardo Posada, *loc. cit., p.* 93, quien plantea que existen delitos informáticos en sentido amplio y en sentido estricto o cibercrimen como tal, pero coincide en que es el uso del Internet lo que determina este tipo de criminalidad.

Con esta definición se reconoce al ciberdelito como una realidad jurídica positiva. A su vez, se le concibe en sentido amplio y restringido[46].

Si bien es cierto, el aspecto controversial del tema radica en si el ciberdelito o cibercrimen **debería o no** ser una categoría normativa. En nuestra consideración, si se apuesta por la existencia de los cibercrímenes como categoría delictiva, el medio empleado no debería ser el componente determinante para su configuración, pues la acción penal debe definirse por el fin perseguido y la lesión causada[47]. Nuestro legislador, lamentablemente, ha incurrido en ese error, tipificando supuestos **nuevos delitos** únicamente por el medio empleado, cuando las conductas incluidas en la LECD podían encuadrarse en los tipos penales existentes en el Código Penal de Nicaragua (CPNic), a como se dejará en evidencia en el siguiente cuadro.

Código Penal de Nicaragua[48]	**Ley Especial de Ciberdelitos**
"**Art. 219 Hurto simple** Quien se apodere ilegítimamente de una cosa mueble total o parcialmente ajena será penado con prisión de seis meses a dos años y de noventa a ciento veinte días multa, siempre que el valor de la cosa hurtada sea mayor a la suma resultante de dos salarios mínimos mensuales del sector industrial".	"**Artículo 15 Hurto por medios informáticos.** El que, por medio del uso de las Tecnologías de la Información y la Comunicación, se apodere de bienes o valores tangibles o intangibles de carácter patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro, siempre que el valor de lo hurtado sea mayor a la suma resultante de dos salarios mínimos mensuales del sector industrial será sancionado con prisión de dos a cinco años y trescientos a seiscientos días multa".

[46] No obstante, conforme a ella, serán ciberdelitos únicamente las conductas sancionadas en dicha ley.

[47] Véase GUERRERO BARRANTES, Elizabeth, y SALAZAR RODRÍGUEZ, Luis Alonso, "Comentarios críticos a la reforma del código penal que introduce la ley 9048 (sobre delitos informáticos en el derecho penal costarricense)", *Revista Judicial*, no. 112, San José, Universidad de Costa Rica, 2014**,** 247-257, p. 250. Disponible en: https://www.kerwa.ucr.ac.cr/handle/10669/81537. Quienes expresan que existen tipos penales que no por el hecho de cometerse con intervención de un elemento informático deben tipificarse como un delito informático.

[48] Ley No. 641, "Código Penal de la República de Nicaragua". En la Gaceta, Diario Oficial de No. 5, 6, 7, 8 y 9 de mayo del año 2007.

En este cuadro comparativo se ilustra que la acción prevista en ambos supuestos consiste en **apoderase** y el objeto de la acción recae, en el Código Penal, en **cosa mueble,** mientras que en la LECD recae sobre **bienes o valores.** En este punto, efectivamente, existe una variante por el uso de los términos **bien** y **cosa,** esto debido a que técnicamente el concepto de cosa no abarca a los bienes inmateriales[49], por ese motivo, se prefiere el uso del término **bien** para abarcar a los tangibles como intangibles. En este contexto, lo pertinente era actualizar la definición del hurto en el CPNic, más no la creación de un nuevo tipo penal, habida cuenta que lo sustancial en la tipificación de la LECD sobre el hurto informático es el medio a través del cual es cometido, siendo las TIC.

Ahora bien, es útil preguntarse ¿si la doctrina penal mayoritaria y la evidencia normativa indican la inviabilidad del ciberdelito como categoría jurídica, por qué se ha difundido su regulación especial a nivel mundial? Para KLEVE y VAN NOORTWIJK la razón más probable de ver a la criminalidad de las TIC como un área de problema es por el temor de que la tecnología de la información guíen a formas de criminalidad que caigan fuera del rango, de control de las autoridades estatales, de manera tal que no es posible hablar de la delincuencia de las TIC como una disciplina legal independiente[50].

Lo expuesto hasta este momento nos permite sostener que la cibercriminalidad, como fenómeno criminológico, es real, así como la existencia de ciertos tipos penales que son propios de las TIC (cibercrímenes en sentido estricto). Por otro lado, a pesar de que en esta investigación no nos propusimos un estudio pormenorizado de los tipos penales de la LECD, es evidente que la mayoría de las conductas podrían ser subsumidas en las disposiciones de nuestro Código Penal vigente, por tanto, si lo que se pretendía era actualizar el lenguaje técnico jurídico, perfectamente pudo haberse cumplido esta tarea en

[49] Sobre esta preferencia véase el comentario del art. 598 del Código Civil**,** en el cual se establece que **"**Se suprime el término "las cosas" y se agrega la expresión "los bienes", ya que el concepto de cosa jurídicamente no abarca los bienes inmateriales", en Decreto Legislativo, "Nuevo Código Civil de Nicaragua". En la Gaceta, Diario Oficial, del 11 de diciembre de 2019, No. 236, pp. 10890-11230.

[50] KLEVE, P., De Mulder, R., y VAN NOORTWIJK, K, *loc. cit.,* p. 167.

una reforma a los tipos penales existentes, además de la inclusión de circunstancias agravantes.

6. CIBERESPACIO

La idea del ciberespacio ha significado para el Derecho Penal una fuente de controversia respecto de uno de sus grandes postulados, como lo es la **teoría del lugar de comisión del delito**, puesto que existe una tendencia doctrinal que concibe al ciberespacio como un lugar indeterminado, como si se tratase de un lugar fuera de este mundo[51]; circunstancia que llama, a criterio de GUTIÉRREZ FRANCES, al "replanteamiento de los postulados más tradicionales de instituciones bien consolidadas en nuestra disciplina"[52]. Debido a esta tendencia resulta imperante, entonces, más que definir el ciberespacio, desentrañar qué es en realidad.

RINCÓN RÍOS concibe el ciberespacio como un "…nuevo continente, este nuevo espacio del espacio se configura a través de la red; invisible, inexistente, real, el ciberespacio está ahí y por él transitamos sin movernos"[53]. Esta definición pone de relieve la concepción del ciberespacio como algo etéreo y al mismo tiempo como terrenal, puesto que por una parte RINCÓN RÍOS expresa que el ciberespacio es invisible e inexistente, y por el otro, afirma que es un espacio real, lo cual es excluyente, pues lo que **no existe**, simplemente **no es.**

No obstante, conviene resaltar a partir de la concepción de RINCÓN RÍOS que este nuevo espacio se configura a través de la red. De ahí, parece que lo más viable es comprender en primer término la definición y funcionamiento de la red informática para aproximarnos a una comprensión sobre la naturaleza del ciberespacio.

---

[51] Para el origen de este debate, véase CLOUGH, Jonathan, *Principles of Cibercrime*, New York, Cambridge University Press, 2010, p. 17.

GUTIÉRREZ FRÁNCES, María Luz, "Reflexiones sobre la ciberdelincuencia hoy (en torno a la Ley Penal en el espacio virtual)", *Revista Electrónica de Derecho de la Universidad de La Rioja*, vol. 1, no. 3, 2005, 69-92, p. 77.

[53] RINCÓN RÍOS, Jarvey, *El delito en la cibersociedad y la justicia penal internacional*. Madrid, Universidad Complutense de Madrid, 2015, p.40. Disponible en: https://eprints.ucm.es/id/eprint/33360/.

Para TANENBAUM y WETHERALL las redes informáticas suponen una serie de sistemas informáticos (por tanto, no sólo ordenadores) conectados entre sí por medio de dispositivos físicos que envían y reciben información a través de cualquier medio hábil para el transporte de datos, con la finalidad de compartir recursos y ofrecer servicios[54]. Dentro de estas redes se encuentra el Internet, siendo la red global más popularizada.

A través del uso de estas redes informáticas (incluido el internet) el ser humano ha establecido conexiones interpersonales en donde no solamente se transmite información, sino que han creado espacios comunitarios, de comercio y de expresión política, con la diferencia que se realizan en un ambiente virtual; a ello es lo que se le denomina el **ciberespacio[55].**

En ese orden de ideas, aparece entonces **lo virtual** como un sinónimo del ciberespacio[56]. Generalmente, el término virtual evoca a algo imaginario, concepción con la cual no coincidimos. Lo virtual, explicado por LÉVY, acontece de la siguiente manera: "Cuando una persona, una colectividad, un acto, una información se virtualizan, se colocan «fuera de ahí», se desterritorializan [s*ic*.]. Una especie de desconexión los separa del espacio físico o geográfico ordinario y de la temporalidad del reloj y del calendario. Una vez más, no son

[54] TANENBAUM, Andrew S., y WETHERALL, David J., *Redes de computadoras*, 5ª edición, traducción al español por Alfonso Vidal ROMERO ELIZONDO, Ed. Pearson Educación, México, 2012, p. 2.

[55] En ese mismo sentido lo concibe *ídem*, p. 144, quien además expresa que Internet no es lo mismo que ciberespacio, pues este último abarca la totalidad de las conexiones interpersonales por las redes telemáticas, en donde el Internet, es solamente un espacio más de interconexión. Ello entra en plena armonía con la visión de GONZÁLEZ HURTADO, J. A. *op. cit*. P. 37, para quien en el concepto de ciberespacio giran otras ideas relacionadas con campos más allá de la informática y las redes como pueden ser el político, el filosófico, el comercial o el jurídico. Para efectos funcionales usaremos de manera indistinta el término de internet para referirnos al ciberespacio al ser un principal catalizador de éste.

[56] Con lo cual coincide MIRÓ LLINARES, *op., cit.*, p. 146, y explica –aunque no concuerda con ello- que normalmente el concepto de espacio virtual se utiliza como como antitético del especio real y a nuestro parecer no es la forma correcta de concebirlo. Sobre este punto nos pronunciaremos sucesivamente.

totalmente independientes del espacio-tiempo de referencia, ya que siempre se deben apoyar sobre soportes físicos y materializarse aquí o en otro sitio, ahora o más tarde"[57].

Esta explicación permite establecer una concepción de **lo virtual** dependiente de soportes físicos que materializan la interacción en el ciberespacio. A lo que nos referimos acá es que esa convivencia en el espacio virtual se hace posible a través de una infraestructura física, como: la fibra óptica, estaciones de base móviles, equipo físico en satélites, entre otros[58], que fungen como medios de transmisión de los datos electrónicos. Visto de esta manera, el ciberespacio o la comunidad virtual, no es más que una metáfora geográfica o social que permite entender el sentido y alcance funcional de lo que, en última instancia, no son más que circuitos de señales electrónicas que contienen información codificada[59] (en ceros y unos). Lo particular en esto es que en el ciberespacio hay una reducción de la percepción del espacio-tiempo. Por ejemplo, una video conferencia sostenida por dos personas vía *Skype* acontece materialmente, es decir, existe la conversación en el plano físico entre dos personas, lo que hacen los medios electrónicos es conducir la imagen y voz del lugar de la digitalización de éstas hacia el ordenador receptor (desterritorialización) y viceversa.

En este contexto, en el ciberespacio interactúan, entonces, las proyecciones de dos cuerpos tangibles y sonoros; de cierta manera el interlocutor y receptor tienen una presencia en **un lugar**¸ pues su conversación produce efectos externos, de la que podrían derivar conductas ilícitas como amenazas o coacciones, por ejemplo. Lo que sucede con este tipo de interacción es su simultaneidad, su unicidad de momentos puede llevar a la impresión de que el ciberespacio es la ausencia de espacio, quizás fruto del equívoco de asimilar la idea

[57] LÉVY, Pierre, *¿Qué es lo virtual?*, Barcelona, Paidós Multimedia, 1999, p. 14.

[58] UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Comprehensive Study on Cybercrime*, Vienna, UNODC, 2013, p. 4. Disponible en https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf., describe que el acceso a internet es posible, entre otras, gracias a una capa de infraestructura pasiva, en la cual se incluyen los componentes mencionados.

[59] MIRÓ LLINARES, *op. cit.*, p. 145.

de espacio a la distancia[60]. En otras palabras, en la era digital la sincronización remplaza la unidad de lugar, mientras que la interconexión sustituye a la unidad de tiempo[61].

Para recapitular, el ciberespacio es una metáfora que se utiliza para denominar la dinámica de interrelación de los usuarios de internet u otras redes telemáticas, en las que convergen para comerciar, socializar, entre otros. Pero dicha comunicación está sustentada en soportes físicos como los cables de fibra óptica, *routers*, satélites, etc.

III. EL LUGAR DE COMISIÓN DEL CIBERCRIMEN

Para frenar el aumento del cibercrimen, los Estados han recurrido, principalmente, al Derecho Penal, ya sea a través de una ley especial o mediante la incorporación de las nuevas conductas a los códigos penales. Sea cual fuera la técnica elegida, la facultad de aplicar su ordenamiento interno para castigar esas conductas, por regla general, se basa en su soberanía para hacer valer las leyes infringidas dentro de su territorio; no obstante, esta facultad territorial se ve mermada por los componentes transnacionales que caracterizan al cibercrimen, porque el *iter criminis* puede desarrollarse en una multiplicidad de jurisdicciones. De ahí, surge la necesidad de establecer en qué lugar se considera cometido el hecho, ya sea para reclamar la jurisdicción o para excluirla[62].

A continuación expondremos las teorías sobre el lugar de comisión del hecho delictivo en el ámbito de las TIC, y en tal efecto, tomaremos como referencia la clasificación aportada

[60] *Ibidem*, p. 146.

[61] LÉVY, Pierre, *op. cit.*, p. 15.

[62] En este sentido, CÁRDENAS ARAVENA considera que, para aplicar el principio de territorialidad, previamente es necesario determinar el lugar donde se considera cometido el delito. Véase CÁRDENAS AREVANA, Claudia, "El lugar de comisión de los denominados ciberdelitos", *Polít. crim.*, n° 6, 2008, 1-14, p. 3. En el mismo sentido coincide MATA Y MARTÍN, *op. cit.*, p. *165*, al referir que, para la tarea de establecer la ley aplicable, es necesaria, en primer lugar, la determinación espacial del hecho delictivo desde el punto de vista jurídico.

por CÁRDENAS ARAVENA[63], quien plantea la posibilidad del ciberespacio como un lugar de comisión del hecho en sentido normativo, así como las teorías tradicionales existentes y las interpretaciones que han merecido a raíz de la aparición de las TICS, como son: **la teoría de la actividad, la teoría del resultado y la teoría de la ubicuidad.**

1. EL CIBERESPACIO VS. EL LUGAR DE COMISIÓN DEL HECHO REAL

CÁRDENAS ARAVENA plantea, aunque tímidamente, la opción de considerar al ciberespacio como un lugar de comisión, sugiriendo que cualquier discusión contraria sería estéril o arcaica; y alude principalmente a que la materia que nos ocupa se caracteriza marcadamente por la ausencia de fronteras[64]. No obstante, dicha autora finalmente descarta esta opción, pues afirma que "no es menos cierto que para los efectos de determinar el derecho aplicable y los tribunales competentes hemos de procurar subsumir esta manifestación cultural en la normativa vigente". En ese sentido, CÁRDENAS ARAVENA descarta dicha posición no tanto por razones teóricas, sino por sanidad legislativa.

Por otro lado, DARAHUGE y ARELLANO GONZÁLEZ proponen una nueva versión del lugar del hecho, a la luz de la evolución tecnológica, denominándolo como "**lugar del hecho real**", al cual definen como "el área definida y determinada en espacio y tiempo donde ocurre un evento o una serie de ellos" [65]. Estos autores sostienen que la información digital, en tanto que representación codificada, se encuentra en uno de tres estados:

[63] Nos decantamos por esta clasificación puesto que, en la bibliografía consultada, es el único autor que centra su estudio del cibercrimen en este aspecto del lugar de comisión del hecho, incluyendo particularmente al ciberespacio como una categoría.

[64] CÁRDENAS AREVANA, *loc. cit.* p. *6.* Tenemos a bien manifestar que este planteamiento se inclina a la idea del ciberespacio que hemos cuestionado en el apartado número 1, es decir, a concebirlo como un espacio ajeno a una realidad física, por tanto, inmaterial. De la misma manera parece interpretarlo GONZÁLEZ HURTADO, J. A, *op. cit.*, p. 267-268, al expresar que CÁRDENAS plantea de forma novedosa esta concepción, aunque finalmente la descarte.

[65] DARAHUGE, María E., y GONZÁLEZ, Luis Arellano, *Empleo de las direcciones virtuales como elemento fundante en las declaraciones de incompetencia por territorialidad*, en Ricardo Antonio PARADA y José Daniel ERRECABORDE (Comp.), *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet*, 1a ed., Buenos Aires, Erreius, 2018, p. 186.

almacenada, en tránsito o en transformación; en cualquiera de ellos, ésta siempre ocupa un lugar en el espacio y es contenida por elementos materiales, de existencia real[66].

Contrario a esta posición, MAYA considera que: "…las acciones digitales o ciberinteracciones son conductas *deslocalizadas* o *desubicadas físicamente*, pues el ciberespacio como realidad virtual es precisamente un ámbito de interacción lógica"[67]. La expresión "deslocalizadas o desubicadas físicamente", parece traducirse en el texto del autor, en un lugar distinto al físico, pues, para él el ciberespacio y los medios informáticos son el ámbito digital en donde tiene lugar la realización lógica del delito[68]. En conclusión, para el referido autor al ciberespacio es un lugar indeterminado y que debe tomarse como tal al momento de incoar un proceso penal[69].

A nuestra manera de ver, la posición de DARAHUGE Y ARELLANO GONZÁLEZ es la más atinada, puesto que, a como se desarrolló en el título I, el ciberespacio, en resumidas cuentas, tiene componentes físicos que hacen posible su existencia y la transmisión de toda la información que en él circula, de ahí que, la actividad ilícita de una persona en la red, desde su inicio hasta final, puede ser rastreada y ubicada en un área geográfica determinada[70].

---

[66] *Ídem.* Además, justifican esta postura en que los electrones o fotones (como transmisores de datos) son partículas y no fantasmas.

[67] MAYA, Ricardo Posada, *loc. cit.,* p. 86.

[68] *Ibídem,* p. 105, en el cual agrega que ni el ciberespacio ni los medios informáticos deben ser considerados solamente como medios o instrumentos de ejecución.

[69] De esta manera, considera que la normativa procesal para determinar la competencia de los hechos es aquella que prescribe: cuando no sea posible determinar el lugar de ocurrencia del hecho o se realice en varios lugares, en uno incierto o en el extranjero, tendrá competencia el juez donde se formule la acusación. Véase *Ídem.,* en referencia al artículo 43 del Código Procesal Colombiano.

[70] Con esto no pretendemos afirmar que la tarea de rastrear y ubicar la actividad ilícita de una persona a través de la red sea una tarea fácil.

2. TEORÍA DE LA ACTIVIDAD

En palabras del Prof. Dr. LUZÓN PEÑA la teoría de la actividad o acción "sostiene como lugar de comisión del delito aquel lugar (en este caso, país) en que se realiza la acción o en que se omite la acción debida"[71]. Esta teoría no se enfrenta con ningún óbice cuando la acción inicia y finaliza dentro del territorio nacional[72]. Empero, la eficacia de esta teoría se ve mermada cuando el acto que inicia la ejecución del delito se da en el país X, pero su consumación acontece en Y[73].

Más allá de los problemas tradicionales de esta teoría, su principal crítica, como destaca MUÑOZ CONDE Y GARCÍA ARÁN, se presenta en los llamados delitos a distancia, en los que la acción y el resultado se producen en lugares distintos[74]. Entre ellos se encuentran, generalmente, los cibercrímenes[75]. Un claro ejemplo de ello sería el ciberataque mediante el denominado gusano *Wannacry*, de tipo *ransomware*, ocurrido el 12 de mayo de 2017, con el cual se inutilizó registros informáticos de computadoras de aproximadamente 150

[71] LUZÓN PEÑA, Diego Manuel, *Lecciones de Derecho Penal: Parte General*, 3.ª ed., ampliada y revisada, con notas de Derecho Penal nicaragüense por los profs. Aráuz Ulloa/ Moreno Castillo/ Vega Gutiérrez, Managua, UCA Publicaciones, 2017, p. 153.

[72] Lo esencial de la formulación de esta teoría se manifiesta en la voluntad, el movimiento corporal, la actuación del sujeto, bien de forma activa u omisiva. Véase DIEZ SÁNCHEZ, J. J. *Ley Penal en el Espacio. Teoría General y Análisis de la Legislación Española*. Tesis doctoral. Universidad de Alicante, p. 385. Disponible en: http://hdl.handle.net/10045/3419

[73] Véase DIEZ SÁNCHEZ, J. J, *op., cit.*, p. 375 y 376, el autor señala que las críticas a esta teoría versan en que el autor respondería únicamente por la acción desplegada en el país que se encontraba, creando impunidad en cuanto a su resultado.

[74] MUÑOZ CONDE, Francisco, y GARCÍA ARÁN, Mercedes, *Derecho Penal: parte general*, 8ª ed., revisada y puesta al día, Valencia, Tirant lo Blanch, 2010, p. 155.

[75] GONZÁLEZ HURTADO, J. A, *op. cit.*, p. 267. En el mismo Sentido MATA Y MARTÍN, Ricardo, *op. cit.*, p. 166*;* CÁRDENAS AREVANA, Claudia. *loc. cit.*, p. 4.

países[76]. En este caso, la actividad ilícita inicio en un país determinado pero el resultado fue en otros.

En ese escenario, de acuerdo con la teoría de la actividad, el ilícito de destrucción de registros informáticos[77] solo podría ser punible en el lugar donde se ejecutó la instrucción informática para inutilizar los registros informáticos, más no en los lugares donde se produjo la inutilización *per se*.

CÁRDENAS AREVANA cuestiona que a esta teoría se ha interpretado tan ampliamente en algunos cibercrímenes que se ha considerado como el lugar de la acción aquel servidor donde se alojan los datos a disposición para que otras personas puedan revisarlo[78]. Sobre esta cuestión resulta interesante traer a colación el criterio del Tribunal de Justicia de la Unión Europea (TJUE)[79] en el caso *Wintersteiger versus Products 4U*[80].

---

[76] BALBOA ROMERO, Francisco José, *Ramsomware, hacking y phishing: conducta típica de daños informáticos*, Trabajo de fin de Grado en Derecho, La Rioja, Universidad de Internacional de la Rioja, 2018, p. 9. Disponible en: https://reunir.unir.net/handle/123456789/6929.

[77] Utilizando como referencia el tipo penal nicaragüense, establecido en el art. 245 del CPNic.

[78] Referente a los delitos de exhibición o de difusión de contenido, CÁRDENAS AREVANA, Claudia. *loc. cit.* p. 8.

[79] Su pronunciamiento es sobre un caso de materia mercantil, pero su solución al caso en litis puede arrojar argumentos de interés en materia penal.

[80] En este caso una empresa radicada en Austria, denominada *Wintersteiger*, demandó la protección sobre su derecho de marca ante los tribunales austríacos con el objetivo de solicitar la cesación del uso de la marca *Wintersteiger* por parte de la empresa *Products 4U*, radicada en Alemania, por el uso publicitario de una palabra clave coincidente con dicha marca en el motor de búsqueda de *Google*, limitado al dominio nacional de primer nivel alemán, es decir, el uso publicitario estaba limitado al sitio web www.*Google.de*. La empresa alemana Products 4U se opuso a la competencia internacional de los tribunales austríacos, alegando que la empresa Wintersteiger debió demandar ante los tribunales alemanes, pues el anuncio publicitario estaba dirigido exclusivamente a ciudadanos alemanes, ergo, el hecho ocurrió en Alemania. asunto C 523/10, resuelto por STJUE de 12 abril de 2012. El texto puede consultarse en: https://curia.europa.eu/juris/document/document.jsf?text=&docid=121744&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=6989572.

En este caso la Corte Suprema de Justicia de Austria presentó una petición de decisión prejudicial ante el TJUE, para que aclarara de qué manera debía interpretarse la expresión "lugar donde se hubiere producido o pudiere producirse el hecho dañoso", con el objetivo de decidir el tribunal competente. Al respecto, el TJUE se planteó la posibilidad de considerar al lugar del servidor como el lugar del hecho causal (lugar de la acción), puesto que, al fin y al cabo, el desencadenamiento del proceso técnico de exhibición por el anunciante se efectúa, en un servidor perteneciente al explotador del motor de búsqueda utilizado por el anunciante. En otras palabras, el proceso de exhibición del contenido ilícito se realiza materialmente en el lugar del servidor del proveedor de servicios (*Google*).

A continuación, el TJUE esgrimió un argumento armónico con la realidad de las TIC, expresando que "…habida cuenta del objetivo de previsibilidad al que deben orientarse las reglas de competencia, el lugar de establecimiento de dicho servidor, dada su incierta ubicación, no podría considerarse el lugar del hecho causal…". Este principio de previsibilidad permite que al momento de su actuar ilícito el demandado pueda prever en qué jurisdicción puede ser demandado y a la víctima determinar fácilmente el órgano ante el cual puede ejercer su acción[81].

3. TEORÍA DEL RESULTADO

Conforme a esta teoría el delito se entiende cometido en donde se produce el resultado típico[82]. Lo imperante conforme a esta teoría es que solamente se toma en cuenta el último momento de la acción criminal, es decir, el de la consumación, prescindiendo así de cualquier otra consideración y, en concreto, del lugar de realización de la acción[83].

[81] Este planteamiento nos parece muy razonable puesto que la ubicación de los servidores de datos de los proveedores de servicio es muchas veces desconocida, el autor del hecho ilícito no tendría idea alguna de en qué país podrían almacenarse esos datos.

[82] CÁRDENAS AREVANA, Claudia, *loc. cit*., p. 8.

[83] DIEZ SÁNCHEZ, J. *op. cit.*, p. 381.

En materia del cibercrimen, CÁRDENAS ARAVENA señala que han surgido interpretaciones extensivas respecto de qué ha de entenderse por resultado; pues algunos lo entienden como la afectación del bien o interés jurídicamente protegido. Ello implica -en opinión de dicha autora- que "...todo ciberdelito tendría un resultado, no existirían los delitos formales, como de hecho lo son aquellos que consisten en el hacer accesibles contenidos considerados ilegales"[84]. Por ejemplo, la difusión de pornografía infantil por medios de las TIC[85].

En síntesis, lo que critica la referida autora es que, en tanto que cualquier nacional de otras jurisdicciones podrá acceder al contenido ilegal, los efectos de la publicación acontecerán en una multiplicidad de territorios, dando lugar a que cualquier país reclame su jurisdicción, amparado en una interpretación laxa del concepto de resultado[86].

Ejemplo de una interpretación laxa de la teoría del resultado, lo podemos apreciar en el caso ***UEJF & LICRA***[87] ***vs Yahoo! Inc***., en el cual *Yahoo!* fue demandado en Francia por exhibir en su sitio web *yahoo.com* una subasta de artefactos nazis. En la resolución del

[84] CÁRDENAS AREVANA, Claudia. *loc. cit*., p. 8; *Confr*. con PLASCENCIA VILLANUEVA, Raúl, *Teoría del delito*, 2da. Reimp., México, Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México, 2000, p. 54, quien aclara que en los delitos formales no existe un resultado material, sino una afectación subjetiva al bien jurídico protegido.

[85] Sancionado como explotación sexual, pornografía y acto sexual con adolescentes mediante pago en nuestra legislación penal en el art. 175, segundo párrafo, del CPNic, reformado por la Ley No. 779, "Ley Integral Contra la Violencia hacia las Mujeres y de Reformas a la Ley No. 641, "Código Penal", en la Gaceta, Diario Oficial No. 19, del 30 de enero del 2014. Nos referimos acá únicamente a la conducta de publicar el contenido.

[86] BRENNER, Susan W., y KOOPS, Bert-Jaap, "Approaches to cybercrime jurisdiction". *J. High Tech. L*, Vol. 4, No. 1, [en línea], 2004, p. 1 y ss. Consultado el 21 de junio del 2021. Disponible en https://www.researchgate.net/profile/Susan-Brenner/publication/ . Expone esta misma interpretación respecto a publicar un sitio web con el referido contenido ilícito, pero en concreto, ella se refiere a que cuando cada persona accede a ese contenido, se está produciendo el efecto del delito, no se refiere específicamente al resultado.

[87] Corresponden a las siglas en francés de La Unión de Estudiantes Judíos Franceses y Liga Internacional contra el Racismo y el Antisemitismo con sede en París, respectivamente.

caso, un tribunal francés ordenó a *Yahoo!* que interrumpiera el acceso a ciudadanos franceses sobre cualquier contenido en su sitio web *yahoo.com* que hiciera apología del nacismo, en virtud de que el Código Penal francés prohíbe el uso de símbolos nazi en su territorio[88].

En la primera audiencia el abogado defensor señaló que *Yahoo*! mantuvo un sitio web en francés (*yahoo*.fr) que cumplía con la ley francesa. Y que los usuarios de Internet que visitan *yahoo.com* realizan un viaje virtual a los EE. UU, por lo que no se puede argumentar que se haya cometido ningún delito en Francia[89]. Por su parte, el referido tribunal sostuvo que, aunque el sitio *yahoo.com* estaba ubicado en un servidor en California, y tal vez destinado a una audiencia estadounidense, se sufrieron daños en territorio francés[90].

El caso *Wintersteiger Vs. Products 4U* podría brindar una solución más viable a este tipo de problemática. En éste, en sus alegatos conclusivos, el Abogado General señaló que, para determinar el lugar de producción del daño, el elemento fundamental es si determinada información tiene visos reales de causar un impacto en un territorio concreto. Es decir, que no basta con que el contenido de la información incurra en un riesgo de infracción, "sino que ha de constatarse la existencia de elementos objetivos que permitan discernir una conducta que por sí misma tenga una vocación extraterritorial. A estos efectos pueden ser útiles diversos criterios, como la lengua en la que se expresa la información, su accesibilidad, o la presencia comercial del demandado en el mercado de protección de la marca nacional" [91].

---

[88] Para más detalles del caso véase COHEN-ALMAGOR, Raphael, "Freedom of Expression, Internet Responsibility, and Business Ethics: The Yahoo! Saga and Its Implications", J Bus Ethics, No. 106, 2012,353–365.

[89] LE MENESTREL, M., Hunter, M., y DE BETTIGNIES, H.-C., "Internet e-ethics in confrontation with an activists' agenda: Yahoo! On trial", Journal of Business Ethics, No. 39, 2002, 135–144, p. 138. Disponible en: https://www.jstor.org/stable/25074828.

[90] *Ibidem*, p. 143.

[91] CRUZ VILLALÓN, Pedro, "Conclusiones", presentadas ante el TJUE, en el asunto C 523/10, del 16 de febrero de 2012, [en línea], párr. 28, 30, 37 y 38. Consultado el 11 de agosto del 2021, Disponible en:

De esto, puede desprenderse que, para efectos de determinar el lugar del resultado, debe tomarse en cuenta un elemento subjetivo y otro objetivo. Así pues, en el subjetivo, se valoraría el *animus* del sujeto que publica un contenido en la web, para determinar su intención respecto de a qué país o países él dirige ese contenido. Y en lo objetivo, mediante un análisis de previsibilidad, determinar si el contenido de la información era susceptible de ocasionar *a priori* un resultado lesivo en otro territorio. Ello se podría colegir a partir de los medios empleados por el sujeto como el dominio de primer nivel del sitio web (*.com; .fr;.ni,* entre otros), el idioma utilizado, la accesibilidad de la información, determinada por la distancia territorial entre los Estados, entre otros[92].

4. TEORÍA DE LA UBICUIDAD[93]

En la actualidad, para LUZÓN PEÑA esta es la teoría mayoritaria preferible político-criminalmente para resolver los problemas clásicos de jurisdicción que surgían con las teorías tradicionales de la actividad y del resultado, los cuales afectaban la finalidad del principio de territorialidad[94]. Ahora, sobre la base de esta teoría el Estado puede fundamentar su jurisdicción en ambos momentos de realización del delito.

A pesar de que la teoría de la ubicuidad fue la solución unificadora de estas dos posturas disidentes, su concepción ha ido evolucionando. Como sucedió en la Sala General del 3 de

---

https://curia.europa.eu/juris/document/document.jsf;jsessionid=10B9E683DA5E00551B85527422DA8DFC?text=&docid=119515&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=5176208.

[92] Para una crítica sobre esta posición de los elementos que podrían restringir el concepto de resultado, Cfr. CÁRDENAS AREVANA, Claudia. *loc. cit.*, p. 10.

[93] Esta teoría ha merecido distintas denominaciones, tales como: teoría de conjunto, unitaria, mixta, teoría de la unidad o equivalencia de lugar, o teoría de la competencia concurrente. Tales denominaciones dejan en evidencia *per se* el significado de esta teoría, en la que se ven involucradas dos posiciones sobre el lugar del hecho: la de la actividad y la del resultado. DIEZ SÁNCHEZ, j. *op. cit.*, p. 382.

[94] Sobre las razones de preferencia de esta teoría véase LUZÓN PEÑA, Diego Manuel, *op. cit.*, p. 153, quien, además, considera que el principio de territorialidad se concibe como el ejercicio de la potestad punitiva para garantizar la seguridad jurídica en todo el territorio del Estado, tanto por los actos como por el resultado de un delito que se produzcan es ese territorio.

febrero del 2005, por la Sala Penal del Tribunal Supremo Español, en la cual estableció como Acuerdo que "el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo…"[95].

En relación con los cibercrímenes, esta interpretación amplia plantearía la posibilidad de incluir como lugar del hecho a aquel Estado en el cual transitaran los datos electrónicos. No obstante, para MORENO VERDEJO resulta irrelevante jurídicamente fundar la jurisdicción de un Estado bajo este presupuesto de ruta telemática, ello como consecuencia obligada de la ausencia de un bien jurídico ofendido en ese lugar de tránsito de los datos[96].

Sobre ello podría contraargumentarse que pueden existir razones jurídicas, como que el curso causal de la acción ilícita se desarrolla parcialmente dentro de su territorio, y político-criminales, como la de prevenir el delito y reafirmar una política basada en la seguridad ciudadana, que podrían sustentar esta postura amplia en los cibercrímenes[97]. No obstante, como se señaló *supra*, el criterio del TJUE pareciera ser la solución más adecuada en pro de los derechos del acusado y de una correcta administración de justicia.

5. TOMA DE POSTURA

Como se ha visto, tanto la acción como el resultado de los cibercrímenes, en su concepción amplia, pueden entenderse acaecidos o manifestados en diversos territorios, ello debido a la estructura del Internet, en el cual los datos electrónicos transitan por distintos territorios, de la misma manera en la que se pueden difundir sus efectos nocivos.

---

[95] TRIBUNAL SUPREMO ESPAÑOL (Sala de lo Penal, asunto primero), Acuerdo del 3 de febrero del 2005. En cuanto al desarrollo jurisprudencial de esta teoría en España, véase MORENO VERDEJO, Jaime, *Algunas Cuestiones acerca de la estafa informática y el uso de tarjetas*, en ECHANO BASULDA (Dir.), *op. cit.*, 180 y 181.

[96] MORENO VERDEJO, Jaime, *op. cit.*, p. 182; en el mismo sentido Cárdenas Aravena, *loc., cit.*, p. 11; MATA Y MARTÍN, *op. cit.*, p. 166.

[97] Aunque esta posibilidad parezca aislada, el Estado de Virginia del Oeste en EEUU prevé en su legislación la facultad de atribuirse el conocimiento de un hecho ilícito si los datos electrónicos transitan por su territorio, véase ampliamente BRENNER, S. W y KOOPS, *op. cit.*, p. 20.

Esto no significa que la acción como tal exista en un ámbito inmaterial, pues, a nuestro criterio la acción, manifestada a través de las instrucciones informáticas, se realizará dentro de un territorio determinado, de la misma manera que el resultado. Aunque el sujeto utilice complejos mecanismos para ocultar su ubicación física, a fin de cuentas, los datos viajarán por los denominados "anclajes de la red con el mundo físico"[98], estos son los cables de fibra óptica, *routers*, etc. Así pues, el ciberespacio, desde el punto de vista jurídico, debe concebirse como un lugar o conjunto de lugares físicos, en el que es posible (sin obviar las dificultades que ello implica) determinar el lugar de acción y del resultado delictivo, sin abandonar el modelo territorial del lugar de comisión del hecho.

Debido al inmanente carácter transnacional de las redes telemáticas, en consecuencia, de las conductas ilícitas cometidas por medio de ellas, la teoría de la ubicuidad es la más completa, pues permite extender el rango de protección estatal en los distintos estadios de la conducta criminal, en concreto, del cibercrimen, todo ello al amparo del principio de territorialidad.

Aunque las fortalezas de la referida teoría no necesariamente impliquen la fórmula decisiva en la resolución de conflictos de jurisdicción, su comprensión y desempeño frente al cibercrimen nos parece indispensable para lograr determinar con propiedad el lugar de la acción y el del resultado en medio de las complejidades de este tipo de delitos.

Insistimos en señalar que determinar el lugar del hecho no es la fórmula definitiva para los conflictos de jurisdicción, sin embargo, debería considerarse el primer paso a tomar en la labor de esa solución, en tanto que constituye un componente del principio de territorialidad. En este sentido, veremos a continuación los criterios adoptados por los

[98] Los terminales, los servidores, los proveedores, las conexiones y la información circulante por todo el mundo, véase FLORES PRADA, Ignacio, "Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia", *Revista Electrónica de Ciencia Penal y Criminología*, No. 17-20, [en línea], 2015, 1-40, p. 8. Consultado el 29 de julio del 2021. Disponible en: http://criminet.ugr.es/recpc.

países miembros del Sistema de Integración Centroamericana (en adelante, SICA) [99] para encarar las dificultades que presenta la referida teoría de la ubicuidad frente a estas conductas transfronterizas.

IV. CRITERIOS PARA LA APLICACIÓN DE LA LEY PENAL EN EL ESPACIO EN LOS PAISES MIEMBROS DEL SICA

Ya expuestas las principales aristas del lugar donde se considera cometido el cibercrimen, es de interés examinar los criterios que adoptaron las legislaciones de los miembros del SICA para aplicar su facultad jurisdiccional frente a los delitos cometidos en el entorno virtual[100]. También consideramos importante anticipar que los países que disponen de una ley especial para combatir la ciberdelincuencia son: El Salvador, Nicaragua, República Dominicana y Belice, mientras que Guatemala, Costa Rica[101], Panamá y Honduras la regulan en sus respectivos códigos penales.

---

[99] De acuerdo con el sitio web oficial del SICA, los países miembros son Belice, Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Panamá y República Dominicana. Véase *Estados Miembros*, Secretaría General del Sistema de la Integración Centroamericana, © *2020*. Consultado el 13 de agosto del 2021. Disponible en: https://www.sica.int/estadosmiembros. Conviene aclarar que el análisis de la legislación nicaragüense se abordará en el V título, con el propósito de desarrollar con amplitud el tema.

[100] Es meritorio advertir que se hará una revisión de los criterios contenidos en leyes contra el cibercrimen y, en aquellos países en los que no se regule a través de una ley especial, se tomarán en cuenta los criterios acogidos por los códigos penales, como normas generales. Para cumplir con el referido objetivo hemos sistematizado los criterios adoptados por dichas legislaciones y los agrupamos bajo un mismo título según sus descripciones, de esa manera utilizamos la misma técnica desarrollada por BRENNER, S. W y KOOPS, *op. cit.*, p. 1 y ss., en su exposición sobre los criterios adoptados por los países de corte anglosajón. Además, cabe mencionar que legislación nicaragüense se estudiará en el IV título.

[101] En el caso de Costa Rica es menester indicar que se aprobó una ley que reforma su Código Penal únicamente en cuanto a la tipificación de las conductas sobre los sistemas informáticos, véase ASAMBLEA LEGISLATIVA DE COSTA RICA, Ley No. 9048, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal", Gaceta N.º 214, del 06 de noviembre del 2012. Disponible en: https://www.imprentanacional.go.cr/pub/2012/11/06/ALCA172_06_11_2012.pdf

1. CRITERIO DE TERRITORIALIDAD

Aunque la doctrina se incline por concebir el ámbito delictivo de los cibercrímenes como un espacio intangible, lo cierto es que algunas legislaciones, basadas en una cosmovisión territorial del delito, mantienen la vigencia de este principio respecto de la actividad delictiva que se desarrolla por medios digitales. De hecho, el Convenio de Budapest, en su art. 22, estatuye que "Cada parte adoptará las medidas legislativas…para afirmar su jurisdicción… cuando el delito se haya cometido: a) en su territorio…". No obstante, como se demostró en el título anterior, decidir cuándo el cibercrimen se ha o no cometido dentro de determinado territorio no es una tarea sencilla, ello se complica más cuando los Estados tienen diferentes perspectivas legislativas para considerar cuándo el hecho se ha cometido dentro de un territorio soberano. A continuación, veremos los distintos factores que los países toman en cuenta para reclamar su jurisdicción basados en el principio de territorialidad.

A. UBICACIÓN DEL ACTO Y/O DEL RESULTADO

La Ley sobre crímenes y delitos de alta tecnología de República Dominicana, en su art. 2, declara que "Esta ley se aplicará en todo el territorio de la Republica Dominicana, a toda persona física o moral, nacional o extranjera, que cometa un hecho sancionado por sus disposiciones, en cualquiera de las siguientes circunstancias: **A)** Cuando el sujeto activo origina u ordena la acción delictiva dentro del territorio nacional" [102].

La manera en la que se encuentra redactada esta disposición se ajusta a la realidad informática, pues, efectivamente, en este tipo de delitos, el sujeto activo, al ejecutar su plan criminal, **origina** un proceso lógico en su computadora y, al teclear una serie de códigos, **ordena** al *software* la ejecución de instrucciones informáticas para producir un resultado lesivo. Así, se observa que dicha norma acoge, entre otras, la teoría de la actividad y

[102]CÁMARA DE DIPUTADOS DE REPÚBLICA DOMINICANA, Ley No. 53-07, "Ley sobre crímenes y Delitos de Alta tecnología", 23 de abril de 2007, pp. 17-40. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf.

presenta una correcta armonía entre la teoría general del delito con el componente informático de los cibercrímenes[103].

En la actualidad, el criterio de Guatemala es el contenido en el art. 4 del Código Penal, el cual dispone que "…este Código se aplicará a toda persona que cometa delito o falta en el territorio de la República o en lugares o vehículos sometidos a su jurisdicción…". Más adelante, en el art. 20, dicha norma aclara que "El delito se considera realizado: en el lugar donde se ejecutó la acción, en todo o en parte; en el lugar donde se produjo o debió producirse el resultado"[104]. Los códigos penales de Costa Rica y Panamá[105] prevén una disposición similar a la de Guatemala, acogiendo de esa manera el modelo tradicional de la teoría de ubicuidad desarrollada en el título II.

---

[103] De la muestra de países estudiados, República Dominicana es el único que desarrolla este lenguaje técnico con relación a la acción cibernética. Aunque, cabe mencionar que en la República de Guatemala, el proyecto de decreto de la iniciativa que dispone aprobar la ley de prevención y protección contra la ciberdelincuencia, propone una fórmula idéntica al criterio legislativo de la República Dominicana, señalando que la aplicación de esta ley será "… extensiva a toda persona física, nacional o extranjera, que cometa un hecho sancionado como delito, en cualquiera de las **condiciones o circunstancias siguientes:** a) cuando el sujeto activo origina, ordena o ejecuta la acción delictiva dentro del territorio nacional" Véase art 3, inciso a. COMISIÓN DE ASUNTOS DE SEGURIDAD DE NACIONAL, Congreso de la República de Guatemala. Dictamen Favorable con Modificaciones de la iniciativa No. 5601, que dispone aprobar Ley de Prevención y Protección contra la Ciberdelincuencia. 18 de noviembre del 2019. Consultado el 16 de agosto del 2021, Disponible en: https://www.congreso.gob.gt/assets/uploads/info_legislativo/dictamen/32a2e-dictamen-5601.pdf.

[104] CONGRESO DE LA REPÚBLICA DE GUATEMALA, Decreto No. 17-73, "Código Penal", Diario Oficial, del 27 de julio de 1973. Disponible en: http://ww2.oj.gob.gt/es/.

[105] Véase art. 20, ASAMBLEA LEGISLATIVA DE COSTA RICA, Ley No. 4573, "Código Penal", Gaceta No. 257, del 15 de noviembre del 1970, versión No. 31, del 24 de junio del 2010. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=5027. Así mismo, el art. 20, ASAMBLEA NACIONAL DE PANAMÁ, Ley No. 14, "Código Penal", de 2007, en Procuraduría General de la Nación, "Texto único del Código Penal de Panamá Actualizado", 2019. Disponible en: https://ministeriopublico.gob.pa/wp-content/uploads/2016/09/CODIGO-PENAL-2019-FINAL-1.pdf. Con la excepción de que el caso de Panamá adopta este criterio específicamente a conflictos con otras jurisdicciones, pues estatuye que "también se aplicará la ley penal a los delitos cometidos en el extranjero, cuando: 1. Produzcan o deban producir sus resultados en el territorio panameño".

Cabe destacar que la fórmula legislativa citada permite incluir en el ámbito de aplicación de dicho código, las modalidades de ejecución inacabada, al apuntar que también se considera realizado en el lugar donde debió producirse el resultado. Por su parte, El Salvador[106] y Honduras[107] aunque se acogen a la teoría de la ubicuidad, no prevén estos supuestos de ejecución inacabada.

Por otro lado, vale destacar que el Código Penal de Costa Rica introduce una aclaración en el postulado del lugar del hecho, según el cual "…El hecho se considera cometido: a) en el lugar que se desarrolló, en todo o en parte, la actividad delictuosa de autores o partícipes". Esta disposición, aplicada a los cibercrímenes, permitiría reconocer la jurisdicción de Costa Rica si, por ejemplo, desde el extranjero se desplegara un ciberataque contra otro país, pero desde el territorio costarricense se brindara algún tipo de ayuda técnica para perpetrar el hecho, en ese supuesto, pues, este país podría atribuirse el conocimiento del cibercrimen[108].

Por otro lado, la ley de ciberdelitos de Belice, si bien adopta la teoría de la ubicuidad, no obstante, introduce una variante y es que el acto delictivo se lleve a cabo: "(a) total o en parte sustancial dentro de su territorio"[109]. La exigencia de que el hecho se realice en parte sustancial dentro de su territorio excluiría la posibilidad de atribuirse la jurisdicción por el

[106] Art. 2, segundo párrafo, estipula: "los hechos punibles cometidos total o parcialmente en el territorio nacional o en los lugares sometidos a su jurisdicción... De igual forma se aplicará la Ley si la ejecución del hecho se inició en territorio extranjero y se consumó en territorio nacional…" Visible en: ASAMBLEA LEGISLATIVA DE EL SALVADOR, Decreto No. 260, "Ley Especial Contra Los Delitos Informáticos y Conexos", Diario Oficial No. 40, tomo 410, del 26 de febrero del 2016. Disponible en https://www.asamblea.gob.sv/decretos/details/2688.

[107] Art. 10, véase CONGRESO NACIONAL DE HONDURAS, Decreto No. 130-2017, "Código Penal", Gaceta Diario Oficial No. 34,940, del 10 de mayo del 2019. Disponible en: https://www.tsc.gob.hn/biblioteca/index.php/codigos/830-codigo-penal-2019.

[108] Una referencia más clara sobre este criterio la encontramos en el art. 2 de la Ley sobre crímenes y delitos de alta tecnología de República Dominicana, la cual dispone que se aplicará: "d) Cuando se caracterice cualquier tipo de complicidad desde el territorio dominicano.

[109] Art. 43, SENATE OF BELIZE, Act. No. 32, "Cybercrime Act", Gazetted, 7 de octubre del 2020. Disponible en: https://www.nationalassembly.gov.bz/wp-content/uploads/2020/10/Act-No.-32-of-2020-Cybercrime.pdf

simple tránsito de los datos por sus servidores, siempre y cuando dicha acción no represente un peligro a sus bienes jurídicos

B. UBICACIÓN DE LOS MEDIOS INFORMÁTICOS

Contrario a la mentalidad legislativa de Belice, la Ley No. 53-07 de República Dominicana sí contempla explícitamente la posibilidad de reclamar su jurisdicción en un cibercrimen "...Cuando el origen o los efectos de la acción se produzcan en el extranjero, utilizando medios que se encuentran en el territorio nacional[110]". Si bien es cierto, esta ley no indica cuáles son esos **medios**, éstos pueden ser los servidores, computadoras, teléfonos, entre otros.

En este sentido, la Ley especial de ciberdelitos de El Salvador, introdujo una disposición más específica, al declarar que dicha ley se aplicará si el hecho se hubiere realizado "…utilizando las Tecnologías de la Información y la Comunicación instaladas en el territorio" [111]. Ya en el Título I se indicó qué dispositivos pueden incluirse dentro de esta categoría de las TIC. Un tema que podría ser objeto de discusión sobre este criterio es lo relacionado al internet satelital. Empero, para BRENNER Y KOOPS la ubicación territorial de los satélites es su estación terrestre, la cual contaría como una computadora, por lo tanto, se rige por el principio de territorialidad[112].

C. UBICACIÓN DEL CENTRO DE INTERESES

Vale la pena resaltar que la legislación de Belice es la única que hace referencia a la aplicación de su ley cuando el hecho se lleve a cabo: "b) contra la condición de personas, o intereses en cosas, presentes en su territorio". Este criterio, al igual que los demás

[110] Art. 2 inciso d.

[111] Art. 2, segundo párrafo.

[112] BRENNER, S. W y KOOPS, *op. cit.*, p. 16-17. De acuerdo con dichos autores, en la Convención de Budapest, se valoró, inclusive, incluir una disposición que requiriera a los países ejercer su jurisdicción referente a los satélites registrados bajos sus nombres, pero para los redactores esa cláusula era innecesaria porque toda comunicación satelital se originará desde y/o será recibida en la tierra.

adoptados por Belice para afirmar su jurisdicción frente al cibercrimen, parece tener su origen en el Derecho Norteamericano[113].

Para contextualizar este criterio con la legislación en estudio, puede plantearse como ejemplo que un periódico digital nicaragüense difunde información falsa de un empresario X residente en Belice, alegando que este se ha involucrado en actos de corrupción en dicho territorio para lograr posicionarse como una de las empresas con más ganancias en ese país, lo cual le ocasionó un perjuicio a la reputación profesional de X en Belice, en tanto que sus socios nicaragüenses cesaron sus inversiones con dicha empresa[114]. En este supuesto, la conducta no se realizó en Belice, ni se consumó, en sentido material, en territorio beliceño, pero evidentemente se produjo un daño contra los intereses del empresario X, que tienen una conexión directa con su territorio[115].

D. UBICACIÓN DEL EFECTO

Para BRENNER y KOOPS, en referencia al derecho anglosajón, es común que los Estados basen su ejercicio de la jurisdicción penal en una conducta que ocurrió en el extranjero pero

[113] Véase la sección No. 402 del AMERICAN LAW INSTITUTE, *Restatement (Fourth) of Foreign Relations Law of the United States, Philadelphia, Copyright © 2018 by the American Law Institute.* Aunque también guarda similitud con el criterio del "centro de intereses" desarrollado por el TJUE en el caso *eDate Advertasing y otros,* en el cual estableció el criterio de que "…en caso de que se alegue una lesión de los derechos de la personalidad mediante el contenido publicado en un sitio de Internet, la persona que se considera lesionada puede ejercitar una acción de responsabilidad por la totalidad del daño causado… ante los órganos jurisdiccionales del Estado miembro en el que se encuentra su centro de intereses…". STJUE, asuntos, C-509/09 y C-161/10, del 25 de octubre del 2011. El texto puede consultarse en: https://curia.europa.eu/juris/document/document.jsf?text=&docid=111742&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=1701079.

[114] Esta conducta ilícita se puede subsumir en el art. 15, sección 4, inciso a) de la Ley de ciberdelitos de Belice.

[115] Consideramos que este supuesto podría estar abarcado por la doctrina del efecto (la cual abordaremos a continuación) ya que es un término muy amplio y la conducta planteada en el supuesto, bien podría ser abarcada por dicha doctrina.

que tuvo un efecto lesivo en el territorio nacional[116]. No obstante, en la muestra de países estudiados en este título, solamente tres legislaciones prevén esta referencia al **efecto** del delito dentro de su legislación, entre ellos están República Dominicana y Belice[117].

En ese sentido, la Ley sobre crímenes y Delitos de Alta tecnología de República Dominicana establece, en el art.2, que se aplicará: "b) Cuando el sujeto activo origina u ordena la acción delictiva desde el extranjero, produciendo efectos en el territorio dominicano". Mientras que la Ley de Ciberdelitos de Belice dispone que se aplicará cuando el acto delictivo se lleve a cabo "(c) fuera de su territorio, pero tiene o se pretende que tenga un efecto sustancial dentro de su territorio" (art. 43). Respecto a esta disposición conviene resaltar dos aspectos. El primero, que, al igual Costa Rica, extiende la aplicación de la ley a las modalidades de ejecución inacabada. El segundo, requiere que el efecto que se produzca o que se pretende producir sea sustancial[118].

2. POR LA PERSONALIDAD

El Convenio de Budapest consagra el principio de **personalidad activa**, al requerir que cada Estado Parte adopte las medidas legislativas para afirmar su jurisdicción cuando el delito se haya cometido: "…d) por uno de sus nacionales…" (art. 22, inc. d). Esta disposición surge de la necesidad de evitar una laguna de impunidad en aquellos supuestos en los que una persona, tras cometer un delito, se refugiare en su país de origen, en el cual rige el principio de no entrega de nacionales frente a otro Estado que lo reclame[119]. Por consiguiente, se impone la obligación de entregar o castigar (*aut dedere aut punere*).

---

[116] *Ibidem*, p. 19.

[117] En el subsiguiente título se verá que Nicaragua es el otro país que prevé esa disposición en su legislación.

[118] Además de ello, cabe resaltar que ambas legislaciones, tanto la dominicana como la beliceña, evitan el uso del término **resultado,** prefiriendo el del **efecto.** Creemos que esta preferencia por el **efecto** viene dada por la problemática de que existen cibercrímenes que no son de resultado o resultativos, como los considerados delitos formales, *exempli gratia*, los de difusión de contenido, donde no existe un resultado material, sino una afectación subjetiva al bien jurídico protegido. Por ello, esta fórmula legislativa vendría a responder de manera acertada a dicha crítica.

[119] LUZÓN PEÑA, Diego Manuel, *op. cit.*, pp. 143 y 144.

Dentro de las legislaciones que se ajustan a esta exigencia se encuentran los códigos penales de Costa Rica[120], Guatemala[121], Honduras[122] y de Panamá[123]. No existe una variante significativa en la manera cómo este criterio es incluido dentro de dichas legislaciones. Por otra parte, es meritorio mencionar que, curiosamente, Belice, El Salvador y República Dominicana, a pesar de contar con una ley especial que regula los cibercrímenes, no contemplan en ella este criterio exigido por la Convención de Budapest.

Además de la nacionalidad del perpetrador, algunas legislaciones prevén la nacionalidad de la víctima como factor para establecer su jurisdicción (**principio de personalidad pasiva**). Guatemala, por ejemplo, aplica su Código Penal "por delito cometido en el extranjero contra guatemalteco"[124]. Costa Rica y Panamá, además de contemplar que el hecho sea cometido contra algún nacional, agregan que sea cometido contra los derechos de éste[125], supuesto que podría aplicarse a aquellos hechos cometidos contra personas jurídicas radicadas en el extranjero, con socios nacionales, por ejemplo. La legislación hondureña pareciera validar esta interpretación cuando requiere que el hecho "…Se cometa contra alguna persona natural o jurídica hondureña o contra sus derechos…"[126] .

En esa misma línea, la ley de ciberdelito de Belice extiende este criterio más allá de los derechos de sus nacionales, exigiendo que el hecho se lleve a cabo "contra las actividades, intereses, condiciones o relaciones de éstos, tanto afuera, como dentro de su territorio"[127]. Por su parte, El Salvador, introduce una variante que dista mucho del criterio de nacionalidad, al establecer que su ley "se aplicará a cualquier persona…por delitos que

[120] Art. 6 numeral 4.

[121] Art. 5 numeral 3.

[122] Art. 9 inciso c.

[123] Art. 20 numeral 4.

[124] Art. 5 numeral 4.

[125] Art. 6 numeral 3. Del Código Penal de Cos Rica y el art. 20 numeral 2 del Código Penal de Panamá.

[126] Art. 9, numeral 1, inciso b.

[127] Art. 43, inciso d.

afecten bienes jurídicos… de sus habitantes …"[128]. Esta disposición no requiere que el bien jurídico lo ostente un nacional, sino que basta el hecho de que sea cometido contra uno de sus habitantes, lo cual quiere decir que la residencia prima sobre la nacionalidad.

3. PRINCIPIO REAL O DE PROTECCION DE INTERESES

"Se habla de principio real, o también de defensa o de protección de intereses, en supuestos en que, aunque el hecho se cometa en el extranjero y con independencia de la nacionalidad de los autores, afecta a intereses o bienes jurídicos importantes para el Estado, y por ello le es aplicable al hecho la ley penal del Estado"[129]. Este principio, por regla general, se aplica a un catálogo preestablecido de delitos que, como se indicó, se estiman que atentan contra bienes estatales.

Los códigos penales de Costa Rica, Honduras, Panamá y Guatemala prevén -aunque algunos no explícitamente- el principio real y despliegan una lista de delitos que atentan contra el Estado. No obstante, en ninguno de dichos códigos se menciona un cibercrimen en sentido restringido o amplio. Tampoco lo hace ley de República Dominicana, pese a regular específicamente la materia de ciberdelincuencia. Por otro lado, Belice y El Salvador sí contienen en su legislación una manifestación del principio real, a como se verá a continuación.

La Ley de Ciberdelito de Belice, declara que se establecerá su jurisdicción cuando el hecho se lleve a cabo: "e) fuera de su territorio por personas que no sean sus nacionales y que esté dirigido contra la seguridad del estado o contra una clase limitada de otros intereses estatales"[130]. No obstante, no contempla cuáles son esos delitos que atentan contra la seguridad o intereses del estado[131]. Mientras que la ley de El Salvador sí contempla algunos

[128] Art. 2.

[129] LUZÓN PEÑA, Diego Manuel, *op. cit.*, p. 145.

[130] Art. 43, inciso a.

[131] Por lo tanto, su interpretación quedaría a la discreción judicial.

supuestos en los que se vería socavada la propiedad o seguridad del Estado[132], *verbi gratia*: la estafa informática[133] y el espionaje informático[134].

V. ANÁLISIS DEL ÁMBITO DE APLICACIÓN ESPACIAL DE LA LECD

De acuerdo con la revisión de la legislación contra los cibercrímenes de los países miembros del SICA se dejó establecido cuáles son los criterios empleados para combatir este tipo de criminalidad, los cuales comparten, en la mayoría de los casos, semejanzas para reclamar sus jurisdicciones frente a los hechos cometidos en el ciberespacio. A continuación, estudiaremos el criterio adoptado por la ley especial de ciberdelitos de Nicaragua y cuáles son sus implicaciones.

1. ÁMBITO DE APLICACIÓN ESPACIAL ILIMITADO

Con relación a su ámbito de aplicación, el art. 2 de la LECD establece: "…La presente Ley es de orden público y se aplicará a quienes cometan los delitos previstos en ésta, dentro o fuera del territorio nacional.". En otras palabras, esta disposición faculta al Estado de Nicaragua atribuirse la jurisdicción sobre cualquier cibercrimen que se cometa en el planeta, habida cuenta que no estipula límite de jurisdicción.

Con un somero estudio del art. 2 podría afirmarse que el legislador incorporó un novedoso criterio de jurisdicción, el cual permitiría al Estado eliminar cualquier atisbo de impunidad que se vislumbre en las complejidades que entraña la comisión de los cibercrímenes. Empero, ya existe una disposición similar en nuestra legislación y la encontramos en el art. 3 de la Ley contra la trata de personas, la cual contempla: "Esta Ley es de orden público y

[132] Véase Art. 2, el cual establece que la Ley "se aplicará a cualquier persona…por delitos que afecten bienes jurídicos del Estado …".

[133] Art. 10.

[134] Art. 11.

se aplicará a quienes cometan el delito de trata de personas, dentro o fuera del territorio nacional y en favor de aquellas personas que resulten afectadas por este delito."[135]

De ahí, el art. 3 de la Ley Contra la Trata De Personas puede considerarse un antecedente legislativo nacional del criterio recogido en el art. 2 de la LECD, en tanto que se utilizó una técnica muy similar. No obstante, en el caso del art. 3 de la Ley Contra la Trata de Personas encuentra justificación en el hecho de que la trata de personas está incluida en el catálogo de delitos cubiertos bajo el principio de universalidad, previsto en el art. 16 inc. f) del CPNic. En cambio, este no es el caso de la LECD. Y pese a que en su exposición de motivos no se establece nada al respecto, sí puede extraerse la justificación del legislador de la exposición de motivos de su iniciativa, en la cual se documenta que:

"la presente iniciativa de Ley Especial de Ciberdelitos es de Orden Público con protección a la seguridad soberana del Estado, y se aplicará a quienes cometan los delitos previstos en la Ley, dentro o fuera del territorio nacional. Esto último se relaciona a que los ciberdelitos son delitos de orden internacional, ya que el *iter criminis* puede iniciarse o consumarse tanto fuera como dentro del territorio nacional"[136].

Aunado a la exposición de motivos de la iniciativa de la LECD, el Magistrado Marvin Aguilar justificó -implícitamente- esta disposición, al señalar que: "…No se debe olvidar que se presentarán en los delitos cibernéticos cuestiones de jurisdicción y competencia. Ejemplo de ello son los hechos ilícitos realizados en un país y cuyos efectos llegan a otro

[135] Ley No. 896, "Ley Contra la Trata de Personas". En La Gaceta, Diario Oficial, del 25 de febrero de 2015, No. 38. En su art. 3 contempla una disposición sobre el ámbito de aplicación muy similar al de la LECD, no obstante, de aquella no se cuestiona el rango de aplicación, debido a que se encuentra dentro del catálogo de delitos del principio de universalidad recogido en el art. 16 del CPNic.

[136] Ver párrafo primero de la Exposición de motivos de la *Iniciativa de la Ley Especial de Ciberdelitos*, Managua, 28 de septiembre del 2020. Disponible en: http://legislacion.asamblea.gob.ni/SILEG/Iniciativas.nsf/xpIniciativa.xsp.

país; o hechos ilícitos realizados en Nicaragua, con efecto en otros países; o en otros países que tienen efecto en Nicaragua…"[137].

Tales supuestos, tanto los planteados en la exposición de motivos de la mencionada iniciativa, como los manifestados por el Magistrado AGUILAR, podían ser solucionados por los principios de territorialidad y extraterritorialidad de la ley, previstos en el CPNic (a como se reflejará más adelante). Dicho esto, pese a que el legislador nicaragüense tuviera la buena voluntad de asegurarse la inexistencia de cualquier circunstancia de impunidad, esta disposición puede ser cuestionada por tener roces con los principios del Derecho Internacional, a como lo desarrollaremos a continuación.

2. EL CIBERCRIMEN: ¿DELITO INTERNACIONAL O DELITO TRASNACIONAL?

No se puede soslayar la controvertida expresión de la exposición de motivos de la iniciativa de la LECD de que los cibercrímenes son de orden internacional, pues ello remite inmediatamente al concepto legal de delito internacional, en los cuales el principio de universalidad encuentra su principal fundamento, habida cuenta de su efecto preventivo[138]. Dicho esto, conviene preguntarse ¿pueden los cibercrímenes considerarse delitos internacionales? de no ser así ¿podría aún justificarse la aplicación de una justicia universal en los cibercrímenes?

---

[137] Dirigirse a los minutos 12:48-13:15 en AGUILAR, Marvin, "Seminario Taller sobre las reformas y adiciones a la Constitución Política, Código Penal, Procesal Penal y Ley 779 de la República de Nicaragua", [video], Managua, 21 de abril del 2021.

[138] Véase BASSIOUNI, M. Cherif, "Jurisdicción Universal para Crímenes Internacionales: Perspectivas Históricas y Práctica Contemporánea" ("Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice"), traducido al español por el Centro de Derechos Humanos, Facultad de Derecho, Universidad de Chile, *Va. J. Int'l.* L., Vol. 42, No. 81, 2001, 1-67, p. 59. Disponible en: https://corteidh.or.cr/tablas/R08116.pdf. Quien sostiene que la jurisdicción universal representa el método más efectivo para frenar y prevenir los crímenes internacionales mediante el incremento de la probabilidad de procesamiento y castigo de sus autores.

Para que una conducta sea elevada a la categoría de delito internacional requiere que su magnitud y gravedad sean suficientemente relevantes y, que, además, respondan a una política o plan de cuando quien ejerce el poder o, bien, la tolera o simplemente no la puede reprimir[139]. Además, esas conductas deben producir o ser capaz de producir violaciones a bienes jurídicos supraindividuales o violaciones masivas o sistemáticas a bienes jurídicos individuales, ya sea por el mismo Estado o con el consentimiento expreso o tácito de éste.

Sumado a ello, se requiere que esas violaciones sean contra los derechos humanos fundamentales, lo cual se traduce en crímenes graves contra los valores jurídicos fundamentales de la humanidad y son, por lo tanto, codificados como crímenes fundamentales internacionales, como, por ejemplo, los contemplados en los artículos 5-8 del Estatuto de la Corte Penal Internacional [140]. Es necesario recalcar, asimismo, que tales acciones se desarrollan en un contexto de marcroriminalidad política, tanto por agentes estatales como no estatales[141].

En ese orden de ideas, los cibercrímenes contemplados en la LECD, en tanto no constituyan graves, sistemáticas y masivas violaciones a los derechos fundamentales de la humanidad cometidas por organizaciones macrocriminales, no pueden ser considerados como delitos internacionales, máxime cuando estas conductas no están contempladas como tal en las normas de Derecho Penal Internacional.

---

[139] CASTILLO MONTERREY, Marcelo Antonio, *Expolio y Recuperación de las Riquezas Nacionales, Nuevos Retos para el Derecho Penal Internacional*, Tesis Doctoral, España, Universidad de Salamanca, 2012, p. 140.

[140] AMBOS, Kai, "Punishment without a Sovereign? The Ius Puniendi Issue of International Criminal Law: A First Contribution towards a Consistent Theory of International Criminal Law", *Oxford Journal of Legal Studies*, Vol.33, No.2, 2013, *293–315*, p. 309.

[141] Sobre la macrocriminalidad política en sentido amplio véase AMBOS, Kai, *La parte general del derecho penal internacional: Bases para una elaboración dogmática*, (trad. de Ezequiel Malarino), Montevideo, Konrad Adenauer Stiftung, 2005, pp. 46 y 47.

Sin perjuicio de lo anterior, para el Prof. AMBOS, los ataques informáticos, por lo general, son las únicas formas de delitos cometidos en el ciberespacio lo suficientemente serias para ser calificadas como crímenes internacionales y, así, quedar cubiertas por una jurisdicción penal internacional como la de la Corte Penal Internacional[142]. Por ataques informáticos o ciberataques se entiende acá el uso de medios técnicos para pelear una guerra contra un enemigo en el ciberespacio[143]. En consecuencia, los actos de guerra cometidos por medios de las TIC quedarían englobados bajo las categorías de delitos internacionales existentes.

Es indiscutible que los cibercrímenes tienen un componente transfronterizo o transnacional[144], debido a la interconectividad de las redes telemáticas y al efecto globalizador de éstas, aún así, se debe ser muy cuidadoso en no confundir esta naturaleza transfronteriza con conductas delictivas elevadas a tipos penales internaciones.

RINCÓN RÍOS, siguiendo la tesis del Prof. SUÑÉ LLINÁS, propone considerar al cibercrimen como un delito global u obicuo[145]. Tomando en cuenta la naturaleza transfronteriza y la complejidad investigativa de estas conductas, bajo esa premisa**,** este autor pretende justificar la aplicación del criterio de universalidad a los cibercrímenes y audazmente evita recurrir a la categoría de delito internacional, en cambio, utiliza la expresión de delito global u obicuo, semejante a la característica del delito transnacional.

Lo cierto es que los delitos internacionales no son los únicos que justifican, en la práctica legislativa, la aplicación de la jurisdicción universal, también los conocidos como delitos

---

[142] AMBOS, Kai, "Responsabilidad Penal Internacional en el ciberespacio" (trad. Lucas Tassara), Barcelona, *Revista para el Análisis del Derecho,* 2015, 1-32, p. 13.

[143] *Ídem.*

[144] De acuerdo con UNITED NATIONS OFFICE ON DRUGS AND CRIME, *op. cit.,* p. 55, entre el cincuenta y cien por ciento de los cibercrímenes con los que se enfrenta la Policía involucran un elemento transnacional.

[145] RINCÓN RÍOS, Jarvey, *op. cit,* pp. 23-24, considera esta propuesta como una solución a corto plazo, mientras que su solución a largo plazo consistiría la modificación de un tratado internacional. En ambos supuestos, considera que la CPI sería la competente, en primera instancia, de conocer tales crímenes.

transnacionales[146]. Es decir, aunque el cibercrimen no se considere un delito internacional, existe la posibilidad de aplicar la jurisdicción universal, siempre y cuando pueda considerársele como delito transnacional. En consecuencia, es pertinente preguntarnos si éste puede incluirse en la categoría de delitos transnacionales o transfronterizos.

De acuerdo con AMBOS, los delitos transnacionales son aquellos que están basados en tratados internacionales, que son objetos de las denominadas convenciones de supresión, como la Convención de la ONU sobre la Tortura, la Convención contra el bombardeo terrorista, las Convenciones sobre las Drogas de la ONU, entre otras[147]. El punto característico de estos delitos -por tanto, diferenciador de los delitos internacionales- estriba en que su criminalización y represión se encuentran sujetas a nivel nacional de los Estados parte, mientras que los internacionales tienen autonomía típica y disponen de un órgano represor a nivel internacional[148].

Otro aspecto que destacar sobre a la naturaleza de los delitos transnacionales es que su represión efectiva puede difícilmente ser ejercida por los Estados respectivos si actúan aisladamente; es necesaria, entonces, una cooperación internacional porque tales actos

---

[146] HUERTAS DÍAZ, Omar, "La sociedad mundial y los delitos transnacionales", *Revista Logos, Ciencia & Tecnología*, Bogotá, Policía Nacional de Colombia, vol. 1, No. 2, 2010, 8-17, p. 14. Considera que "el dato de que un delito sea perseguible bajo el principio de justicia mundial no lo convierte en delito internacional en el sentido estricto propuesto, en primer lugar [Sic] porque esta técnica se emplea también, siendo en realidad éste su ámbito originario, para la represión de los delitos transnacionales o transfronterizos". *Confr.,* AMBOS, Kai, "Judicial Creativity at the Special Tribunal for Lebanon: Is There a Crime of Terrorism under International Law?", *Leiden Journal of International Law* Vol. 24, No, 03, [en línea], 2011, 655–675, pp. 667 y 668. Consultado el 15 de septiembre del 2021. Disponible en: http://journals.cambridge.org/abstract_S0922156511000215. Quien sugiere que la jurisdicción universal en sentido estricto debería ser aplicable únicamente a los verdaderos delitos internacionales.

[147] AMBOS, Kai, "Judicial Creativity…", *loc. cit.,* p 667.

[148] Para AMBOS, las Convenciones de represión antes citadas claramente obligan a los Estados parte a asegurarse de que las conductas prohibidas conforme a estos instrumentos "sean delitos bajo su ley penal, mientras que las Convenciones, como la del Genocidio, contempla claramente los "delitos bajo el derecho internacional", para una perspectiva más amplia de estas diferencias véase *Ídem.*

traspasan las fronteras del Estado o pueden concernir en sus implicaciones a todos los Estados[149].

Con todas estas consideraciones, los cibercrímenes podrían considerarse delitos transnacionales. No obstante, a nuestro criterio esta posibilidad no parece factible en el momento actual, pues, aunque la investigación y represión de tales conductas requiera inexorablemente de la cooperación internacional, los principales instrumentos que los regulan tienen un alcance territorial limitado y su regulación no es uniforme[150].

El Convenio de Budapest, que se ha caracterizado como una guía internacional en la elaboración de leyes contra el cibercrimen y como un marco referencial en temas de cooperación internacional, solo cuanta con sesenta y seis Estados parte y once observadores[151], mientras que la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas, cuenta con ciento noventaiún Estados parte[152]. Esto explicaría el motivo por el cual los académicos del DPI no incluyen a las figuras típicas del cibercrimen dentro de la categoría de delitos transnacionales[153].

En ese orden de ideas, no es sustentable la tesis de que los cibercrímenes sean considerados delitos transnacionales, ergo, tampoco lo es la aplicación del principio de universalidad bajo ese argumento. Sumado a lo anterior, debe tomarse en cuenta que ni los modelos

---

[149] HUERTAS DÍAZ, Omar, *loc. cit.*, p. 13.

[150] Ampliamente *UNITED NATIONS OFFICE ON DRUGS AND CRIME*, p. 62 y ss., donde se identifica que la multiplicidad de ordenamientos nacionales, regionales e internacionales conlleva a disposiciones que se contradicen, generando lagunas de impunidad.

[151] Sobre la lista de países partes y observadores de dicha convención, consúltese *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*. Council of Europe, © 2021. Consultado el 12 de septiembre del 2021. Disponible en: https://www.coe.int/en/web/cybercrime/parties-observers.

[152] *United Nations Treaty Collection*. United Nations, © 2021. Consultado el 12 de septiembre del 2021. Disponible en: https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=VI-19&chapter=6&clang=_en.

[153] Véase AMBOS, Kai, "Punishment without a Sovereign?", *op. cit.*, p. 296; HUERTAS DÍAZ, Omar, *loc. cit.*, p. 14 y ss.

penales de las principales potencias económicas aplican la jurisdicción universal a los cibercrímenes en sentido estricto, ni los tratados internacionales[154].

De acuerdo con COLANGELO: "un solo estado no puede determinar unilateral y subjetivamente qué crímenes están dentro de su jurisdicción universal, esa es una cuestión de jurisdicción internacional, no nacional"[155]. Y en ese sentido, consideramos que la disposición del art. 2 de la LECD no es compatible con los estándares del Derecho Internacional. La consecuencia práctica de una disposición tan amplia como esta, versa en que puede ocasionar fricciones con otras jurisdicciones concurrentes y amenazaría con coartar la soberanía de otros Estados en su espacio geográfico.

Consideramos que la técnica legislativa en la redacción del art. 2 de la LECD obedece a una inadecuada comprensión del lugar de comisión del hecho en los cibercrímenes y de los criterios de aplicación espacial de la ley para enfrentar el fenómeno, puesto que, a como hemos señalado con anterioridad, es amplia la tendencia de asumir al ciberespacio como un lugar inaprehensible[156]. En ese orden de ideas, es necesario preguntarse ¿cómo pueden los tribunales nacionales hacer frente a la ambigüedad del ámbito de aplicación de la LECD? A esta pregunta trataremos de responder a continuación.

---

[154] Véase ampliamente QIANYUN WANG, *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe*, Tesis Doctoral, Erasmus University of Rotterdam, 2016, p. 1 y ss.

[155] COLANGELO, Anthony J., "Double Jeopardy and Multiple Sovereigns: A Jurisdictional Theory", *WASH. U. L, Vol.* 86, No. 4, 769-857, p. 796. Disponible en: https://openscholarship.wustl.edu/law_lawreview/vol86/iss4/1. Sumado a esto debe mencionarse que Nicaragua no ha ratificado la Convención de Budapest.

[156] Esa circunstancia puede reflejarse en el art. 39 de la LECD, en la cual faculta a cualquier Juez de Distrito de lo Penal a autorizar, en la etapa investigativa, actos de investigación para la obtención y conservación de la información contenida en sistemas informáticos. Art. 39, LECD. Contrariamente a lo que contempla el art. 246 del Código Procesal Penal de Nicaragua., en el cual exige que el Juez de Distrito de lo Penal que autorice actos de investigación, deba tener competencia territorial, Ley No. 406, "Código Procesal Penal de la República de Nicaragua", La Gaceta, Diario Oficial, de diciembre del 2021, No. 243 y 244.

3. PROPUESTA DE SOLUCIÓN: CONEXIÓN SIGNIFICATIVA Y *TEST DE RAZONABILIDAD*.

Un estudio exhaustivo sobre el cibercrimen determinó que "Las respuestas de los países no revelan, de momento, ninguna necesidad de formas adicionales de jurisdicción sobre una dimensión putativa de 'ciberespacio'. Más bien, las formas de jurisdicción basadas en la territorialidad y la nacionalidad casi siempre bastan para asegurar una conexión suficiente entre los actos del delito cibernético y al menos uno de los Estados" [157].

Conforme a ello, hay que subrayar dos aspectos, primero, que el principio de territorialidad y el de personalidad han mostrado ser los más viables para enfrentar los desafíos de la jurisdicción en los cibercrímenes y, segundo, que en la aplicación de ambos principios se precisa de una **conexión suficiente y razonable** entre el hecho punible y su jurisdicción[158].

De esa manera, a pesar de que expresamente no exista una remisión de la LECD hacia el CPNic o el Código Procesal Penal de Nicaragua, en cuanto a los criterios de jurisdicción, consideramos que, ante conflictos de jurisdicciones deberían aplicarse las disposiciones de ambas normas generales, pues, tal y como indica la práctica legislativa y judicial de otros Estados, los principios de territorialidad y de personalidad, desarrollados en los arts. 13 y 14 del CPNic, contienen una base sólida para enfrentar los desafíos de jurisdicción. Por consiguiente, nos enfocaremos en las siguientes líneas a desarrollar los puntos de conexión en ambos principios.

---

[157] UNITED NATIONS OFFICE ON DRUGS AND CRIME, *op. cit.* p. 215.

[158] En esta línea QIANYUN WANG, *op., cit.,* pp. 267 y ss.; CLOUGH, Jonathan, *op. cit*, p. 413; asimismo, UNITED NATIONS OFFICE ON DRUGS AND CRIME, *op. cit*., p. 210., expresa que "Un elemento común a todos estos principios es un sentido amplio de exigir que se necesita una 'conexión suficiente' o un 'vínculo genuino' entre el delito y el estado que ejerce jurisdicción." De igual manera, HAYASHI, Mika, "Objective territorial principle or effects doctrine? Jurisdiction and cyberspace", *INT'L LAW*, No. 6, 2006, 284-302, p. 300; ROBERTS, Lynne, "Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An Analysis on Cyber Stalking", *International Journal of Cyber Criminology*, Vol. 2, No., 2008, 271-285, p. 281.

Por puntos de conexión nos referimos a los elementos, efectos, actos, sistemas informáticos, ubicación o nacionalidad de los autores o partícipes, y cualquier otra circunstancia que vincule el hecho ilícito con la jurisdicción del Estado[159]. Estos elementos deben identificarse, en la medida de lo posible, en la aplicación de los principios de territorialidad y personalidad.

En nuestra legislación el principio de territorialidad debe interpretarse en congruencia con el art. 12 del CPNic, el cual contempla que "El hecho punible se considera realizado tanto en el lugar donde se desarrolló, total o parcialmente, la actividad delictiva de los autores y partícipes, como en el lugar donde se produjo o debió producirse el resultado o sus efectos"[160].

Conforme a esta disposición, el **principio de territorialidad** podría aplicarse a delitos consumados en el extranjero pero que se iniciaron en territorio nacional (**ubicación del acto**), así como aquellos hechos iniciados fuera del país pero que produjeron sus resultados en Nicaragua (**ubicación del resultado**); cabe resaltar que la jurisdicción nicaragüense absorbería las **acciones de los partícipes** en ambos supuestos, así como lo establece el Código Penal de Costa Rica y la ley de Belice. Aunado a lo anterior, tal disposición prevé los **supuestos de ejecución inacabada**, de la misma manera en que lo hacen Costa Rica, Panamá y Belice, al establecer que el hecho se considerará cometido también en el lugar donde debió producirse el resultado o sus efectos. Asimismo, esto último nos hace subrayar que el CPNic, a como se anticipó en el título III, acoge la **doctrina de los efectos**, igual que Belice y República Dominicana.

---

[159] UNITED NATIONS OFFICE ON DRUGS AND CRIME, *op. cit*., p. 223, refiere que "…**el alma del debate jurisdiccional está la interpretación de la colocación de los elementos y los efectos del delito dentro de fronteras geográficas**. Ya sea que esto se analice desde la perspectiva de 'actos', 'conductas', 'circunstancias', 'datos' o 'sistemas informáticos', para evitar conflictos jurisdiccionales se debe mantener un umbral lo suficientemente alto para el 'vínculo genuino'…".

[160] Art. 12 CPNic. Asimismo, lo desarrolla el art. 19 del Código Procesal de Nicaragua, al estipular que "La jurisdicción penal se extiende a los delitos y faltas cometidos total o parcialmente en el territorio nacional y a aquellos cuyos efectos se producen en él".

Todos los elementos resaltados líneas arriba son los que deberían identificarse por los órganos jurisdiccionales y sus auxiliares cuando haya que resolver un conflicto de jurisdicción. En nuestra opinión, esta disposición sobre el lugar del hecho es la más completa entre los países miembros del SICA, en tanto que los elementos recogidos permitirían superar los desafíos de aplicación espacial de la ley.

Por otro lado, nos parece loable que el CPNic contenga la doctrina de los efectos, pues con ella se superaría la discusión en torno a los delitos de difusión de contenido ilegal cometidos a través de la red, expuesta ya en capítulos anteriores[161]. Hay que tomar en cuenta, también, la declaración conjunta sobre mecanismos internacionales para la promoción de la libertad de expresión con relación a este tipo de delitos, en la cual sugiere que, al momento de ejercer la jurisdicción, se tomen en cuenta la residencia del autor, el lugar de publicación del contenido y si tal contenido está dirigido al Estado en cuestión[162]. Así pues, todos estos puntos precisarían identificarse al momento de vincular el hecho con la jurisdicción del Estado que la reclama.

Ahora bien, el otro punto de conexión señalado tiene que ver con la **nacionalidad** del autor o de la víctima, acogidos por el denominado **principio de personalidad** activa o pasiva[163], respectivamente. En el caso de Nicaragua, este principio se encuentra recogido en el art. 14 del CPNic, conforme a éste, aunque el hecho sea cometido en el exterior, sin ningún otro vínculo territorial, la ley penal le será aplicable al autor por la única circunstancia de su nacionalidad nicaragüense[164].

---

[161] Aunque lo preferible sería que el art. 12 del CPNic, requiriese que el efecto producido en el territorio nacional sea sustancial o significativo, como sí lo hace Belice.

[162] Relator Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión, *et. al.,* "Declaración conjunta sobre la libertad de expresión e Internet", Organization for Security and Co-operation in Europe, Suecia, 1 de junio del 2011, 1-5, p. 3. Disponible en: http://www.osce.org/fom/78309.

[163] Cabe mencionar que el CPNic no contiene el principio de personalidad pasiva.

[164] En virtud de que el Convenio de Budapest orienta a que los Estados parte tomen las medidas legislativas para afirmar su jurisdicción basados en la nacionalidad del autor del hecho, este es un criterio es válido para determinar la jurisdicción en los cibercrímenes. Véase sección 3, art. 22, inciso d.

Es menester señalar que la aplicación de este principio tiene ciertas restricciones en nuestra legislación, como son la necesidad de la doble incriminación, que la víctima o su representación formalicen la acusación en Nicaragua y el respeto al principio *ne bis in ídem*, lo cual se ajusta a las normas de Derecho Internacional.

Por otra parte, es precisamente la falta de estas restricciones lo que se critica en la aplicación del principio de territorialidad cuando hay componentes transfronterizos en los cibercrímenes[165]. A nuestra manera de ver, ese vacío obedece a que el fundamento de este principio está diseñado para las modalidades delictivas cometidas en el modelo tradicional de territorio.

Producto de este vacío es que pueden presentarse casos en los que se juzguen a personas por difusión en la red de contenido considerado ilícito en un país, pero no en el país desde donde se cargó el contenido[166]. Independientemente de la discusión sobre la parte subjetiva del tipo que pudiera existir en estos casos, se trata, además, del principio de legalidad de reconocimiento internacional. El ciudadano que actúa en el territorio del que es nacional, adecúa su conducta a las leyes nacionales, teniendo así la seguridad jurídica de las repercusiones de sus actos.

No obstante, que un Estado pretenda afirmar su jurisdicción territorial sobre todo hecho que involucre contenido ilegal en la red, aun cuando en el país que se cargó el contenido no era ilegal, significaría asumir una especie de jurisdicción universal, socavando, por tanto, los derechos humanos y la soberanía de otro Estado[167]. En tal sentido, con el propósito de

[165] CÁRDENAS AREVANA, Claudia, *loc. cit.,* p. 11-12.

[166] UNITED NATIONS OFFICE ON DRUGS AND CRIME, *op. cit.,* p. 62, recoge el fallo del *Bundesgerichtshof* alemán, 1 StR 184/00, del 1 de diciembre del 2000, pp.228 y ss., en el cual se declaró culpable un ciudadano de Oceanía por subir a la red de su país material con contenido de discurso de odio, el cual se descargó en Alemania.

[167] De acuerdo con el "Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia". En la Gaceta, Diario Oficial, 4, del 03 de marzo de 2020. A Nicaragua, le estaría limitado el ejercicio de la jurisdicción para investigar y solicitar extradición de

establecer límites a la jurisdicción, consideramos que debería tomarse en cuenta en estos supuestos el principio de previsibilidad objetiva desarrollado en el título II de este trabajo, aplicado por el TJUE, como lo es que se identifiquen en el caso en concreto elementos objetivos que permitan deducir que el autor del hecho podía prever que su acción causaría efectos en determinado país o países.

Esta perspectiva, se enmarca en lo que se le conoce como el estándar de razonablilidad (*reasonableness standard*)[168], principio de razonabilidad[169] o jurisdicción idónea[170], para hacer referencia a la técnica empleada en el año 1970 por los tribunales de EEUU para determinar el impacto o alcance del ejercicio extraterritorial de su jurisdicción, sopesando los intereses nacionales con los intereses del otro Estado y la razonabilidad de ejercer la jurisdicción en los casos concretos[171], técnica que ha tomado mucha acogida tanto por la doctrina[172] como por los instrumentos internacionales, como, por ejemplo, en el art. 22 de la Convención de Budapest, el cual orienta a los países a tomar medidas con el fin de decidir la jurisdicción más adecuada para incoar la acción penal[173].

Esto se compagina con la jurisprudencia del TJUE reiterada en el caso *Wintersteiger vs. Products 4U*, de que la decisión respecto del órgano jurisdiccional competente para conocer el caso, además de identificar la conexión entre el hecho y los órganos jurisdiccionales competentes, se debe justificar bajo las máximas de la buena administración de justicia y de una sustentación adecuada del proceso[174].

---

un ciudadano en estos supuestos, en tanto que el art. 3 de dicho Convenio establecen como requisito para la cooperación la observancia de los principios de *ne bis in ídem* y de doble incriminación.

[168] Denominada así por BRENNER y KOOPS, *loc. cit.*, p, 29.

[169] HAYASHI, Mika, *loc. cit.*, p. 300.

[170] Por FLORES PRADA, *loc. cit.*, p. 27.

[171] HAYASHI, Mika. *loc. cit.*, p. 300.

[172] Por todos: CLOUGH, Jonathan, *op., cit.*, p. 413.

[173] El art. 22, inciso 5, del Convenio de Budapest, indica que "En el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción penal".

[174] Véase *supra* nota 79.

FLORES PRADA ha explicado con profusión la jurisdicción idónea, postulando que por tal se debe "…entender aquella jurisdicción nacional que, en un caso concreto y en concurrencia con otras jurisdicciones nacionales, está en las mejores condiciones para asumir el conocimiento de litigio con la máxima eficacia procesal y con el máximo respeto a las garantías procesales de las partes y víctimas"[175].

Cuando el Estado de Nicaragua se enfrente a los conflictos de jurisdicción, tanto positiva como negativa, en primer término, debería emprender la tarea de identificar los puntos de conexión en el caso en concreto, individualizando los elementos concurrentes, tales como el lugar del acto, del resultado, el efecto, la nacionalidad del autor y la víctima, los intereses de Nicaragua y de las jurisdicciones en conflicto, entre otros.

En segundo término, una vez que se identifiquen estos elementos, debería de elaborar un examen de equilibrio (*balancing test*), en el cual someta al caso en concreto a una jerarquización de esos elementos y que le permita concluir en si el ejercicio de la jurisdicción por el Estado de Nicaragua es apropiado, tomando en cuenta el principio de previsibilidad, de buena administración de justicia y la adecuada sustentación del proceso. Esto se traduciría en identificar si puede acceder o no a los medios de prueba, si está en la disposición de sufragar los costes de una investigación internacional, entre otros, de ser negativo, deberá conceder la solicitud a otro Estado cuya jurisdicción sea la más apropiada para el reproche de la conducta.

VI. CONCLUSIONES

Las TIC, como medio y fin delictivo, han causado un efecto disruptivo en la concepción tradicional del lugar de comisión del hecho, por consiguiente, en la capacidad jurisdiccional de los Estados para hacer cumplir sus leyes penales. Es así como la solución jurídica a esa problemática es una tarea pendiente a nivel global. En esta investigación no ha sido posible

[175] FLORES PRADA, *loc. cit.*, p. 27.

analizar todas las aristas de dicha problemática, sin embargo, todos los aspectos abordados nos permitieron cumplir nuestros objetivos y arribar a las siguientes conclusiones:

1. El conocimiento básico de los distintos componentes que forman parte del funcionamiento de las TIC es indispensable como punto de partida para el análisis de las diferentes problemáticas de la ciberdelincuencia.

2. Aunque no exista un consenso sobre la denominación final de este fenómeno, sí es posible establecer un criterio que delimite su ámbito de estudio, el cual consiste en que la ciberdelincuencia se circunscribe a aquellas infracciones penales que se cometen operando un sistema informático, ya sea que la acción recaiga sobre el mismo sistema o sirva solamente como medio para lesionar otro bien jurídico.

3. En correspondencia con lo anterior, la denominación de "cibercrimen", marcada, principalmente, por el uso de internet, puede interpretarse en sentido amplio y restringido. El primero, además de los delitos puramente informáticos, comprende los hechos tradicionales que pueden cometerse por medio de un sistema informático; y, el segundo, incluye únicamente aquellas conductas que solo son concebibles con el uso de los sistemas informáticos, como los denominados ataques *DDos*.

4. El denominado ciberespacio no es más que una metáfora geográfica empleada, generalmente, para dotar de significado a esa interacción social, comercial o económica que acontece en las redes telemáticas. No obstante, la transmisión de la información digital o electrónica es gracias a sus componentes físicos, como los *routers,* cables de fibra óptica, los centros de base de datos, entre otros (anclajes de red).

5. De acuerdo con lo anterior, la acción delictiva, su resultado típico o sus efectos acaecen materialmente un territorio determinado, aunque el sujeto utilice complejos mecanismos para ocultar su ubicación física, a fin de cuentas, los datos viajarán por los denominados anclajes de la red. Ergo, (sin obviar las dificultades que ello implica) es posible determinar el lugar de la acción y del resultado delictivo, sin abandonar el modelo territorial del lugar de comisión del hecho.

6. En consonancia con esa concepción material, la teoría de la ubicuidad es la más viable en el postulado del lugar de comisión del cibercrimen, pues permite afirmar la vigencia de la ley penal en todas las fases del *inter criminis.* No obstante, no es la solución definitiva a los conflictos de jurisdicción que se pueden presentar en los cibercrímenes dado su carácter transfronterizo.

7. En el breve análisis de las legislaciones en materia de ciberdelincuencia de los países del SICA se logra apreciar que el ámbito de aplicación de sus leyes se basa en una concepción territorial del hecho delictivo y acogen, aunque con ciertos matices, la teoría de la ubicuidad. En algunos casos, también se acogen a la doctrina de los efectos, para solventar así los problemas que se presentan con los delitos de difusión de contenido ilegal, en los cuales se cuestiona la existencia de un resultado típico.

8. En la revisión de la LECD se observó que contiene un ámbito de aplicación espacial de la ley con efecto ilimitado, probablemente producto de una incorrecta comprensión del lugar donde se comete el cibercrimen. A pesar de la intención de evitar lagunas de impunidad, el art. 2 de dicha ley no se ajusta a los estándares del Derecho Internacional y podría crear fricciones con los territorios soberanos de otros Estados.

9. Los órganos de justicia que se enfrente a conflictos de jurisdicción en los cibercrímenes deberían de aplicar de forma supletoria los principios de territorialidad y de personalidad activa, contenidos en los arts. 13 y 14 del CPNic., procurando afirmar o denegar su jurisdicción bajo un estándar razonable, que tome en cuenta los puntos de conexión significativos entre el hecho y el reclamo de jurisdicción del Estado, así como, que coloque en una balanza los intereses y capacidad del Estado de Nicaragua para perseguir y sancionar el hecho de que se trate.

VII. FUENTES DEL CONOCIMIENTO

1. DISPOSICIONES NORMATIVA CITADAS

A. NACIONAL

Decreto Legislativo, "Nuevo Código Civil de Nicaragua". En la Gaceta, Diario Oficial, del 11 de diciembre de 2019, No. 236, pp. 10890-11230.

Ley No. 406, "Código Procesal Penal de la República de Nicaragua", La Gaceta, Diario Oficial, de diciembre del 2021, No. 243 y 244.

Ley No. 641, "Código Penal de la República de Nicaragua". En la Gaceta, Diario Oficial No. 5, 6, 7, 8 y 9, de mayo del año 2007.

Ley No. 779, "Ley Integral Contra la Violencia hacia las Mujeres y de Reformas a la Ley No. 641, "Código Penal", en la Gaceta, Diario Oficial, del 30 de enero del 2014, No. 19.

Ley No. 896, "Ley Contra la Trata de Personas". En La Gaceta, Diario Oficial, del 25 de febrero de 2015, No. 38.

Ley Nº. 1042**, "**Ley Especial de Ciberdelitos**".** En la Gaceta, Diario Oficial, del 30 de octubre de 2020, Nº. 201, pp. 9319-9316.

B. EXTRANJERA

ASAMBLEA LEGISLATIVA DE COSTA RICA, Ley No. 4573, "Código Penal", Gaceta No. 257, del 15 de noviembre del 1970, versión No. 31, del 24 de junio del 2010. Disponible en: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=5027.

ASAMBLEA LEGISLATIVA DE COSTA RICA, Ley No. 9048, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal", Gaceta N.º 214, del 06 de noviembre del 2012. Disponible en: https://www.imprentanacional.go.cr/pub/2012/11/06/ALCA172_06_11_2012.pdf

ASAMBLEA LEGISLATIVA DE EL SALVADOR, Decreto No. 260, "Ley Especial Contra Los Delitos Informáticos y Conexos", Diario Oficial No. 40, tomo 410, del

26 de febrero del 2016. Disponible en https://www.asamblea.gob.sv/decretos/details/2688.

ASAMBLEA NACIONAL DE PANAMÁ, Ley No. 14, "Código Penal", de 2007, en Procuraduría General de la Nación, "Texto único del Código Penal de Panamá Actualizado", 2019. Disponible en: https://ministeriopublico.gob.pa/wp-content/uploads/2016/09/CODIGO-PENAL-2019-FINAL-1.pdf.

CÁMARA DE DIPUTADOS DE REPÚBLICA DOMINICANA, Ley No. 53-07, "Ley sobre crímenes y Delitos de Alta tecnología", 23 de abril de 2007, pp. 17-40. Disponible en: https://www.oas.org/juridico/PDFs/repdom_ley5307.pdf.

COMISIÓN DE ASUNTOS DE SEGURIDAD DE NACIONAL, Congreso de la República de Guatemala. Dictamen Favorable con Modificaciones de la iniciativa No. 5601, que dispone aprobar Ley de Prevención y Protección contra la Ciberdelincuencia. 18 de noviembre del 2019. Consultado el 16 de agosto del 2021, Disponible en: https://www.congreso.gob.gt/assets/uploads/info_legislativo/dictamen/32a2e-dictamen-5601.pdf.

CONGRESO DE LA REPÚBLICA DE GUATEMALA, Decreto No. 17-73, "Código Penal", Diario Oficial, del 27 de julio de 1973. Disponible en: http://ww2.oj.gob.gt/es/.

CONGRESO NACIONAL DE HONDURAS, Decreto No. 130-2017, "Código Penal", Gaceta Diario Oficial No. 34,940, del 10 de mayo del 2019. Disponible en: https://www.tsc.gob.hn/biblioteca/index.php/codigos/830-codigo-penal-2019.

SENATE OF BELIZE, Act. No. 32, "Cybercrime Act", Gazetted, 7 de octubre del 2020. Disponible en: https://www.nationalassembly.gov.bz/wp-content/uploads/2020/10/Act-No.-32-of-2020-Cybercrime.pdf.

2. JURISPRUDENCIA

A. EXTRANJERA

STJUE, asunto C 523/10, del 12 abril de 2012. El texto puede consultarse en: https://curia.europa.eu/juris/document/document.jsf?text=&docid=121744&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=6989572.

STJUE, asuntos, C-509/09 y C-161/10, del 25 de octubre del 2011. El texto puede consultarse en: https://curia.europa.eu/juris/document/document.jsf?text=&docid=111742&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=1701079.

TRIBUNAL SUPREMO ESPAÑOL (Sala de lo Penal, asunto primero), Acuerdo del 3 de febrero del 2005.

3. INSTRUMENTOS INTERNACIONALES

CONSEJO DE EUROPA, "Convenio sobre Cibercriminalidad", Budapest. Budapest, abierto a la firma el 23 de noviembre de 2001, Serie de Tratados Europeos, No. 185, pp. 1-26.

"Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia". En la Gaceta, Diario Oficial, 4, del 03 de marzo de 2020.

4. REFERENCIAS BIBLIOGRÁFICAS

AMBOS, Kai, "Punishment without a Sovereign? The Ius Puniendi Issue of International Criminal Law: A First Contribution towards a Consistent Theory of International Criminal Law", *Oxford Journal of Legal Studies,* Vol.33, No.2, 2013, *293–315*.

AMBOS, Kai, "Judicial Creativity at the Special Tribunal for Lebanon: Is There a Crime of Terrorism under International Law?", *Leiden Journal of International Law* Vol. 24, No, 03, [en línea], 2011, 655–675. Consultado el 15 de septiembre del 2021. Disponible en: http://journals.cambridge.org/abstract_S0922156511000215.

AMBOS, Kai, *La parte general del derecho penal internacional: Bases para una elaboración dogmática*, (trad. de Ezequiel Malarino), Montevideo, Konrad Adenauer Stiftung, 2005, 594 p.

AMBOS, Kai, "Responsabilidad Penal Internacional en el ciberespacio" (trad. Lucas Tassara), Barcelona, *Revista para el Análisis del Derecho*, 2015, 1-32.

AMERICAN LAW INSTITUTE, *Restatement (Fourth) of Foreign Relations Law of the United States, Philadelphia, Copyright © 2018 by the American Law Institute.*

BALBOA ROMERO, Francisco José, *Ramsomware, hacking y phishing: conducta típica de daños informáticos*, Trabajo de fin de Grado en Derecho, La Rioja, Universidad de Internacional de la Rioja, 2018, p. 9. Disponible en: https://reunir.unir.net/handle/123456789/6929.

BASSIOUNI, M. Cherif, "Jurisdicción Universal para Crímenes Internacionales: Perspectivas Históricas y Práctica Contemporánea" *("Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice"),* traducido al español por el Centro de Derechos Humanos, Facultad de Derecho, Universidad de Chile, *Va. J. Int'l.* L., Vol. 42, No. 81, 2001, 1-67, p. 59. Disponible en: https://corteidh.or.cr/tablas/R08116.pdf.

BENÍTEZ, William Guillermo Jiménez, y QUINTANA, Orlando Meneses, "La investigación y práctica jurídicas", *Revista Prolegómenos Derechos y Valores*, vol. 20, no. 40, Colombia, Universidad Militar Nueva Granada, 2017, 43-61. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6091041.

BRENNER, Susan W., "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare", *Journal of Criminal Law and Criminology*, no. 97, United States of América, Northwestern University School of Law Scholarly Commons, 2007, 379-476.

BRENNER, Susan W., y KOOPS, Bert-Jaap, "Approaches to cybercrime jurisdiction", *J. High Tech. L*, Vol. 4, No. 1, [en línea], 2004, 1-46. Consultado el 21 de junio del 2021. Disponible en https://www.researchgate.net/profile/Susan-Brenner/publication/.

CÁRDENAS AREVANA, Claudia, "El lugar de comisión de los denominados ciberdelitos", *Polít. crim.*, n° 6, 2008, 1-14.

CASTILLO MONTERREY, Marcelo Antonio, *Expolio y Recuperación de las Riquezas Nacionales, Nuevos Retos para el Derecho Penal Internacional*, Tesis Doctoral, España, Universidad de Salamanca, 2012, 543 p.

CLOUGH, Jonathan, *Principles of Cibercrime*, New York, Cambridge University Press, 2010, 449 p.

COHEN-ALMAGOR, Raphael, "Freedom of Expression, Internet Responsibility, and Business Ethics: The Yahoo! Saga and Its Implications", J Bus Ethics, No. 106, 2012,353–365.

COLANGELO, Anthony J., "Double Jeopardy and Multiple Sovereigns: A Jurisdictional Theory", *WASH. U. L, Vol.* 86, No. 4, 769-857. Disponible en: https://openscholarship.wustl.edu/law_lawreview/vol86/iss4/1.

DARAHUGE, María E., y GONZÁLEZ, Luis Arellano, "Empleo de las direcciones virtuales como elemento fundante en las declaraciones de incompetencia por territorialidad", en Ricardo Antonio PARADA y José Daniel ERRECABORDE (Comp.), *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet*, 1a ed., Buenos Aires, Erreius, 2018, 183-189.

DE LA MATA BARRANCO, Norberto, "Los delitos vinculados a la tecnología de la información y comunicación", en ECHANO BASULDA (Dir.), *Delito e informática: algunos aspectos, Cuadernos Penales José María Lidón*, no. 4, Bilbao, Publicaciones de la Universidad de Deusto, 2007, 13-41.

DEPARTMENT OF JUSTICE, *Prosecuting Computer Crime*, 2da. ed., Washington D.C, Office of Legal Education Executive Office for United States Attorneys, 2007, 207 p. Disponible en: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

DIEZ SÁNCHEZ, J. J., *Ley Penal en el Espacio. Teoría General y Análisis de la Legislación Española*, Tesis doctoral. Universidad de Alicante, 505 p. Disponible en: http://hdl.handle.net/10045/3419

FLORES PRADA, Ignacio, "Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia", *Revista Electrónica de Ciencia Penal y Criminología*, No. 17-20, [en línea], 2015, 1-40, p. 8. Consultado el 29 de julio del 2021. Disponible en: http://criminet.ugr.es/recpc.

FLORES SALGADO, Lucerito, *Derecho informático*, México, Grupo Editorial Patria, 2014, 223 p.

GUERRERO BARRANTES, Elizabeth, y SALAZAR RODRÍGUEZ, Luis Alonso, "Comentarios críticos a la reforma del código penal que introduce la ley 9048 (sobre delitos informáticos en el derecho penal costarricense)", *Revista Judicial*, no. 112, San José, Universidad de Costa Rica, 2014**,** 247-257, Disponible en: https://www.kerwa.ucr.ac.cr/handle/10669/81537.

GUTIÉRREZ FRANCÉS, María Luz, *Fraude informático y estafa*, Madrid, Ministerio de Justicia de España, 1991, p. 642.

GUTIÉRREZ FRÁNCES, María Luz, "Reflexiones sobre la ciberdelincuencia hoy (en torno a la Ley Penal en el espacio virtual)", *Revista Electrónica de Derecho de la Universidad de La Rioja*, vol. 1, no. 3, 2005, 69-92.

HARTWIG, Robert. L, *Basic TV Technology: Digital and Analog*, 4ta ed., EE. UU, ELSEVIER, 192 p.

HAYASHI, Mika, "Objective territorial principle or effects doctrine? Jurisdiction and cyberspace", *INT'L LAW*, No. 6, 2006, 284-302.

HERNÁNDEZ DÍAZ, Leyre, "El delito informático", EGUZKILORE: Cuaderno del Intituto Vasco de Criminología, Número, no. 23, Fundación Dialnet [en línea], 2009, 227-243, p.235. Consultado el 24 de julio del 2021. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3343365.

HUERTAS DÍAZ, Omar, "La sociedad mundial y los delitos transnacionales", *Revista Logos, Ciencia & Tecnología*, Bogotá, Policía Nacional de Colombia, vol. 1, No. 2, 2010, 8-17.

Iniciativa de la Ley Especial de Ciberdelitos, Managua, 28 de septiembre del 2020. Disponible en: http://legislacion.asamblea.gob.ni/SILEG/Iniciativas.nsf/xpIniciativa.xsp.

KLEVE, P., De Mulder, R., y VAN NOORTWIJK, K, "The definition of ICT Crime", *Computer Law & Security Review, vol. 27, no. 2,* [en línea], 2011, *162–167.* Consultado el 22 de julio del 2021. Disponible en: www.sciencedirect.com.

LABORATORIO NACIONAL DE CALIDAD DEL SOFTWARE, *Ingeniería del software: metodologías y ciclos de vida*, España, Instituto Nacional de Tecnologías de la Comunicación, 2009. 83 pp.

LE MENESTREL, M., Hunter, M., y DE BETTIGNIES, H.-C., "Internet e-ethics in confrontation with an activists' agenda: Yahoo! On trial", Journal of Business Ethics, No. 39, 2002, 135–144. Disponible en: https://www.jstor.org/stable/25074828.

LÉVY, Pierre, *¿Qué es lo virtual?*, Barcelona, Paidós Multimedia, 1999, 126 p.

LUZÓN PEÑA, Diego Manuel, *Lecciones de Derecho Penal: Parte General*, 3.ª ed., ampliada y revisada, con notas de Derecho Penal nicaragüense por los profs. Aráuz Ulloa/ Moreno Castillo/ Vega Gutiérrez, Managua, UCA Publicaciones, 2017, p. 875.

MATA Y MARTÍN, Ricardo M, *Delincuencia informática y Derecho Penal*, Managua, Hispamer, 2003, 196 p.

MAYA, Ricardo Posada, "El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual", *Nuevo Foro Penal*, vol. 13, no 88, [en línea], 2017, 72-112. Consultado el 19 de junio del 2021. Disponible en: https://publicaciones.eafit.edu.co/index.php/nuevo-foro-penal/article/download/4751/pdf/.

MIRÓ LLINARES, F., *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012, 332 pp.

MORENO VERDEJO, Jaime, "Algunas Cuestiones acerca de la estafa informática y el uso de tarjetas", en ECHANO BASULDA (Dir.), *Delito e informática: algunos aspectos, Cuadernos Penales José María Lidón,* no. 4, Bilbao, Publicaciones de la Universidad de Deusto, 2007, 173-227.

MUÑOZ CONDE, Francisco, y GARCÍA ARÁN, Mercedes, *Derecho Penal: parte general*, 8ª ed., revisada y puesta al día, Valencia, Tirant lo Blanch, 2010, 647 p.

PAOLI, J. Antonio, "Comunicación e información". *Perspectivas teóricas.* México, *Trillas*, UAM, 1983, 138 p.

PARKER, D. B., *Crime by Computer*, New York, Charles Scribner's Sons, 1976, 320 p.

PARKER, D. B., *Fighting Computer Crime*, New York, Charles Scribner's Sons, 1983, 357 p.

PLASCENCIA VILLANUEVA, Raúl, *Teoría del delito*, 2da. Reimp., México, Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México, 2000, 287 p.

QIANYUN WANG, *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe*, Tesis Doctoral, Erasmus University of Rotterdam, 2016, 354 p.

RELATOR ESPECIAL DE LAS NACIONES UNIDAS PARA LA LIBERTAD DE OPINIÓN Y DE EXPRESIÓN, *et. al.,* "Declaración conjunta sobre la libertad de expresión e Internet", Organization for Security and Co-operation in Europe, Suecia, 1 de junio del 2011, 1-5. Disponible en: http://www.osce.org/fom/78309.

RIGDON, John C., en *Dictionary of computer and internet terms,*1. a ed., Catersville, Eastern Digital Resources. 2016, [en línea], Consultado el 1 de julio del 2021. Disponible en: http://www.damanhour.edu.eg/pdf/738/dictionaries/Dictionary_of_Computer_and_Internet_Terms_Words.pdf.

RINCÓN RÍOS, Jarvey, *El delito en la cibersociedad y la justicia penal internacional*. Madrid, Universidad Complutense de Madrid, 2015, 503 p. Disponible en: https://eprints.ucm.es/id/eprint/33360/.

ROBERTS, Lynne, "Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An Analysis on Cyber Stalking", *International Journal of Cyber Criminology*, Vol. 2, No., 2008, 271-285.

TANENBAUM, Andrew S., y WETHERALL, David J., *Redes de computadoras*, 5ª edición, traducción al español por Alfonso Vidal ROMERO ELIZONDO, Ed. Pearson Educación, México, 2012, 791 p.

TOMPKINS JR., Joseph B., y MAR, Linda A., "The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem", *The John Marshall Journal of Information Technology & Privacy Law*, no. 6, [en línea], 1986, 459-483, p. 460. Consultado el 23 de julio del 2021, disponible en: https://repository.jmls.edu/cgi/viewcontent.cgi?article=1512&context=jitpl.

UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Comprehensive Study on Cybercrime*, Vienna, UNODC, 2013, 287 p. Disponible en https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf..

ZUPPO, Colrain M., "Defining ICT in a boundaryless world: the development of a working hierarchy", *International Journal of Managing Information Technology*, vol. 4, No.32, [en línea], 2012, 13-22. Consultado el 22 de julio del 2021. Disponible en: http://www.airccse.org/journal/ijmit/papers/4312ijmit02.pdf.

5. CONTENIDO MULTIMEDIA

AGUILAR, Marvin, "Seminario Taller sobre las reformas y adiciones a la Constitución Política, Código Penal, Procesal Penal y Ley 779 de la República de Nicaragua", [video], Managua, 21 de abril del 2021.

6. SITIOS WEB

CRUZ VILLALÓN, Pedro, "Conclusiones", presentadas ante el TJUE, en el asunto C 523/10, del 16 de febrero de 2012, [en línea], párr. 28, 30, 37 y 38. Consultado el 11 de agosto del 2021, Disponible en: https://curia.europa.eu/juris/document/document.jsf;jsessionid=10B9E683DA5E00551B85527422DA8DFC?text=&docid=119515&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=5176208.

Estados Miembros, Secretaría General del Sistema de la Integración Centroamericana, *© 2020.* Consultado el 13 de agosto del 2021. Disponible en: https://www.sica.int/estadosmiembros.

FUNDÉU RAE, "las TIC, mejor que las TICs o las TICS", [en línea]. Consultado el 15 de julio del 2021. Disponible en https://www.fundeu.es/recomendacion/las-tic-mejor-que-las-tics-o-las-tics/.

Oxford University, *Oxford English and Spanish Dictionary, Synonyms, and Spanish to English*, [en línea], 2021. Consultado el 5 de julio del 2021, disponible en https://www.lexico.com/en/definition/cyber-.

Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY. Council of Europe, © 2021. C*onsultado el 12 de septiembre del 2021. Disponible en: https://www.coe.int/en/web/cybercrime/parties-observers.*

RAE, *Ciber, en: Diccionario panhispánico de dudas,* [en línea], 2005. Consultado el 5 de julio del 2021, disponible en: http://lema.rae.es/dpd/srv/search?id=tb7u92tGpD6zzdh481.

THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION, *Telcom Glossarry: informatiom system,* [en línea]. Consultado el 15 de julio del 2019. Disponible en: http://standards.tiaonline.org/market_intelligence_/glossary/index.cfm?term=%26%23%24%3B%5BR%227G%0A.

United Nations Treaty Collection. United Nations, © 2021. Consultado el 12 d septiembre del 2021. Disponible en: *https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=VI-19&chapter=6&clang=_en.*