

EL CIBERCRIMEN Y EL FUTURO DE LA ADMINISTRACIÓN DE LA JUSTICIA: ALGUNOS DILEMAS PROCESALES Y PROBATORIOS PARA LA PERSECUCIÓN DE LOS DELITOS CIBERNÉTICOS

*Sergio Andrés Lizarazo Gil, Samuel Camilo Bernal Cortés,
María Lucía Mariño Ríos y Saray Liliana Silva Jaimes*

*Tutor: Daniel Felipe Garavito Rincón
Universidad Santo Tomás*

Resumen:

Mediante una comprensión integral del derecho penal, que articula sus dimensiones criminológicas, político-criminales y dogmáticas, se realiza una aproximación a los principales retos que impone el *cibercrimen* al futuro de la administración de la justicia. De esta manera, a lo largo de este artículo, se analizan algunas de las dificultades para la persecución y sanción del *cibercrimen* en el ámbito de la teoría del delito, y, en especial, en procesal (Competencia y pruebas). Se arriba a la conclusión de que las principales dificultades se encuentran vinculadas a la organización estatal de la persecución y sanción del delito y, por ello, a la necesidad de solidificar los estándares internacionales para la definición del *cibercrimen*, los estándares probatorios, y las formas de cooperación internacional que permitan una adecuada respuesta punitiva.

Palabras clave: Cibercrimen, competencia, cooperación internacional probatoria, futuro de la administración de justicia.

Abstract:

Through a comprehensive understanding of criminal law, which articulates its criminological, political-criminal, and dogmatic

dimensions, an approach made to the mains challenges that cyber-crime imposes on the future of the administrations of justice. In this way, throughout this article, some of the difficulties for the prosecution and punishment of cybercrime are analyzed in the field of crime theory, and, especially, in the procedural (competence and evidence). The conclusion is reached that the main difficulties are linked to the state organizations of the prosecution and punishment of the crime and, therefore, to the need to solidify the international standards for the definition of cybercrime, the evidentiary standards and the forms of international cooperation that allow an adequate punitive response. **KEY WORDS:** Cybercrime, competition, international evidentiary cooperation, future of the administration of justice.

Introducción

El mundo contemporáneo tiene como característica fundamental un grado alto de *complejidad social* que ha llevado a concebir nuestra sociedad como una *sociedad del riesgo*, esto es, una formación social en la que las relaciones sociales, en el marco del proceso de globalización y la extensión de múltiples avances en el dominio de la técnica, conlleva la aparición de múltiples riesgos ampliamente visibilizados por las redes sociales y los medios de comunicación¹.

Aunque los riesgos no deben ser comprendidos como un factor negativo por sí mismo —pues ofrecen múltiples posibilidades y aperturas para la resolución de diversos problemas²—, es necesaria la generación de diferentes mecanismos regulatorios (sociales, éticos y jurídicos) que permitan reducir los resultados lesivos de los derechos de los sujetos.

Ahora bien, dentro de los múltiples riesgos que emergen en este contexto destaca, especialmente por el desarrollo y extensión de Internet en el mundo, la ampliación de los riesgos en el *ciberspacio* que conllevan en los casos más complejos a la aparición de resultados lesivos de bienes jurídicos como la libertad, el patrimonio, el derecho a la imagen, la libertad sexual, la integridad física y psíquica y el honor entre otros³, es decir, conlleva la posible aparición del *ciberdelito*.

¹ BECK, Ulrich. La sociedad del riesgo. Barcelona: Paidós. 1998.

² KAUFMANN, Arthur. Filosofía del derecho. Bogotá: Universidad Externado de Colombia. 1999. pp. 530-531.

³ RAYÓN, M y GÓMEZ, J. *Ciberdelitos*: particularidades en su investigación y enjuiciamiento. En: Anuario Jurídico y Económico Escurialense. 2014. XLVII. 209-234. ISSN: 1133-3677. p. 211.

La comprensión de los principales retos que el *cibercrimen* impone al derecho penal y el futuro de la administración de la justicia requiere un análisis capaz de articular los principales elementos criminológicos, axiológicos y dogmáticos en juego⁴. Para ello, se propone una lectura que articula estas tres dimensiones fundamentales en una perspectiva integradora y que, a su vez, recoge el método prudencial de Tomas de Aquino como mecanismo para la lectura de los problemas que se imponen en nuestra época.⁵

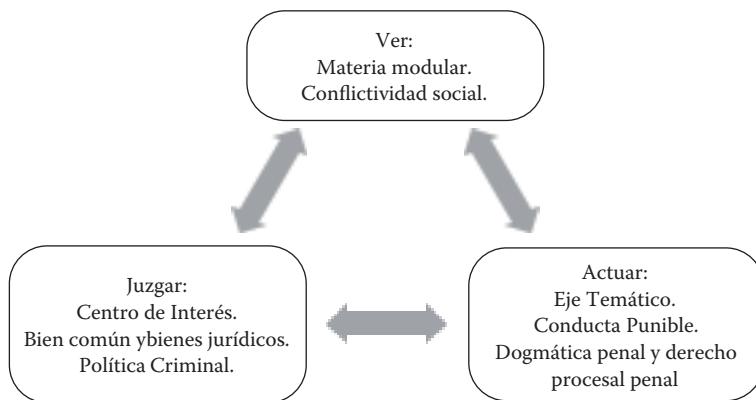


Tabla 1. Modelo integrado de derecho penal y método prudencial.

De esta manera, se intenta responder a la pregunta ¿Cuáles son los principales retos para la administración de la justicia penal en materia de competencia y pruebas que impone el *cibercrimen* en las sociedades contemporáneas y en específico en el ordenamiento jurídico colombiano? Para ello, se realiza en primer lugar una lectura de las principales características criminológicas del *cibercrimen* desde una perspectiva capaz de analizar la manera en la que esta forma de la *conflictividad social* se desenvuelve en las sociedades contemporáneas; en segundo lugar, se realiza un análisis valorativo de la manera en la que el *bien común* y los *bienes jurídicos* pueden verse lesionados mediante las diferentes expresiones del *cibercrimen*; en tercer lugar, se realiza un análisis de los

⁴ GARAVITO, Daniel. Emociones, responsabilidad penal y política criminal. Tunja: Ediciones USTA.2022. P. 82-85. Esta misma concepción de la ciencia integral del derecho penal puede ser encontrada en la obra de Velázquez Velázquez y Mir Puig. Véase. MIR PUIG, Santiago. Derecho penal. Parte General. Barcelona: Reppetor.2016 y VELÁZQUEZ VELÁZQUEZ, Fernando. Manual de Derecho Penal. Parte General. Bogotá, D.C.: Ediciones Jurídicas Andrés Morales. 2013.

⁵ CÁRDENAS, A. y Cárdenas, C. Módulo Penal. En: Núcleos problemáticos (Módulos siglo XXI)(págs. 41-52). Bogotá: Universidad Santo Tomás. 2002.

principales retos que impone para la dogmática penal el análisis del *cibercrimen* como *conducta punible*. En cuarto lugar, se realiza una aproximación a las principales peripecias que, en el campo del derecho procesal, en específico en el ámbito de la competencia, y en del derecho probatorio, impone el *cibercrimen*. Finalmente, se realiza una propuesta que, fundada en la cooperación internacional en materia probatoria para la persecución del crimen y la generación de estándares internacionales del *cibercrimen*, permita un adecuado tratamiento del *cibercrimen*.

Cibercrimen: importancia de la teoría del delito

1. Notas criminológicas del *cibercrimen*

El modelo integrado de derecho penal requiere, en primer lugar, disponer de elementos para *ver* las principales modificaciones que se operan en un momento particular de la historia y que tienen impacto en la ciencia del derecho penal. Para ello, se requiere una reflexión sobre las principales modificaciones en las relaciones políticas, sociales, culturales, económicas y técnicas que generan nuevas formas de *conflictividad social*. En este sentido, la criminología, como ciencia empírica e interdisciplinaria encargada del estudio del crimen, el delincuente, la víctima y las formas de la reacción social ofrece herramientas para comprender los mecanismos de prevención reacción frente a nuevas formas delictivas⁶.

En este sentido, vale la pena indicar que, dentro de la ciencia criminológica existe una parte especial, donde se encuentran las denominadas “ciencias específicas” o “criminologías alternativas” y en las que tiene cabida el estudio del fenómeno de la cibercriminalidad. A propósito de este término, puede decirse que este ha sido objeto de atención reciente, pues se atribuye su origen a Jaishankar quien lo considera como un nuevo campo o una subdisciplina de la criminología.⁷ Para Jaishankar, la *cibercriminología* “implica el examen del comportamiento criminal y la victimización en el ciberespacio desde una perspectiva teórica y criminológica”⁸ pues no solo se encarga del estudio de los delitos que tienen cabida dentro del ciberespacio, sino que también reflexiona sobre el impacto que estos tienen sobre el espacio físico.

⁶ GARCÍA-PABLOS DE MOLINA, Antonio. Tratado de criminología. Valencia: Tirant Lo Blanch. 2003. p.47.

⁷ CÁMARA ARROYO, Sergio. Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. En: Derecho y cambio social. Abril, 2020. ISSN 2224-4131.

⁸ Ibid., p, 472.

Así pues, a raíz de la incidencia con la que la *cibercriminalidad* se ha desarrollado, muchos autores han pretendido, por medio de una serie de teorías, explicar el fenómeno de la ciberdelincuencia y su génesis; pues esta no es más que una de las formas que se encuentra para llevar a cabo comportamientos criminales.

En primer lugar, nos encontramos con la *teoría del aprendizaje social* y la *asociación diferencial*, de Sutherland y de Akers, por medio de la cual se busca dar una explicación acerca de la adquisición y/o modificación de la conducta delictual, partiendo de la premisa de que la comunicación es fuente de aprendizaje y, por ende, es así como los comportamientos delictuales son aprendidos mediante un proceso de asociación diferencial. En realidad, la conducta delictual, que se constituye como conducta desviada, es aprendida y se modifica a través mecanismos cognitivos. Es decir, la *teoría del aprendizaje* “explica el hecho de que las personas se vuelvan propensas a la conducta delictiva o desviada, así como la estabilidad o al cambio en dicha propensión”⁹.

Por otro lado, la *teoría del control social*, de los *vínculos sociales* y del *auto-control*, propone que el factor que se debe tener en cuenta de manera primaria con respecto de la delincuencia es el hecho de que el individuo tiene la capacidad para controlar sus impulsos y detener sus deseos. De esta manera, un control débil por parte del individuo puede llegar a reflejar una ausencia o poca capacidad para socializarse, además de dilucidar fracturas dentro de la crianza al interior del hogar. En lo concerniente a la *cibercriminalidad* se afirma que el acometimiento tecnológico puede haber coadyuvado a que al estancamiento de los vínculos sociales: la llegada de la tecnología supone la existencia de un mundo que cada vez se encuentra más conectado, en donde la información sea conseguida de manera más veloz y eficaz con respecto de los métodos tradicionales.

En tercer lugar, se encuentra la *teoría general de la tensión*, desarrollada por el autor Agnew, que propone que el crimen tiene su origen en la frustración que padece un sujeto como consecuencia las tensiones generadas por la imposibilidad de alcanzar ciertas expectativas que le son impuestas socialmente trayendo como corolario que reprima de su ser todo tipo de estímulos positivos por estar inmerso en situaciones negativas que el sujeto no puede evitar haciendo del crimen una manera de escapar de ello. En la medida de que estas tensiones padecidas en “mundo real” pueden evitarse en el ciberespacio, este se considera “libre” dejando escapar sus frustraciones¹⁰.

En cuanto a la *teoría de las ventanas rotas* (*Broken Windows*), propuesta por Wilson y Kelling, es importante señalar que muchos delitos sostienen su

⁹ Ibid., p, 474.

¹⁰ Ibid., p, 474.

permanencia en, la decadencia social lo que supone la escasa importancia atribuida a ciertas conductas delictuales: por ejemplo, cuando se está frente a casos de piratería informática, y más aún, cuando se normalizan este tipo de conductas. Se da entonces la aceptación social frente a conductas, en teoría, son delictuales¹¹.

Conviene subrayar que, dentro de la *teoría de la transición espacial*, una persona que dentro del espacio físico posee una suerte de conductas reprimidas que no puede materializar por determinadas restricciones encuentra en el ciberespacio un medio de ejecución. Además de verse tentado por la flexibilidad de la identidad, que ofrece el ciberespacio, debido a que la existencia del anonimato, lo que proporciona, en término coloquiales, al delincuente una herramienta para cometer ciberdelitos¹². Así mismo, Cámara Arroyo propone que muchos de los ciberdelitos son cometidos porque el ciberespacio ofrece mayores facilidades con respecto del mundo físico. Lo anterior parece que confirmar que el análisis de la *cibercriminalidad* no es unitario, sino que supone la búsqueda de diversos factores que pueden llegar a contribuir a su aparición, como el aumento desenfrenado de la utilización las nuevas tecnologías de la comunicación.

En definitiva, la exposición al internet puede traer consigo una serie de riesgos que se derivan del altísimo alcance que este posee a nivel mundial, haciendo que la información y los espacios de seguridad sean más vulnerables.

2 El *cibercrimen* en el mundo

Es entonces cuanto menos imperativo para los sistemas legales contemporáneos, según Aaron Dennis, una clara conceptualización del concepto *cibercrimen*, así como la delimitación de los elementos contingentes de este que permitan su valoración con la menor cantidad de variaciones posibles, removiendo el caótico conflicto de heterogeneidad no solo entre legislaciones nacionales, sino también en la relación de cooperación internacional entre ellas.¹³

Un hito clave en la evolución del concepto de *cibercrimen* fue la adopción del Convenio sobre la Ciberdelincuencia del Consejo de Europa en Budapest el año 2001. Este tratado internacional representó un esfuerzo pionero por armonizar las leyes nacionales y establecer un marco de cooperación entre países en materia de delitos informáticos. El Convenio definió una serie de conductas delictivas relacionadas con el acceso no autorizado a sistemas, la interceptación ilegal de datos, los delitos contra la confidencialidad, la integridad y la

¹¹ Ibid., p, 474-475.

¹² Ibid., p, 476.

¹³ DENNIS, Michael Aaron. *Cibercrimen*. En: Encyclopedia Britannica. Junio, 2024. p. 4.

disponibilidad de los sistemas y datos informáticos, así como los delitos vinculados a la pornografía infantil¹⁴. Esta definición es la base para la comprensión unificada del *cibercrimen* a nivel internacional, delimitado al *cibercrimen* como un comportamiento ilícito perpetrado mediante operaciones electrónicas que atentan en contra de la seguridad de los sistemas informáticos o los datos procesados por estos. Sin embargo, esta definición, como lo señala Kirsty Phillips, adolece de dos grandes problemas. El primero, es que el *cibercrimen* está sujeto con antelación a una conducta ilícita ya reconocida por el ordenamiento jurídico, es decir, típica. El segundo, referencia entonces esta definición a *cibercrimen* como una categoría netamente dependiente de delitos típicos que se desarrollan en un entorno virtual.¹⁵ Los dos anteriores planteamientos son cuanto menos problemáticos. El primero entiende al *cibercrimen* como una categoría ya creada y reconocida al interior de los ordenamientos jurídicos y, la segunda, como lo advirtió Julia C. Davidson, supone tratar al *cibercrimen* como el compendio de delitos ordinarios perpetrados mediante el uso cualquier dispositivo de cómputo, redes o Hardware, siendo diferencia sustancial con los crímenes ordinarios el entorno de su comisión. Esta definición, no atiende a que los sistemas de datos pueden ser un agente o facilitador del crimen, en tanto se trata únicamente de un medio de comisión, tal y como lo sería un arma de fuego en el delito de homicidio.¹⁶

Por otra parte, a medida que las tecnologías digitales evolucionaron y se diversificaron, el alcance y la complejidad del *cibercrimen* también se expandió. El Estudio sobre Ciberdelincuencia de la ONU de 2013 resaltó esta tendencia, analizando cómo los delitos informáticos se habían vuelto más sofisticados, transnacionales y de mayor impacto a nivel global. Temas emergentes como el fraude y el robo de identidad, los ataques con malware, los secuestros de datos (ransomware) y los delitos relacionados con la explotación sexual de menores fueron identificados como algunas de las principales amenazas que enfrentan los Estados¹⁷. Gordon and Ford definieron el *cibercrimen* como el conjunto de actividades criminales mediadas por computadoras, ilegales o ilícitas por

¹⁴ CONSEJO DE EUROPA. (185:2001: Budapest) Convenio sobre la ciberdelincuencia. Budapest: Serie de tratados europeos, 2001. p. 26.

¹⁵ PHILLIPS, Kristy. DAVIDSON, Julia. FARR, Ruby. R. BURKHARDT, Christine. CANE-PPELE, Stefano. y AIKEN, Mary. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. En:Forensic Sci. Abril, 2022, vol. 2, no.1 pp. 379-398. DOI: <https://doi.org/10.3390/forensicsci2020028>

¹⁶ Ibíd., p. 382

¹⁷ NACIONES UNIDAS. Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante esefenómeno. Viena: UNODC, 2013. 18 p.

diversas partes y que pueden realizarse mediante redes globales¹⁸; sin embargo, acepta que estas conductas deben ser tipificadas bajo similares elementos descriptivos del tipo ya no solo en un Estado, sino que, por la característica misma de transnacionalidad del *ciberdelito*, en otros Estados.

En respuesta a estos desafíos globales, mediante informe anual sobre la Evaluación de la Amenaza del Crimen Organizado en Internet de Europol (2021), se pretende monitorear las tendencias emergentes y coordinar acciones entre los Estados miembros de la Unión Europea¹⁹. Esto ha permitido una comprensión más profunda de los métodos y las redes delictivas que operan a través de las fronteras, facilitando una respuesta más efectiva.

Ahora bien, es necesario destacar la diferenciación entre tipos de delitos cometidos por actividades mediadas por computadoras o sistemas de procesamiento de datos, Estos pueden clasificarse en tres grandes grupos²⁰, el primero, delitos de contacto humano (Tipo I), el segundo, en donde el uso de la tecnología es incidental (II) y el tercero, siendo una extensión del primero que representan delitos futuros o tecnológicamente más avanzados (Tipo III). Como se muestra en la tabla 1²¹, cada tipo está sujeto a una relación de dependencia o mediación mayor al uso de dispositivos de procesamiento, divididos en seis grupos, así:

Tabla 1. Clasificación de delitos cibernéticos y ciber desviaciones.

Type III	Type I			Type II		
	Cyber-Dependent		Cyber-Enabled			
	I "Crimes against the machine"	II "Crimes using the machine"	III	"Crimes in the machine"		IV "Cyber assisted"
	1. Attacks Against Data and Systems	2. Attacks Against Property or Theft	3. Interpersonal Violence	4. Sexual Violence	5. Violence Against Groups	7. Incidental Technology Use
	1A. Against Individuals & Organizations Illegal access (hacking/cracking) Illegal data acquisition (data espionage) Illegal interception Data interference System interference Misuse of devices Extortion/Ransomware Hoax 1A. Against States and Nations Political interference Cyberwarfare Espionage	Computer-related forgery Computer-related fraud Copyright infringements Trademark related offenses Digital piracy Spam Identity theft Phishing Cyberfraud	Harassment Cyberbullying Trolling Coercion Extortion (e.g., Romance Fraud) Inciting violence	Pornographic material Child sexual abuse material/Exploitation Grooming Stalking Image based abuse Sexual Sex trade Sex trafficking Sex tourism Sexting	5A. Protected Characteristics Hate speech Religious offenses Xenophobia 5B. Terrorism Terrorism Radicalisation	Illegal gambling Illegal gaming Laundering Money muling Drug trade Criminal communications
	V Cross-category: Organised Crime, Deep Web Markets, Illegal Virtual Marketplaces and Cybercrime-as-a-Service					
	VI Cross-category: Information and Behavioural Manipulation					
	6A. Using Advanced Technology		6B. Using False Information		Cyber troops, Fake news, Misinformation, Disinformation	
	AI, ML, Algorithmic profiling, Deep fakes, Bots, Botnets					
	Cyber Security			Cyber Safety		

¹⁸ GORDON, Sarah y FORD, Richard. On the definition and classification of cyber-crime. En: JComput Virol. Febrero, 2006. Vol. 2. DOI: 10.1007/s11416-006-0015-z.

¹⁹ EUROPOL. Internet Organised Crime Threat Assessment (IOCTA). Luxemburgo: PublicationsOffice of the European Union, 2021. 19p. ISBN 978-92-95220-35-5.

²⁰ PHILLIPS, Kristy. DAVIDSON, Julia. FARR, Ruby. R. BURKHARDT, Christine. CANE-PPELE, Stefano. y AIKEN, Mary. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. En: Forensic Sci. Abril, 2022, vol. 2. Op. cit., pp. 391. DOI: <https://doi.org/10.3390/forensicsci2020028>

²¹ *Ibíd.*, p. 12

3. Definición del *cibercrimen* desde la teoría del delito

Ricardo Posada²² nos ofrece los aspectos diferenciadores entre los cibercrímenes y los delitos comunes en el ámbito de la teoría del delito desde la siguiente clasificación:

- A. *El bien jurídico*: El *cibercrimen* tiene como objetivo principal proteger la seguridad de la información, los datos y el adecuado funcionamiento de los sistemas informáticos. Así, aparece un bien jurídico intermedio o autónomo, de efecto sombrilla, puesto que protege diversos bienes jurídicos permitiendo la adaptabilidad de los mismos en el hecho realizado, este bien jurídico es uno de los pocos bienes de naturaleza colectivo individual que genera exclusión de responsabilidad a partir del consentimiento otorgado por el titular de los datos informáticos.
- B. *La acción o el nacimiento de la ciberacción*: la acción del *cibercrimen* tiene varios matices diferenciadores de la acción física que conocemos dentro de la conducta, esta acción no es desarrollada dentro de un entorno físico o tangible; por el contrario, tiene un carácter virtual. De igual manera, la acción es caracterizada por la ejecución de instrucciones procesables por el sistema informático de carácter interactivo/reactivo permitiendo a la mente humana la utilización de herramientas informáticas para la ejecución de la acción. A su vez, la acción no puede ser ubicada en un plano de tiempo y espacio como las acciones físicas, puesto que están deslocalizadas y desubicadas físicamente generando conflictos con las asignaciones de competencia. Por último, su capacidad de automatización y programabilidad desligan al sujeto de la dependencia de la ejecución de la conducta gracias a la capacidad de determinar momentos y horas exactas de su realización sin presencia del autor.
- C. *Los sujetos activos del crimen*: existe una gran complejidad para la identificación del sujeto activo o el autor material de la conducta dentro del *cibercrimen*. En la medida de que las herramientas informáticas permiten el anonimato el sujeto activo resulta escurridizo²³.
- D. *Los objetos sobre los cuales recae la acción y los medios tecnológicos en el cibercrimen*: la protección de los delitos comunes o físicos es de corto alcance en relación a la protección de los objetos del *cibercrimen* que no

²² RICARDO POSADA MAYA, El *cibercrimen* y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. Enero- junio, 2017, vol. 13, No. 88. ISSN 0120-8179.

²³ ADARVE, Laura y CAMPAZ, Malcom. La Identidad del Sujeto Activo en el Delito de Estafa bajo la Modalidad Virtual Frente al Incumplimiento Contractual de una Transacción Digital en Colombia. Santiago de Cali. 2021. p, 26.

están dentro de la esfera física, sino que superan esta y necesitan una mayor cobertura. Los objetos sobre los que recae la acción del *cibercrimen* son los datos informáticos, la información, el software y los sistemas informáticos, que tienen en común el carácter virtual de bienes jurídicos no protegido dentro de los tipos comunes.

- E. *El resultado*: el *cibercrimen* amplió la concepción del resultado más allá de la mera modificación del mundo exterior y le otorgarla un carácter inmaterial. De esta manera, las modificaciones en los objetos o datos digitales y la trazabilidad dentro de los movimientos de las herramientas informáticas que pueden generar daños silenciosos a mayor escala, se convierten en una forma de resultado.
- F. *Nexo de causalidad*: aunque existe la impresión de que este aspecto objetivo del tipo, en cuanto a su práctica, es ausente en la medida de que la acción dentro del *cibercrimen* puede ser programada y automatizada, y por tanto dificultando unir el hecho que genera el daño y el daño causado: la infraestructura tecnológica podría verse como un tercero que rompe este nexo causal; sin embargo, es posible adjudicar responsabilidad desde la aplicación de la teoría de la imputación objetiva para que baste con sobrepasar el riesgo permitido.
- G. *El dolo*: las dificultades que se presentan en la aplicación de este concepto se centran en los medios para ejecutar la acción puesto que estas conductas tienen la posibilidad de ser automatizadas y programadas, haciendo difícil establecer conexión entre tiempo real de la ejecución del delito y el conocimiento y la voluntad del sujeto activo sobre su actuar. Así, es necesario modificar la ubicación del dolo y la voluntad en el momento de la programación de las funciones y no en la ejecución de las mismas.
- H. *El dominio del hecho y la autoría*: el dominio del hecho supone que el sujeto activo controla las circunstancias y cumple con los elementos del tipo penal establecido; sin embargo, en el desarrollo del *cibercrimen* no se puede hablar de una participación completa en la ejecución del acto puesto que en el desenlace de esta se inmiscuye la participación de herramientas electrónicas. De esta manera, es importante analizar en esta etapa el papel del sistema informático al considerarlo como medio y no otorgarle un papel decisivo dentro la realización del acto. Esto en tanto que como los ejecutores de conductas como el *cibercrimen* cuentan con una gran cantidad de recursos tecnológicos que les otorgan un camino lleno de alternativas para evadir la responsabilidad y realizar el delito²⁴.

²⁴ MANJARRÉS, I & JIMÉNEZ, F. (2012). Caracterización de los delitos informáticos en Colombia. *Pensamiento Americano*, 71-82.

- I. *Otras Figuras como la pena*: se requieren nuevas modalidades de medidas de aseguramiento puesto que las tradicionales no generan efectividad ante la necesidad de la pena. Una de las medidas de seguridad más adecuadas es la inhabilitación especial que elimina o restringe el derecho del ciberdelincuente para conectarse virtualmente al sistema informático. Así, las restricciones deben dirigirse a la imposibilidad de acceso a los medios informáticos, no a su derecho de locomoción en el espacio físico. De igual manera, es necesario generar medidas de prevención del daño que no son aplicables como una pena, pero si son necesarias para disminuir la necesidad de la misma. Las medidas preventivas en este aspecto son escasas y los sujetos que constituyen nuestra sociedad no están en igualdad de armas para detectar, analizar y entender cuando un daño informático es inminente²⁵.

***Cibercrimen* y competencia: algunos dilemas de la persecución del *cibercrimen* leídos desde el ordenamiento jurídico colombiano**

1. Un caso complejo

Imagine el lector: se encuentra desde la comodidad de su hogar, en algún lugar del territorio nacional, siendo parte de un prestigioso congreso internacional en tecnologías disruptivas en Derecho, realizado mediante inmersión al interior de entorno virtual perteneciente y monitoreado por Google. Es partícipe de todos los niveles sensitivos posibles, incluso el tacto. Presencia usted el primer ataque Ciberterrorista en un entorno virtual ultra real. El sistema fue hackeado e inducen en usted y todos los presentes —mediante descargas eléctricas descontroladas provenientes del sistema de tecnología háptica cuyo fabricante es la empresa TeslaSuit—una sensación de dolor profunda mediante contracciones musculares fuertes provocándole espasmos, y rupturas fibrales que le impiden a su vez moverse libremente durante al menos un cuarto de hora. Además, uno de los invitados presentes, un conferencista español que se encontraba conectado desde su natal Bilbao, muere a causa de un infarto provocado por una fibrilación ventricular severa, arritmia inducida por los alterados impulsos eléctricos que le ordenan al corazón latir.

Inicialmente sería necesario adecuar la acción dañosa a las descripciones estrictas de cada conducta típica. Así, en el caso concreto podría pensarse en

²⁵ AGUILAR, M. M. (2015). *Cibercrimen* y ciber victimización en Europa: instituciones involucradas en la prevención del cibercrimen en el Reino Unido. *Revista Criminalidad*, 57 (1): 121-135.

las lesiones personales, teniendo como objeto de examen los espasmos, el dolor y las secuelas que pudiesen desprenderse de las rupturas fibrales, tratándose de una vulneración clara al bien jurídico de la vida e integridad personal. De igual manera, las acciones cuyo resultado condujeron al deceso del conferencista podrían ser un homicidio agravado. Por otra parte, si la valoración recae sobre la retención en la movilidad de los sujetos víctimas, el sistema legal colombiano supondría la existencia de una vulneración de la libertad individual, adecuando la conducta al delito de secuestro simple. En otro momento, el operador judicial, puede incluso realizar adecuación típica respecto a la vulneración al bien jurídico de *la protección de la información y los datos*, en dependencia de los medios utilizados por el sujeto o sujetos activos para transgresión del sistema informático que monitoriza y parametriza el entorno virtual.

2. La competencia en el derecho penal colombiano

Para comenzar, es imperioso referir que como dice Manzini²⁶, la jurisdicción ha sido entendida como la función soberana que tiene por finalidad la determinación de si es aplicable o no una norma jurídica en un caso concreto, es decir la posible concreción de la voluntad que de ella se manifiesta en el caso. De igual manera, la jurisdicción es una consecuencia de la heterocomposición de los conflictos mediante órganos judiciales que fungan como instituciones representantes del poder estatal y que, a su vez, son un tercero legitimado dentro de la solución de los conflictos²⁷. De hecho, la jurisdicción ha sido entendida como “la facultad que tiene el Estado para administrar justicia por medio de los órganos judiciales instituidos para tal efecto, que tiene por finalidad la realización del derecho mediante la materialización de la ley a casos concretos”²⁸. Ahora bien, es importante resaltar que la jurisdicción es una manifestación que ejerce el Estado con el propósito de ser garante de la correcta efectividad del derecho. En este sentido, la jurisdicción puede ser comprendida como: “Soberanía del Estado, aplicada por conducto del órgano especial a la función de administrar justicia, principalmente para la realización o garantía del derecho objetivo y de la libertad y de la dignidad humanas, y secundariamente para la composición

²⁶ MANZINI, Vincenzo, Tratado de derecho procesal penal, II, Ediciones de Cultura Jurídica, 1998, pp. 23 y ss.

²⁷ ROSERO RICO, Dairo Andrés. La unidad de la jurisdicción en el Estado colombiano. Una mirada a partir de la Constitución Política de 1991. La jurisdicción. En: Diálogos de Derecho y Política. Abril, 2014, no. 13 ISSN2145-2784.

²⁸ ALVARADO VELLOSO, Adolfo. Jurisdicción y competencia [Online] [Citada 17/04/2024]. https://campus.academiadederecho.org/upload/Cvaav/Pdf/NF%200AD/Ad/Jurisdiccion_y_Competencia A AV.pdf

de los litigios o para dar certeza judicial a los derechos objetivos mediante la aplicación de la ley a casos concretos, de acuerdo con determinados procedimientos y mediante decisiones obligatorios”²⁹.

La conceptualización de la soberanía se encuentra vinculada directamente con el poder político que se desprende de los Estados, incluso vale la pena referir que este término comienza a tener peso de manera significativa a finales del siglo XVI al mismo tiempo en que juega un papel determinante el Estado absoluto³⁰. De ahí que cuando se supera el Estado absoluto y florece el Estado Constitucional Moderno, la soberanía se proclama como una suerte de independencia frente al poder estatal, siendo una de las inequívocas expresiones del asentamiento del Estado Constitucional Moderno; es más puede llegar a decirse que es una de sus características esenciales³¹. Precisamente, Arendt hace buena alusión a esto cuando refiere a que “el elemento democrático del Estado Nacional es la soberanía popular”³². En este mismo sentido. Jacques Maritain³³ afirma que la soberanía refiere a una suerte de independencia y poder que son ejercidos por el cuerpo político, debido a que se deriva de un derecho inalienable y natural. De esta manera, existe una soberanía interna que es ejercida al interior de los Estados, los cuales disponen de un “poder supremo”³⁴ con respecto de las personas, o más bien del pueblo, a quien gobiernan.

Lo anterior no es más que decir que la jurisdicción, tal y como proviene del latín “*uiris dictio*”, es la potestad que cuenta el Estado para “decir el derecho”³⁵, derecho que tiene por objeto el que las partes inmersas en una disputa diriman

²⁹ DEVIS DE ECHANDIA, Hernando. Teoría general del proceso. Tercera Edición. Buenos Aires: Editorial Universidad. 538 p.

³⁰ BOBBIO, Norberto. Citado por MARCIO CRUZ, Paulo. Soberanía y transnacionalidad: Antagonismos y consecuencias. Junio, 2010. ISSN 1794-2918.

³¹ MARCIO CRUZ, Paulo. Soberanía y transnacionalidad: Antagonismos y consecuencias. Junio, 2010. ISSN 1794-2918

³² ARENDT, Hannah. Estado Nacional y Democracia. En: ARBOR Ciencia, Pensamiento y Cultura. Marzo, 2010. ISSN 0210-1963, p. 191.

³³ MARTAIN, Jacques. El Hombre y el Estado. Capítulo segundo: El concepto de soberanía. Tercera edición. Buenos Aires: Guillermo Kraft Ltda., 1983, 247 p.

³⁴ MARITAIN, Ibid., p. 66. Con respecto de “poder supremo”, Jacques Maritain menciona que debería ser un poder relativamente supremo, pero que en vez de eso se habla de un poder que es absolutamente supremo y altísimamente cuestionable porque no es un poder que sea ejercido con responsabilidad y que se toma a todo el cuerpo político y al pueblo de manera que absorbe a estos.

³⁵ Es decir que el principal objeto de la jurisdicción deviene en la declaración de la tutela judicial efectiva de los derechos de las partes dentro de un proceso judicial por parte del Estado a través de su poder coercitivo.

sus conflictos³⁶ por medio de las instancias judiciales encargadas por mandato legal para ello.

Ahora bien, un funcionario es competente cuando dentro de sus facultades y la naturaleza de su cargo es conocedor de cierto caso en concreto y, por ende, puede resolver el mismo. En este sentido el Consejo de Estado afirma que es “la medida como la jurisdicción se distribuye entre las distintas autoridades judiciales”³⁷ precisando que la jurisdicción es el género y la competencia es la especie, en atención a la coloquial premisa de que todo juez tiene jurisdicción más no competencia, última que se fija atendiendo ciertas reglas. De esta manera, los factores de competencia, que direccionan el funcionamiento de la estructura de la administración de justicia, además que se indica que no son exclusivos de alguna especialidad jurisdiccional, son los siguientes (i) factor objetivo, (ii) factor subjetivo, (iii) factor territorial, (iv) factor funcional y (v) factor conexidad.

En cuanto al factor objetivo es imperioso especificar que este atiende a la naturaleza del asunto, lo cual supone una específica observancia del “tema litigioso que posibilita realizar una labor de subsunción entre ella y la pretensión en concreto”³⁸, ahora bien, en el derecho penal la naturaleza del asunto está dada por la conducta punible. No obstante, es necesario aclarar, siguiendo a la Corte Suprema de Justicia que “el factor objetivo solamente determina tres variables: especialidad, categoría e instancia que -por sí solas- son insuficientes para adjudicar el expediente a un funcionario judicial en específico”³⁹. De esta manera, si bien es determinarte el factor objetivo para fijar la competencia dentro de una disputa judicial, no es suficiente pues se requiere que también se acompañe del factor territorial.

Ahora, el factor de competencia subjetivo, según lo señalado por la Corte Constitucional, se determina a partir de la calidad de las personas interesadas o parte en el proceso en cuestión⁴⁰; es decir, podemos mencionar que el factor subjetivo de la competencia tiene en cuenta ciertas calidades de las personas que hacen parte del proceso. De igual manera, la Corte Suprema de Justicia ha precisado que el factor subjetivo es aquel por el cual se atiende a la calidad de las

³⁶ ROSERO RICO, Op. cit., p. 29

³⁷ CONSEJO DE ESTADO. Consejero Ponente: Dr. Jesús María Lemos Bustamante. Sentencia de doce (12) de julio de 2007, Ref. expediente 200012331000200101282 01.

³⁸ CORTE SUPREMA DE JUSTICIA. M.P: Luis Alonso Rico Puerta. Sentencia AC1470 de veintiocho (28) de abril de 2021, Radicación No. 11001-02-03-000-2021-01215-00.

³⁹ Ibid., p. 5

⁴⁰ CORTE CONSTITUCIONAL. M.P: Dr. Jorge Ignacio Pretelt Chaljub. Sentencia T- 308 de veintiocho (28) de mayo de 2014.

partes en un proceso, permitiendo fijar la competencia según las condiciones particulares o características especiales de ciertos sujetos.⁴¹

Frente al factor funcional “Este comprende la llamada competencia vertical en contraposición con la horizontal que se presenta en el factor territorial, y comprende tanto la competencia por grado como según la etapa procesal en la que se desenvuelva. También se encuentra este factor de competencia los denominados recursos extraordinarios de casación y de revisión”⁴². Es más, se puede decir que este factor de competencia atiende a las específicas funciones de los jueces en las instancias, que ya han sido previamente determinadas legal o constitucionalmente atendiendo a determinadas situaciones, lo que deriva en los variados grados de juzgamiento en los que se desenvuelven los diferentes funcionarios judiciales⁴³.

Por otro lado, el factor de competencia territorial es aquel en el cual la territorialidad es el criterio principal para determinar este, pues allí se tiene en cuenta en donde se encuentren los elementos del proceso, personas o cosas⁴⁴; en el campo del derecho penal se determina, principalmente, en el lugar de comisión de la conducta punible. Por consiguiente, el artículo 14 del Código Penal (Ley 599 de 2000), precisa que para la determinación del factor territorial se deben tener en cuenta tres componentes, a saber: “i) el lugar en el que se ha ejecutado la acción típica –teoría de la actividad-, ii) el lugar donde se produjo el resultado –teoría del resultado – y iii) el que atiende la equivalencia de acción y resultado, indistintamente – teoría de la ubicuidad.”⁴⁵ A su vez, el estatuto procesal penal en su artículo 43 señala que para fijar la competencia territorial se debe tener en cuenta que el juez a quien le corresponde el juzgamiento de la posible conducta delictual será el del lugar en donde se haya cometido el punible objeto de reproche; sin embargo, cuando no sea posible determinar el lugar en donde se cometió la conducta punible o que la misma se haya cometido en diversos lugares, la competencia del juzgador se determinará en donde se haya formulado la acusación por parte de la Fiscalía.

Ahora bien, normalmente un funcionario judicial es conocedor, haciendo énfasis en materia penal, de la ocurrencia de una sola conducta punible. Sin

⁴¹ CORTE SUPREMA DE JUSTICIA. M.P: Dr. Álvaro Fernando García Restrepo. Sentencia AC140 de veinticuatro (24) de enero de 2020, Radicación No. 11001-02-03-000-2019-00320-00.

⁴² CORTE CONSTITUCIONAL, Op. cit., p. 19

⁴³ CORTE SUPREMA DE JUSTICIA, Op. cit., p. 6

⁴⁴ CORTE CONSTITUCIONAL, Op. cit., p. 1

⁴⁵ CORTE SUPREMA DE JUSTICIA. M.P: Dr. Fernando Alberto Castro Caballero. Auto AP5266 de cinco de diciembre de 2018. Radicación No. 52535.

embargo, muchas veces atendiendo al principio de economía procesal, este puede adelantar el juzgamiento de varias conductas punibles debido a una serie de presupuestos que han de ser tenidos en cuenta al momento de determinar si puede ser procedente darle aplicabilidad al factor de conexidad. Con respecto de este factor de competencia, si bien por cada conducta punible se debe adelantar una actuación procesal, hay circunstancias que hacen posible la configuración de una unidad procesal que permite, según los parámetros de la Ley 906 de 2004, que los delitos conexos se adelanten en una sola investigación penal. Así pues, habrá conexidad cuando (i) el delito hay sido cometido con participación de varias personas, (ii) una persona esté siendo imputada por la comisión de más de un delito; o (iii) se le esté imputando a varias personas la comisión de uno o de varios delitos y haya suficiente relación entre los mismos⁴⁶. Para ello, se atiende a una serie de regladas consagradas en el artículo 52 del mencionado estatuto procesal penal, que corresponden a la atención de lo siguiente (i) juez de mayor jerarquía, pues recuérdese que el que conoce de lo más puede conocer de lo menos; (ii) cuando se este frente a jueces que tiene la misma jerarquía, entonces es prudente definir la competencia en atención a una serie de pasos que son de orden preferente, a saber: el lugar en donde se haya cometido la conducta punible más gravosa; (b) en el lugar en donde se hayan cometido pluralidad de conductas punibles; (c) en donde se haya efectuado la primera aprehensión o captura y (d) en donde primero se haya formulado la acusación.

3. Dilemas de la persecución del *cibercrimen*

Ante la comisión de una conducta dañosa, típica, antijurídica y culpable, el Estado expresa su facultad exclusiva para establecer y aplicar sanciones. El *ius punendi*, es entonces también una potestad atribuida a determinados órganos del Estado que administrarán justicia e impondrán penas y/o medidas de seguridad a personas declaradas responsables de la comisión de conductas contrarias al ordenamiento jurídico. Sin embargo, hay que diferenciar en un primer momento en la distribución del ejercicio de la Jurisdicción, siendo entonces la pertinente en temas de responsabilidad civil contractual por el incumplimiento en garantías de seguridad la empresa TeslaSuit y Google, por otra parte, el Estado podría en simultaneo adelantar la persecución penal por todos los delitos que sean contrarios y se encuentren tipificados en su ordenamiento

De esta manera, el ente investigador en el ejercicio de las facultades que se le otorgan como persecutor de las conductas contrarias a la ley, deberá inicialmente determinar si aquellas se tratan o no delitos conexos en los términos del

⁴⁶ Código de Procedimiento Penal, Ley 906 de 2006, artículo 51.

artículo 51 del código de procedimiento penal. Así, para el concreto la fiscalía general de la Nación deberá establecer si el autor o autores ostentan alguno de los tipos de fuero legal y posteriormente evaluar la naturaleza del delito más gravoso y posteriormente, fijar el lugar de ocurrencia de los hechos.

En este escrito nos compete percibir la dificultad existente en la determinación de la competencia para conductas cometidas bajo el concepto ya determinado de Ciber Crimen. En el caso concreto se plantea la existencia de una dualidad conceptual de conductas, por una parte, la comisión de delitos *ordinarios* mediados por dispositivos de cómputo y por otra, delitos cibernéticos referentes a la transgresión de un sistema de información.

Partamos entonces en los términos del artículo 51 del código de procedimiento penal y se tratase de delitos conexos en tanto el órgano persecutor logro determinar se trata de una comisión en coparticipación criminal, es decir, existen dos o más autores. Sin embargo, el factor de conexidad plantea un importante dilema en materia de competencia en desarrollo del numeral segundo y cuarto del artículo referido con anterioridad, los cuales plantean la posibilidad de imputar a una o más persona la comisión de más de un delito cuyas acciones hayan sido realizadas con unidad de tiempo, lugar y homogeneidad en el modo de actuar. Pues si bien es cierto, existe homogeneidad en la acción, unidad de tiempo en todas las conductas punibles descritas, el lugar en el cual se desarrolló la conducta criminal es difuso. Imagine el lector, el ente persecutor mediante una exhaustiva investigación informática, logró determinar uno de los autores operó desde Ankara, Turquía mientras otro lo hizo desde Râmnicu Vâlcea, Rumania. El factor de competencia por conexidad sería inoperante y lo desnaturalizaría de su propósito, la unidad procesal que permite una investigación conjunta. Tratándose de autores transnacionales, no ostentan fuero legal alguno.

Finalmente, con objetivo de determinar la competencia por factor territorial se encontraría el ente persecutor con la mayor de sus dificultades. Inicialmente remitiéndose al artículo 14 – ya referido en uno de los apartados anteriores – teniendo en cuenta tres componentes: i) el lugar en el que se ha ejecutado la acción típica –teoría de la actividad–, ii) el lugar donde se produjo el resultado –teoría del resultado – y iii) el que atiende la equivalencia de acción y resultado, indistintamente – teoría de la ubicuidad.

Así, referente al numeral primero no existiría consenso en el lugar de ejecución de conducta punible, en tanto para los delitos de secuestro y lesiones personales la ejecución referiría a todos y cada uno de aquellos lugares en donde se encontrase un participante del entorno virtual portador de la tecnología Háptica. Por otra parte, respecto a los delitos contra la información, el lugar de ejecución de la acción correspondería a aquel a partir del cual los autores o

participes accedieron a los sistemas de información, como ya se mencionó con anterioridad correspondería a Turquía y Rumania.

Por otra parte, referente al segundo inciso, el lugar en donde se produce el resultado, para los delitos *ordinarios*, el ente investigador ostentaría la misma dificultad del apartado anterior; sin embargo, enfrentaría un nuevo problema respecto a los delitos mediados por sistemas de cómputo en tanto, para el caso concreto, la vulneración recaería sobre los ordenadores de la transnacional Google, que además, cuenta con repetidores de información alrededor de todo el mundo y sería su deber determinar cuál de ellos soportó el acceso ilegal de los autores.

Por último, la fiscalía general de la nación recurriría como última medida para la definición de la competencia territorial al inciso tercero, el cual responde a la teoría de la ubicuidad y siendo competente el juez del lugar en donde los autores o participes realizaren su acción o en donde se producen sus efectos, y es que intuitivamente plantearía una solución viable al problema sin embargo, bajo la teoría de la ubicuidad, el problema central radicaría en establecer si el delito informático se reputa cometido en el lugar en donde se produce el daño con repercusiones físicas – Lesiones personales, secuestro y homicidio – suponiendo estas sean típicas, en el lugar en donde se vulnera el sistema informático o por el contrario en ambos. Así, el caso expuesto accede a todas las dificultades que supone la aplicación del principio de ubicuidad.

La realización de la acción del delito informático y transgresión a los sistemas de información así como para los delitos *ordinarios* convergerían en parte en un solo lugar, aquel de operación de los autores o participes, sin embargo encontraría una dificultad en tanto para las lesiones personales y al homicidio, respecto a su naturaleza la acción corresponde a aquella que produce directamente el daño, es decir la vulneración al sistema de tecnología háptica y que estaría ligada al mecanismo de producción del resultado.

Por otra parte, los efectos encontrarían pluralidad de ubicaciones. Así para los delitos contra la información como ya se había advertido con anterioridad se encontrarían vulnerados sobre la esfera de operación de los servidores o repetidores de Google, como también el lugar de funcionamiento de cada sistema de tecnología háptica; para los delitos ordinarios los efectos estarían ligados al lugar de producción final del resultado, de esta manera, para el delito de lesiones personales y secuestro corresponde a la ubicación física de cada usuario del entorno virtual; y al de homicidio al lugar en donde se produjo el deceso.

Recurriría finalmente, el operador judicial para determinar la competencia por factor cuantía al artículo 43 del código de procedimiento penal, puesto que al existir pluralidad de lugares y estar estos en el extranjero, sería competente el juez del lugar donde la fiscalía general de Nación radica el escrito de acusa-

ción, lugar que como refiere el artículo debe hacerse en donde se encuentren la mayor cantidad de elementos fundamentales de la acusación.

Es decir, ya no nos encontraríamos frente a un problema netamente de carácter procedimental de definición de competencia, si no de eficacia. El ordenamiento jurídico no está adecuado para enfrentarse a la comisión de conductas del tipo ya descritas, pues remitiéndose siempre del Artículo 43 C.P.P para la definición de competencia demostraría la carencia de especialidad en el tratamiento de dichos punibles, que, además, enfrentarían dificultades de carácter probatorio respecto a la recaudación de elementos de prueba.

Justicia penal y cooperación internacional en materia probatoria

1. Cooperación internacional

La cooperación internacional como lo expresa Alejandra Ripoll y Rafat Gorme citando a Keohane⁴⁷ en su artículo la *Cooperación internacional: herramienta de desarrollo o atraso*, es un sistema estructurado de interacciones que involucran diferentes actores y organizaciones con el fin de equilibrar entre estos ciertos niveles de conformidad recíproca en diferentes temas mediante un proceso de negociación, concepto que concuerda con el estipulado por Ana Chiani⁴⁸ en su libro cooperación internacional puesto que considera que la cooperación internacional son aquellas acciones que son ejecutadas por Estados- nación u instituciones que las representen junto con otros países o autoridades pertenecientes a estos con objetivos en común en ámbitos internacionales que desean ser ejecutados.

Partiendo del anterior concepto es importante esclarecer el modo de intervención de la cooperación internacional y los agentes que pueden ejercer su representación, puesto que al hablarse de un ente internacional encargado de direccionar y aglomerar acuerdos es imprescindible saber el *modus operandi* de su participación. Los actores de la cooperación internacional según Ana Chiani⁴⁹ pueden ser Estados - Nación u organización pertenecientes o cons-

⁴⁷ RIPOLL, Alejandra, GHOTME, Rafat. La cooperación internacional: herramienta de desarrollo o de atraso. En: revista Latinoamericana de Bioética, Vol.15, núm.1, 2015. ISSN: 1657-4702. p. 56.

⁴⁸ CHIANI, Ana María. La cooperación internacional: herramienta clave para el desarrollo de nuestra región. Buenos Aires. Konrad Adenauer – Stiftung. Julio 2009. ISBN 978-987-1285-16-7. p.21

⁴⁹ Ibid.,21.

truidas por estos. La primera es concebida como una cooperación bilateral y la segunda como una cooperación multilateral. Junto a esta clasificación también funcionan figuras como país donante que es aquel país preponderante en su capacidad de desarrollo y tiene mayores recursos para otorgar al país receptor que es considerado como un país menos desarrollado, las herramientas para lograr avanzar a la par. Estas colaboraciones entre país también tienen una clasificación según su estatus, si se trata de un país desarrollado como país donante se estaría dando una cooperación Norte- sur o cooperación vertical y si es un país en proceso de desarrollo, pero con capacidad de brindar ayuda a otro país en desarrollo se trata de una cooperación sur- sur o cooperación horizontal.

La cooperación internacional se desarrolla en diferentes estructuras y entre ellas está la cooperación triangular⁵⁰ puesto que involucra tres intervinientes en el proceso del avance, en este tipo de cooperación un país desarrollado se une con otro que está en proceso de desarrollo con el objetivo de complementarse y brindar en colaboración un mayor aporte. El primero contribuye con recursos económicos mientras que el segundo aporta capacidad técnica alcanzada, de esta forma el país en desarrollo ofrece la capacidad de obtener los medios idóneos para alcanzar los avances de los países donantes y el país en desarrollo al tener más cercanía con el conocimiento de las falencias del país receptor brinda los medios más adecuados para afrontarlas.

La anterior cooperación es el concepto oficial o el más utilizado, estipulado como cooperación centralizada. Ana Chiani⁵¹ nos explica el otro concepto de cooperación que es la cooperación descentralizada o la cooperación no oficial, es aquella realizada por organismos de carácter privado sin fines de lucro (ONG), esta se ofrece a organismos pares con el mismo carácter en vía de desarrollo y puede ser de carácter oficial por medio de relaciones directas o indirectas o de carácter no oficial.

Posterior a explicar las generalidades de la cooperación internacional nos adentraremos en su función en el ámbito penal, como lo establece el compendio normativo de cooperación jurídica internacional en materia penal, la cooperación jurídica internacional en materia penal⁵² es un mecanismo por medio del cual los estados de la comunidad internacional generan estrategias para hacer frente a los delitos en general y en especial sobre aquella delincuencia organizada de manera trasnacional. Este proceso es realizado con el objetivo de

⁵⁰ Ibid., 22.

⁵¹ Ibid., 23.

⁵² Ministerio de relaciones exteriores y culto de argentina. 2022. Compendio de tratados de asistencia jurídica mutua en asuntos penales. Organización de los estados americanos. p. 11. <https://www.oas.org/ext/Portals/33/adam/Content/bhbXarCXFUqWOjxfy1lg/Text/dajin-compendio- penal.pdf>

esclarecer las circunstancias en las que sucede el hecho ilícito, identificar el tipo de participación y someterlo a la jurisdicción del estado requirente correcto.

Partiendo del anterior concepto desarrollaremos los principios extraterritoriales para ejercer competencia, tratados en procesos penales por Francisco Javier Dondé⁵³ en materia de cooperación internacional: (i) *Principio aut dedere aut judicare*, este principio parte de la conexión realizada por medio de tratados internacionales, mediante cláusulas que asignan como obligación enjuiciar a probables responsables de crímenes o delitos, o en caso de no realizarlo, extraditarlos a su país de origen para que los mismos pueden llevar un proceso acorde a su ordenamiento interno y no se permita la impunidad; (ii) *Principio de jurisdicción universal*, definido como el ejercicio de competencia por razón de crímenes realizados, sin importar el lugar de la comisión, la nacionalidad de los sujetos pasivos o activos o los efectos de los mismos, se explica que aquellos delitos sujetos a este principio son los que tienen alcance de protección en bienes jurídicos de carácter internacional y directamente derivan barreras que podrían imposibilitar un juicio.

Partiendo de los anteriores principios se generan los primeros canales que conexión entre los diferentes estados para la construcción de normativas universales con la capacidad de afrontar diversas problemáticas en el ámbito tecnológico, económico, social, ambiental, público, privado y para el caso que nos compete en el ámbito penal. El proceso de construcción de esta estructura internacional es imprescindible en la actualidad puesto que los niveles de desarrollo en los países no están equiparados y sin la cooperación entre los mismos sería imposible hacer frente a las problemáticas del futuro.

2. Cooperación internacional en materia probatoria

En el ámbito probatorio son evidentes las alteraciones en materia de aplicación de la normativa en comparación con pruebas tangibles que son las acostumbradas en los delitos físicos. El recaudo de la prueba, su identificación, clasificación, valoración y la adjudicación de la creación de la misma a lugares o personas se estudian de manera distinta en los delitos físicos y los delitos del *cibercrimen*, surgiendo de allí la necesidad de una cooperación internacional en el ámbito probatorio como lo establece de forma muy apropiada Fernando Valencia⁵⁴, el plasma la funcionalidad de la cooperación internacional como eje

⁵³ DONDÉ, Francisco. Cooperación internacional en materia penal. México. 2013. pp. 7-8, pp. 10-11. ISBN 978-607-02-4921-1

⁵⁴ VALENCIA, Fernando, la cooperación internacional en materia de *cibercrimen* y evidencia digital. En: Revista Saber y Justicia. 18 de mayo de 2022. Vol. 1, núm. 21, 2022. ISSN: 2305-2589. ISSN-e: 2676-0827. p. 32.

principal para enfrentar tanto los obstáculos tradicionales que son los legislativos y judiciales encerrando toda relación trasfronteriza, como los obstáculos materiales referentes a la vinculación o asimilación de la prueba en distintos territorios adjudicados a una o varias personas determinadas y las dificultades técnicas que conlleva el *cibercrimen* en cuanto a la fragilidad, el volumen y la segmentación de la evidencia dentro del ciberespacio.

Como lo manifiesta Fernando Valencia citando a La Oficina de las Naciones Unidas contra la Droga y el Delito⁵⁵, en adelante (UNODC) ha brindado parámetros claros y precisos sobre la presentación de la prueba electrónica a nivel internacional estipulando como criterio clave la definición de la autenticidad e integridad de la prueba desde el inicio de su obtención y los métodos adecuados para su extracción, conservación y análisis. Es importante tener en cuenta que las pruebas tratadas en estos procesos requieren mayor experticia en un área en específico puesto que no es lo mismo la conservación de una bala encontrada en un cadáver a la conservación del volumen, la volatilidad, la velocidad y la fragilidad de los datos que quieren ser presentados como prueba. La (UNODC) expresa con claridad los nuevos retos que se enfrentan en la obtención de pruebas el delito de *cibercrimen* como lo es la naturaleza transfronteriza de la ciberdelincuencia y la variedad de ordenamientos jurídicos en el ámbito probatorio generando impedimentos en la reunión, solicitud y utilización de estas pruebas de carácter electrónico en las etapas procesales correspondientes que deben mantener la línea de la protección de los estados de derecho y los derechos fundamentales.

La mejor ejemplificación de la cooperación en materia probatoria es el “Convenio de Budapest”⁵⁶, convenio sobre la ciberdelincuencia, este constituyendo una herramienta unificadora en la normativa probatoria a nivel internacional estableciendo pautas específicas para el desarrollo de procesos penales que involucren el *cibercrimen* como delito, en su título uno contiene los principios generales relativos a la cooperación internacional desarrollando como ordenanza principal la cooperación de las partes como meta de mayor alcance, instando a los países involucrados a la utilización de los instrumentos internacionales pertinentes sobre la cooperación internacional en materia probatoria junto con los acuerdos de su ordenamiento interno que mantengan de manera uniforme y recíproca las generalidades internacionales, con el objetivo de colaborar en la obtención de pruebas en formato electrónico.

⁵⁵ Ibid. p. 32

⁵⁶ Consejo de Europa. Convenio sobre la delincuencia. Informe. Tratado número 45. p.14.

3. La cooperación internacional y la ciberdelincuencia

Es imprescindible la generación de lazos internacionales que construyan caminos de conexión entre los mismos, permitiendo una mayor cobertura en delitos de *ciberdelincuencia*, al presentarse ante la sociedad un delito intangible permitiendo su presencia o impacto en distintos lugares a la vez, generando pequeños rastros por donde transcurre su impacto se necesita del acceso y la comunicación de varios lugares para lograr una adecuada identificación, como lo establece (UNODC)⁵⁷ se busca armonizar la estructura normativa y toda regulación relacionada con la cibernética, los delitos dependientes de la cibernética y los propiciados a ella, salvaguardando los procesos de futuras contradicciones en su desarrollo puesto que al consolidarse una teoría aplicable de manera universal en relación a la prueba no nos enfrentaríamos a futuros rechazos, inadmisiones o exclusiones de la prueba por entrar en contradicción de ordenamientos de los diversos lugares que se vean involucrados.

A partir de lo anteriormente plasmado es imprescindible la generación de acuerdos de regulación en el ámbito probatorio. Partiendo de la información aportada por Fernando Valencia de la Unión Europea⁵⁸ a través de una encuesta realizada por la misma, que establece que más de la mitad de las investigaciones concluyen en la realización de una solicitud de acceso transfronterizo a pruebas electrónicas y estas pruebas son relevantes en aproximadamente el 85% de las investigaciones criminales, junto a esto en el 65% porcientos de estas investigaciones se necesita la solicitud a entidades oficiales o privadas con base en otra jurisdicción evidenciando una gran dependencia de la cooperación internacional para que los resultados de estas investigaciones desde una posición favorable salgan a flote

Conclusiones

El *ciberdelincuencia* representa un desafío más que significativo para la administración de justicia, diversos factores que facilitan la comisión de delitos a través de las nuevas tecnologías de la comunicación, el uso inadecuado de internet; el surgimiento de tecnologías de inmersión ultra realista; la facilidad para manipular datos y programas hacen que la información y los espacios de seguridad sean más vulnerables al *ciberdelincuencia*.

⁵⁷ Oficina de las Naciones Unidas contra la Droga y el Delito. Serie de Módulos universitarios: Delitos Cibernéticos. Módulo 8: Seguridad Cibernética y Prevención del Delito Cibernético Estrategias, Políticas y programas. 2019. <https://www.unodc.org/e4j/es/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html>

⁵⁸ VALENCIA, Op. cit. p. 33.

Uno de los principales retos que enfrenta la administración de justicia es la determinación de la competencia en casos de *ciberdelitos*. Determinarla bajo los parámetros establecidos en el Artículo 14 de la ley 906 de 2004, plantea el problema central de establecer si el delito informático se reputa cometido en el lugar donde se produce el daño, donde se vulnera el sistema informático, o en ambos. De esta forma la acción típica y transgresión a los sistemas de información convergerían en parte en un solo lugar, el de operación de los autores o partícipes. Sin embargo, encontraría dificultades para los delitos ordinarios como lesiones personales y homicidio, cuya acción corresponde a aquella que produce directamente el daño, es decir, la vulneración al sistema de tecnología como la háptica que ligán directamente al usuario informático de entornos virtuales ultra reales a los mecanismos de producción del resultado.

Así, los efectos de los ciberdelitos encontrarían pluralidad de ubicaciones, encontrándose aquellos vulneradores de la información en la esfera de operación de los servidores o repetidores, así como en el lugar de funcionamiento de cada sistema de tecnología háptica o mecanismos de producción del resultado físico. Para los delitos ordinarios, los efectos estarían ligados al lugar de producción final del resultado.

Finalmente, aunque ineficiente solución, el operador judicial determinaría la competencia bajo los parámetros que establece el artículo 43 del Código de

Procedimiento Penal, ya que al existir pluralidad de lugares en el extranjero, sería competente el juez del lugar donde la fiscalía general de la Nación radica el escrito de acusación, que debe bajo condiciones ideales realizarse en el lugar en donde se encuentren la mayor cantidad de elementos materiales probatorios, aquellos que como se ha ilustrado en circunstancias amparadas bajo el concepto del *ciberdelito* se localizarían dispersas por la naturaleza del hecho.

De esta manera, la naturaleza transfronteriza de la ciberdelincuencia, además de la variedad de ordenamientos jurídicos aun jóvenes en el desarrollo de tipos adecuados a las constantes y emergentes conductas dañosas en los entornos digitales, generan dificultades en la recaudación de elementos materiales probatorios y evidencia física que a su vez se denota torpe en la reunión, solicitud y utilización de pruebas de carácter electrónico en las etapas procesales correspondientes. Estas pruebas requieren mayor experticia en un área específica debido a la fragilidad, el volumen, la velocidad y la segmentación de la evidencia dentro del ciberespacio.

Finalmente, el *ciberdelito* plantea una serie de complejidades que requieren una respuesta integral por parte del sistema de justicia. Es necesario entonces fortalecer los mecanismos de cooperación internacional, actualizar el marco legal y desarrollar capacidades especializadas para hacer frente a esta nueva

forma de delincuencia que trasciende las fronteras físicas. Solo a través de una comprensión profunda de los desafíos que plantea el *cibercrimen* podremos diseñar estrategias efectivas para prevenir y combatir este fenómeno en constante evolución.

Bibliografía

- ADARVE, LAURA. CAMPAZ, MALCOM La Identidad del Sujeto Activo en el Delito de Estafa bajo la Modalidad Virtual Frente al Incumplimiento Contractual de una Transacción Digital en Colombia. Santiago de Cali. 2021
- AGUILAR, M. M. (2015). *Cibercrimen* y ciber victimización en Europa: instituciones involucradas en la prevención del ciberdelito en el Reino Unido. Revista Criminalidad.
- ALVARADO VELLOSO, Adolfo. Jurisdicción y competencia [Online] [Citada 17/04/2024]. https://campus.academiadederecho.org/upload/Cvaav/Pdf/NF%200AD/Ad/Jurisdiccion_y_CompetenciaAAV.pdf
- ARENDT, Hannah. Estado Nacional y Democracia. En: ARBOR Ciencia, Pensamiento y Cultura. Marzo, 2010. ISSN 0210-1963
- BECK, Ulrich. La sociedad del riesgo. Barcelona: Paidós. 1998.
- CÁMARA ARROYO, Sergio. Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. En: Derecho y cambio social. Abril, 2020. ISSN 2224-4131.
- CÁRDENAS, A. y Cárdenas, C. Módulo Penal. En: Núcleos problemáticos (Módulos siglo XXI) (pp. 41-52). Bogotá: Universidad Santo Tomás. 2002.
- CHIANI, Ana María. La cooperación internacional: herramienta clave para el desarrollo de nuestra región. Buenos Aires. Konrad Adenauer – Stiftung. Julio 2009. 21p. ISBN 978-987-1285.
- CONSEJO DE ESTADO. Consejero Ponente: Dr. Jesús María Lemos Bustamante. Sentencia de doce (12) de julio de 2007, Ref. expediente 200012331000200101282 01
- CONSEJO DE EUROPA. (185:2001: Budapest) Convenio sobre la ciberdelincuencia. Budapest: Serie de tratados europeos, 2001. pp. 26.
- Consejo de Europa. Convenio sobre la delincuencia. Informe. Tratado número 45.
- CORTE CONSTITUCIONAL. M.P: Dr. Jorge Ignacio Pretelt Chaljub. Sentencia T- 308 de veintiocho (28) de mayo de 2014.

- CORTE SUPREMA DE JUSTICIA. M.P: Dr. Álvaro Fernando García Restrepo. Sentencia AC140 de veinticuatro (24) de enero de 2020, Radicación No. 11001-02- 03-000-2019-00320-00.
- CORTE SUPREMA DE JUSTICIA. M.P: Luis Alonso Rico Puerta. Sentencia AC1470 de veintiocho (28) de abril de 2021, Radicación No. 11001-02-03-000-2021- 01215-00.
- CORTE SUPREMA DE JUSTICIA. M.P: Dr. Fernando Alberto Castro Caballero. Auto AP5266 de cinco (05) de diciembre de 2018. Radicación No. 52535
- DENNIS, Michael Aaron. *Cibercrimen*. En: Encyclopedia Britannica. Junio, 2024. p. 4.
- DEVIS DE ECHANDIA, Hernando. Teoría general del proceso. Tercera Edición. Buenos Aires: Editorial Universidad.
- DONDÉ, Francisco. Cooperación internacional en materia penal. México. 2013. ISBN 978-607-02-4921-1
- EUROPOL. Internet Organised Crime Threat Assessment (IOCTA). Luxemburgo: Publications Office of the European Union, 2021. 19p. ISBN 978-92-95220-35-5.
- GARAVITO, Daniel. Emociones, responsabilidad penal y política criminal. Tunja: Ediciones USTA. 2022.
- GARCÍA-PABLOS DE MOLINA, Antonio. Tratado de criminología. Valencia: Tirant Lo Blanch. 2003. P.47.
- GONZALO IBAÑEZ, Santa María. Revista chilena de derecho.
- GORDON, Sarah y FORD, Richard. On the definition and classification of cybercrime. En: J Comput Virol. Febrero, 2006. Vol. 2. DOI: 10.1007/s11416-006- 0015-z.
- KAUFMANN, Arthur. Filosofía del derecho. Bogotá: Universidad Externado de Colombia. 1999.
- Manjarrés, I & Jiménez, F. (2012). Caracterización de los delitos informáticos en Colombia. Pensamiento Americano.
- MANZINI, Vincenzo, Tratado de derecho procesal penal, II, Ediciones de Cultura Jurídica, 1998,
- MARCIO CRUZ, Paulo. Soberanía y transnacionalidad: Antagonismos y consecuencias. Junio, 2010. ISSN 1794-2918.
- MARITAIN, Jacques. El Hombre y el Estado.
- Ministerio de relaciones exteriores y culto de argentina. 2022. Compendio de tratados de asistencia jurídica mutua en asuntos penales. Organización de los estados americanos. <https://www.oas.org/ext/Portals/33/adam/Content/bhbXarCXFUqWOffjxfy1lg/Text/d ajin-compendio-penal.pdf>

- MIR PUIG, Santiago. Derecho penal. Parte General. Barcelona: Reppetor. 2016
- NACIONES UNIDAS. Estudio exhaustivo del problema del delito cibernético y las Oficina de las Naciones Unidas contra la Droga y el Delito. Serie de Módulos universitarios: Delitos Cibernéticos. Modulo 8: Seguridad Cibernética y Prevención del Delito Cibernético Estratégias, Políticas y programas. 2019. <https://www.unodc.org/e4j/es/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html>
- PHILLIPS, Kristy. DAVIDSON, Julia. FARR, Ruby. R. BURKHARDT, Christine. CANEPPELE, Stefano. y AIKEN, Mary. Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. En: Forensic Sci. Abril, 2022, vol. 2, no.1 pp. 379-398. DOI: <https://doi.org/10.3390/forensicsci2020028>
- POSADA AMAYA, RICARDO El *cibercrimen* y sus efectos en la teoría de la tipicidad de una realidad física a una realidad virtual en: Nuevo Foro Penal Enero- junio, 2017, vol. 13, No. 88. ISSN 0120-8179.
- RAYÓN, M y GÓMEZ, J. *Cibercrimen*: particularidades en su investigación y enjuiciamiento. En: Anuario Jurídico y Económico Escurialense. 2014. XLVII. 209- 234. ISSN: 1133-3677.
- Respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno. Viena: UNODC, 2013. 18p.
- RIPOLL, Alejandra, GHOTME, Rafat. La cooperación internacional: herramienta de desarrollo o de atraso. En: revista Latinoamericana de Bioética, Vol.15, núm.1, 2015. ISSN: 1657-4702.
- ROSETO RICO, Dairo Andrés. La unidad de la jurisdicción en el Estado colombiano. Una mirada a partir de la Constitución Política de 1991. La jurisdicción. En: Diálogos de Derecho y Política. Abril, 2014, no. 13 ISSN 2145-2784.
- TABLA 3. Extraída de: CHIANI, Ana María. La cooperación internacional: herramienta clave para el desarrollo de nuestra región. Buenos Aires. Konrad Adenauer – Stiftung. Julio 2009. 24p. ISBN 978-987-1285-16-7.
- TEMPERENI, MARCELO *CIBERCRIMEN Y DELITOS INFORMÁTICOS*. Los nuevos tipos penales en la era de internet. Buenos Aires, Argentina: talleres gráficos de BluePress SA, Buenos Aires, 2018. 196p, ISBN 978-987-4405-56-2.
- VALENCIA, Fernando, la cooperación internacional en materia de *cibercrimen* y evidencia digital. En: Revista Saber y Justicia. 18 de mayo de 2022. Vol. 1, núm. 21, 2022. ISSN: 2305-2589. ISSN-e: 2676-0827.
- VELÁSQUEZ VELÁSQUEZ, Fernando. Manual de Derecho Penal. Parte General. Bogotá, D.C.: Ediciones Jurídicas Andrés Morales. 2013