TRABAJO FINAL DE LA

CARRERA DE ESPECIALIZACIÓN EN CIBERCRIMEN

ALUMNA: CONSUELO ALIAGA DÍAZ

AÑO 2022

EL FUTURO DE LA COOPERACIÓN PENAL INTERNACIONAL PARA LA INVESTIGACION DE CIBERDELITOS EN EL SEGUNDO PROTOCOLO ADICIONAL AL CONVENIO DE CIBERCRIMINALIDAD

El empoderamiento de las autoridades judiciales, la voluntad política del poder ejecutivo nacional y la creciente importancia de los Equipos Conjuntos de Investigación, Interpol e institutos como el EC3

I. INTRODUCCIÓN

1. Antecedentes:

Este trabajo se centra en la transnacionalidad de los delitos informáticos. Las tecnologías de la información han extendido su brazo facilitador a todas las formas de criminalidad organizada transnacional. Si bien los delitos informáticos por definición no se limitan a aquellos que se cometen en Internet, los mismos son los predominantes e ingresan a las agendas de los gobiernos a partir de la apertura comercial de Internet. Éstos poseen ciertas características generales a partir del entorno virtual donde se produce gran parte de estas conductas.

En materia de narcotráfico, la aparición de Internet como medio de comunicación representó una herramienta útil en términos de distribución y venta de sustancias ilícitas. Si bien históricamente el crimen organizado usó las tecnologías de la época para el desarrollo de sus operaciones, Internet, en tanto herramienta flexible y descentralizada, parece adaptarse mucho más a la forma de organización de estos grupos que operan horizontalmente. Ocurre lo mismo con los delitos de abuso y explotación sexual del que resultan víctimas niños y personas vulnerables a través de internet.

También las maniobras de blanqueo de capitales para los fondos provenientes del narcotráfico y de otros ilícitos rentables, para desarrollar el proceso por el cual los fondos pasan al sistema financiero legal para ser usufrutuados, se valen del uso de tecnologías digitales para el blanqueo de fondos de origen ilegal, lo que se conoce bajo el nombre de “ciberlavado”.

A partir de la popularización de Internet, además del anonimato, la segunda característica que los distingue es la transnacionalidad en tanto que

pueden afectar a varios dispositivos a la vez en diferentes partes del mundo, configurándose un medio nuevo para la comisión de delitos tradicionales como las amenazas, los fraudes o los delitos sexuales con repercusiones en diversos lugares simultáneamente. Ello, además de que el cibercrimen ha dado lugar a nuevas figuras delictivas a partir de la elaboración y distribución de programas maliciosos, tales como virus, gusanos, troyanos, etc., de modo que sin la tecnología informática no sería posible su existencia y distribución.

A su vez, si bien el delito informático parece surgir como un delito ocupacional de tipo profesional en tanto los primeros usuarios de Internet eran en su mayoría ingenieros, programadores y especialistas que desarrollaban su actividad en el marco de un proyecto gubernamental que requería secretismo, con el surgimiento del Word Wide Web en 1990 y la posterior apertura comercial de la red Internet por parte del Gobierno de los Estados Unidos en 1995 hizo que la informática se popularizara para extenderse al uso laboral y hogareño. En la actualidad cualquier persona con conocimientos básicos en computación puede cometer conductas indebidas.

La situación problemática se genera cuando los Estados, auto limitados por los sistemas jurídicos penales territoriales propios del concepto de soberanía nacional, comienzan a evidenciar la preocupación por establecer mecanismos de cooperación internacional para afrontar adecuadamente este fenómeno.

A principios del siglo XXI y del milenio, esta preocupación se cristalizó en diversos Convenios internacionales dirigidos a combatir distintos aspectos de la criminalidad organizada transnacional, entre ellos, el tráfico ilícito de estupefacientes, el blanqueo de capitales de origen delictivo, la trata de personas con fines de explotación sexual o laboral, y por supuesto, los delitos informáticos, a partir del Convenio sobre Cibercriminalidad del Consejo de Europa de 2001, un hito sin precedentes por tratarse del primen tratado internacional en la materia en todo el mundo. Es importante destacar, como veremos, que los redactores este Convenio, evidentemente conscientes del problema de la transnacionalidad y la necesidad de cooperación en las investigaciones, si bien asignaron una importante cantidad de normas a esta temática incorporando herramientas novedosas en relación lo que se acostumbraba en los tratados bilaterales de cooperación penal existentes a este momento, tal como veremos, las mismas resultaron insuficientes.

Es decir, en el contexto internacional sucede que el sistema occidental, también está compuesto por un orden jurídico basado en la concepción

tradicional del Estado donde priman los conceptos de territorio y soberanía. No escapa a esta característica el Convenio de Budapest de 2001. De tal forma, los ordenamientos jurídicos del sistema internacional occidental presentan limitantes al momento de correlacionarse, motivo por el cual los tratados y convenciones están marcados por la "buena voluntad" de las partes contratantes, asunto que termina desconociendo la necesaria "plasticidad del derecho estatal moderno" como una forma de articulación entre los diferentes ordenamientos jurídicos nacionales para enfrentar una amenaza transnacional.

2. Definición del problema

El problema que aquí se plantea, se enmarca en el problema más general de derecho internacional, según el cual, el control de los Estados sobre el sobre el espacio y el tiempo se ha visto superado por los diferentes flujos globales de capital, bienes, servicios, tecnología, comunicación y poder, no obstante lo cual las respuestas de los Estados nación son inadecuadas por su resistencia a la flexibilización de su soberanía. De ese modo, los Estados nación terminan auto limitándose a partir de una escala espacio temporal que se ha impuesto durante los últimos doscientos años y que configuró una concepción político-ideológica que convirtió al Estado en la única y exclusiva fuente de derecho.

En ese marco, en materia de cibercrimen, dado que los servicios basados en la red pueden prestarse desde cualquier lugar y no requieren infraestructura física, instalaciones o personal en el país en cuestión, las pruebas pertinentes a menudo se almacenan fuera del Estado investigador o por un proveedor de servicios establecido fuera de dicho Estado. Entonces, con frecuencia no existirá ninguna otra conexión entre el caso investigado en el Estado en cuestión y el Estado del lugar de almacenamiento o de establecimiento del proveedor de servicio.

Debido a ello, las solicitudes de cooperación se remiten frecuentemente a Estados que acogen a un gran número de proveedores de servicios sin relación con el asunto en cuestión. Además, el número de solicitudes se han multiplicado debido al mayor uso de servicios de red, que por su naturaleza no tiene fronteras. En consecuencia, la obtención de pruebas electrónicas utilizando canales de cooperación judicial a menudo lleva mucho tiempo, más del tiempo que en podrían estar disponibles los indicios.

De igual manera ocurre con los datos almacenados en los dispositivos físicos de un sospechoso con domicilio en el extranjero, ya que las autoridades judiciales locales (los fiscales) ya que para la solicitud de medidas con alto

grado de intrusión en la intimidad del sospechoso, como lo es un allanamiento, una incautación o una intervención de comunicación telefónica o cibernética, se exige la utilización de exhorto de asistencia internacional con intervención de cancillería, el cual genera demoras excesivas que superan el año de duración. En este punto, por más que el Convenio de 2001 intentó medidas superadoras con la regulación de la Autoridad Central uy el Punto de Contacto de la Red 24/7, en la práctica, estos instrumentos no consiguieron reemplazar la exigencia de los exhortos tradicionales porque durante estos veinte años el concepto de soberanía estricta y los controles del orden público interno continuaron teniendo fuerte presencia, incluso en la propia legislación internacional.

Al formular este problema, no puede dejar de hacerse una breve referencia a la clasificación más extendidas de los datos de interés para las investigaciones penales, en datos de abonados, datos de acceso, datos de transacciones y datos de contenido. Al respecto, puede afirmarse por resultar un hecho notorio que no requiere demostración, que las mayores dificultades de los investigadores locales se dan al momento de procurar acceder a los datos de contenido, ya sea que se encuentren alojados en proveedores de servicios con sede en el extranjero, ya sea que se encuentren en los dispositivos electrónicos de un sospechoso con domicilio en el extranjero, o, en su caso, ya sea que se encuentren en los dispositivos de las víctimas o testigos con sede en el extranjero, salvo que mostraran su voluntad de colaborar espontáneamente. Finalmente, valga señalar que los datos de contenido, si bien, a diferencia de los datos de tráfico y de los abonados no son útiles para localizar un sospechoso, sí suelen ser los más buscados por los investigadores por su riqueza probatoria, contenidos de conversaciones, imágenes, fotografías, conteniendo a su vez metadatos que podrían resultar sumamente relevantes.

En esta problemática no puede soslayarse referir que el Convenio sobre Cibercriminalidad del Consejo de Europa (Budapest, 2001) se ocupó especialmente de establecer algunos mecanismos de cooperación penal internacional en la teoría de percibieron de avanzada con la utilización de la figura de la Autoridad Central que cada Estado parte debía designar ante el Secretario General, con la función específica de tramitar las solicitudes de cooperación en los términos del acuerdo. Igualmente, se consideró un avance el establecimiento del Sistema de la Red 24/7 para emergencias, a cuyo fin cada Estado parte debía designar un Punto de Contacto disponible en todo momento para la atención de las solicitudes.

Ahora bien, no obstante ello, con el transcurrir de los años hasta la fecha, la evidencia de la insuficiencia de ese sistema de cooperación para la investigación penal y la obtención de prueba transnacional -tal el objeto de este trabajo- diseñado en el Convenio en la práctico, se hizo evidente a partir de la cantidad y diversidad de reglamentaciones, acuerdos e instituciones que se fueron dictando en el ámbito mismo del Consejo de Europa, para superar las deficiencias hasta llegar a la redacción del Segundo Protocolo Adicional al Convenio sobre cooperación reforzada.

Al respecto, una explicación de aquel fracaso, por llamarlo de alguna manera, no parece encontrarse en el sistema en sí mismo cuyo mecanismo aparece idóneo en miras de acelerar y volver más eficiente los procesos de solicitud y entrega de información, datos o pruebas, sobre todos, si se lo compara con los antiguos tratados de cooperación penal que solo daban la opción de la solicitud de asistencia internacional. Entonces, descartada esa causa, no queda otra que atribuirla a la inacción de los destinatarios de la normativa, esto es, a los Estados, que en este tiempo no han asumido con la fuerza y el compromiso político que requiere la competencia que les cabe al momento de contribuir para hacer efectivos los mecanismos. Es decir, sin la voluntad política del Estado parte no hay posibilidad de que funcione ningún mecanismo internacional de cooperación por bien orquestado que se encuentre. En este punto, dable es suponer que, aun conscientes de estar incurriendo en responsabilidad internacional por esa inercia, termina dominando en la decisión gubernamental nacional la concepción de restrictiva de la soberanía nacional en protección de supuestos intereses de los connacionales que, como veremos, ya no requieren dicha tutela.

Finalmente, solo resta aclarar al lector que este trabajo no tiene una perspectiva técnica ni operativa sino de estrategia política sobe la cooperación, por lo que no es objeto de mismo, profundizar en el desarrollo de ningún medio de prueba en particular ni en relación a procedimiento de obtención de prueba alguno, sino que, por el contrario, el enfoque está puesto la evolución de la política criminal a nivel internacional en materia de cooperación penal para la investigación de ciberdelitos, a partir de un análisis de los principales instrumentos a los que los Estados, en particular la República Argentina, se han adherido, durante los últimos veinte años. De esa manera, se obtiene la información necesaria para explicar cuáles fueron los aciertos y los errores del pasado, como así también, cuáles son las medidas correctivas del presente, para así, llegar a un pronóstico fundando acerca del futuro próximo de la cooperación internacional penal a través de las normas, procedimiento e

institucione, las que contribuirán a un mejoramiento sustancial del sistema de la cooperación penal internacional.

3. El objetivo de la investigación

El objetivo central de este trabajo consiste en demostrar que, a partir de la Adhesión de la República Argentina al Segundo Protocolo Adicional al Convenio de 2001, los operadores judiciales cuentan desde ya -y más allá de la legislación interna que deba dictarse-, con el acceso a una serie de mecanismos que tienen potencial para provocar un mejoramiento sustancial del sistema de la cooperación penal internacional en las investigaciones penales. Ahora bien, como parte de ese mismo objetivo, se demostrará que, no obstante ello, será condición necesaria el apoyo político de las autoridades del poder ejecutivo que, según su área de incumbencia y la responsabilidad internacional que les cabe, deberán brindar apoyo político dictando las instrucciones, directivas o reglamentos necesarios a fin de poner en funcionamiento efectivo esos mecanismos.

Como vemos este objetivo único presenta varios aspectos interdependientes y complementarios entre sí que se pasan a explicar. Así, se determinará que el nuevo instrumento brinda protagonismo a las autoridades judiciales locales, empoderándolas para actuar directamente hacia el exterior solicitando y remitiendo prueba en las investigaciones penales, sin visado ni control de los órganos de cancillería.

Es establecerá que ello requiere, no obstante, el diseño de una política al más alto nivel de autoridades del MPF provinciales o nacional según el caso -Fiscalías Generales-, que incluirá una toma de conciencia sobre la incumbencia, asumiendo la obligación con toda la fuerza y seriedad que son requeridas, para luego impartir las instrucciones necesarias a sus subordinados. Las directivas serán ser coherentes con el espíritu del Segundo Protocolo, tanto al momento de habilitar a los fiscales para actuar directamente solicitando o remitiendo datos electrónicos hacia el exterior, como al momento de Equipos Conjuntos de Investigación y promocionar una actitud de socialización institucional sostenida en el tiempo con organismos de la cooperación penal internacional de relevancia en la actualidad, como lo es Interpol y el EC3.

Se demostrará, en esta línea, que no se trata de una simple recomendación que surge de la normativa internacional, sino que ha emergido para el Estado argentino una auténtica obligación susceptible de generar responsabilidad internacional en caso de incumplimiento.

En la misma dirección, determinaré que, para la efectiva implementación de esos mecanismos, se requiere el accionar conjunto con los otros poderes del Estado, en sintonía política con la nueva tendencia internacional para la cooperación penal, en razón de las incumbencias que tiene el poder ejecutivo a través del Ministerio de Relaciones Exteriores y Culto, del Ministerio de Justicia y Derechos Humanos, del Ministerio de Seguridad y del Ente Nacional de comunicaciones en conjunto con la Dirección de ciberseguridad dependiente de la Jefatura de Gabinete de Ministros, en cuyos ámbitos actúan la Autoridad Central y el Punto de Contacto de la Red 24/7 en cumplimiento del Convenio de 2001, como así también, se tramitarán las relaciones con la oficina nacional de Interpol y bajo cuya órbita (ENACOM) deben controlarse los proveedores de servicios de comunicaciones electrónicas. Pues, todos estos organismos configuran engranajes fundamentales en la logística necesaria para implementar los mecanismos avanzados de cooperación.

En definitiva, entonces, el objetivo de este trabajo será demostrar que, más allá de los lineamientos jurídicos para los operadores judiciales que emergen del Segundo Protocolo Adicional, el instrumento impone una serie de obligaciones adicionales tácitas que recaen, también, en otros poderes del estado y demandan un alineamiento comprometido con las políticas de máxima cooperación. En esa línea, se harán explícitas en este trabajo algunas de esas obligaciones tácitas, en base a las cuales, se efectuarán recomendaciones y se dejarán sentadas las bases para futuras investigaciones.

Para concluir con los aspectos del objetivo central -facetas de una misma solución- se reafirmará que, como dije antes, sin el apoyo político del Estado en sus distintas funciones, ninguna posibilidad de éxito tienen los nuevos mecanismos previstos. Las denuncias y declamaciones de preocupación por el flagelo de los delitos transnacionales potenciados por las nuevas tecnologías y la insuficiencia de la respuesta penal al 2021, tal como que se plantean en el Preámbulo del Segundo Protocolo y en su video de presentación, deja en evidencia que el Estado parte no tiene margen para desatender su compromiso sin incurrir en responsabilidad internacional.

II. ANÁLISIS DE FUNDAMENTOS: EL MARCO CONCEPTUAL, EL MARCO NORMATIVO Y EL MARCO TEÓRICO DE LA INVESTIGACIÓN

El marco conceptual de este trabajo está conformado por los siguientes conceptos técnicos: delitos informáticos transnacionales; derecho penal

transnacional; cooperación penal internacional; datos de contenido almacenados en el extranjero; proveedor de servicios con sede en el extranjero; autoridad central y punto de contacto de la Red 24/7; autoridades judiciales, autoridades competentes del poder ejecutivo nacional, Ministerio Público Fiscal, Organización Internacional de Policía Criminal (Interpol); European Cybercrime Center (EC3); Equipos Conjuntos de Investigación (ECI).

En lo relativo al marco normativo, esta investigación se basa, en lo sustancial, en las siguientes convenciones y reglamentos: Convención de Cibercriminalidad del Consejo de Europa (Budapest, 2001); Segundo Protocolo Adicional al Convenio de 2001 sobre cooperación reforzada (2022); Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional y sus protocolos (2000); la Propuesta de Reglamento del Parlamento y del Consejo de Europa sobre orden de conservación y orden de entrega de pruebas electrónicas (2018); y la Guía del MPF de la Nación sobre cooperación penal internacional y Equipos conjuntos de Investigación.

En lo relativo al marco teórico de esta investigación, vale explicar que en este acápite desarrollaré algunas elaboraciones de la doctrina que se han ocupado de problemáticas semejantes a la planteada en este trabajo, aunque no están referidas específicamente al fenómeno de los delitos informáticos con el enfoque se realiza en este trabajo, puesto que es allí justamente donde efectuaré mi aporte. Del análisis de fuentes pude comprobar que es profusa la producción científica de juristas que han trabajado en ese sentido durante los últimos diez años, lo que a mi entender encuentra explicación, lógicamente, en la proliferación de los delitos transnacionales y las dificultades actuales de los Estados para hacer frente al fenómenos de manera adecuada.

1. El derecho penal transnacional y del derecho penal internacional.

Afirman este doctrinario del derecho internacional público (1) que entre las causas de la transformación de la criminalidad en la sociedad global se ubican la facilidad de movimientos de personas y cosas que caracteriza la globalización; el avance de las telecomunicaciones que provoca nuevas formas de criminalidad a través de sistemas informáticos y de comunicaciones; el incremento de la actividad económica que aumenta los delitos económicos; entre otros.

A este respecto, explica que el Derecho penal clásico, limitado al territorio nacional, no puede contener de manera suficiente este tipo de delincuencia, ante lo cual se han implementado algunos mecanismos para combatir la delincuencia transnacional: a) Ampliar la jurisdicción nacional más

allá del principio de territorialidad, que también se ha visto ampliado con la asunción del principio de ubicuidad, adoptando los Estados principios tales como los de personalidad activa y/o pasiva, de protección de intereses o de justicia universal. b) La aprobación de instrumentos de lucha contra la criminalidad de carácter supranacional, especialmente en dos niveles: 1. En el ámbito del Derecho penal transnacional sustantivo para establecer criterios uniformes, a través de mecanismos de armonización de las figuras típicas y de atribución de responsabilidad penal; y 2. En el ámbito del Derecho penal transnacional procesal se trataría de elaborar instrumentos eficaces de cooperación penal internacional, como son los tratados de extradición y auxilio judicial que incluyen las comisiones rogatorias, la notificación de documentos y resoluciones judiciales, la comparecencia de peritos, testigos y acusados, etc.

Nadie desconoce ya que la globalización conduce a que la importancia de la legislación penal y de la política criminal del Estado nacional disminuya, siendo la "interlegalidad" el fenómeno clave del derecho penal de la globalización, lo cual conduce a nuevos agentes, formas, orientaciones y contenidos de la legislación penal. En esta línea, explicita la diferenciación conceptual entre el Derecho penal transnacional, como aquél referido los crímenes transnacionales y el Derecho penal internacional, como aquél referido los crímenes internacionales stricto sensu.

Es decir, que mientras el Derecho penal internacional abarca una serie de delitos regulados en el Tratado de Roma de la Corte Penal Internacional, firmemente asentados en el Derecho internacional consuetudinario por afectar a bienes jurídicos especialmente significativos de la comunidad internacional en su conjunto; el Derecho penal transnacional es un sistema de obligaciones interestatales que dan lugar a leyes penales nacionales.

Afirma el autor, que los tratados internacionales que se ocupan de los crímenes transnacionales únicamente imponen obligaciones a los Estados parte de aprobar e implementar ciertos mecanismos de lucha contra la criminalidad, por ejemplo, a tipificar determinadas conductas. El incumplimiento de dichos tratados dará lugar únicamente a responsabilidad internacional del Estado y la persecución de las conductas delictivas se llevará a cabo cuando el Estado haya incorporado a su ordenamiento penal nacional las disposiciones del tratado. A su vez, los crímenes transnacionales protegen bienes jurídicos de un segundo nivel, ya que no se trata de la protección de la comunidad internacional o la humanidad como tal, y comprenden conductas cuyo elemento común es que afectan a intereses de carácter social, económico, cultural o de otro tipo que conciernen a todos o a un número muy significativo de Estados.

Entonces, explica, existe un doble fundamento para la represión de las conductas que integran el denominado Derecho penal transnacional:

a) Por un lado, los delitos transnacionales surgen para reprimir conductas con un elemento transfronterizo, elemento transnacional fáctico, bien porque el hecho se realiza en más de un Estado, bien porque se comete en un Estado pero una parte sustancial de su preparación, planificación, dirección o control se ha llevado a cabo en otro Estado; bien porque se comete en un Estado pero involucra a un grupo criminal organizado que lleva a cabo actividades delictivas en más de un Estado; o bien porque se comete en un Estado pero tiene efectos relevante sobre el territorio de otro Estado.

b) Por otro lado, también pueden ser considerados delitos transnacionales aquellos que, sin requerir la existencia de un elemento transfronterizo, pretenden evitar y reprimir conductas cuya comisión produce tal rechazo que existe un consenso internacional sobre su ilegalidad, elemento transnacional normativo, que estará vinculado normalmente a la violación de derechos humanos, por ejemplo, la prohibición de la tortura, la trata de seres humanos o el terrorismo, pero ello no es un requisito necesario.

Así las cosas, las dos organizaciones internacionales más activas en este cometido son la Organización de Naciones Unidas y el Consejo de Europa. La primera, lidera la promoción de convenios internacionales de carácter universal, especialmente en materia de lucha contra el terrorismo, el crimen organizado, la corrupción, la piratería o el tráfico de drogas. Por su parte, en el seno del Consejo de Europa se han aprobado convenios internacionales de ámbito regional en materia de corrupción, el blanqueo de capitales, la cibercriminalidad, la trata de seres humanos, o la explotación sexual infantil.

A su vez, el art. 83.1 TFUE autoriza la aprobación de normas sobre hechos graves que tengan una dimensión transfronteriza, tales como: a) terrorismo; b) la trata de seres humanos y la explotación sexual de mujeres y niños; c) el tráfico ilícito de drogas; d) el tráfico ilícito de armas; e) el blanqueo de capitales; f) la corrupción; g) la falsificación de medios de pago; h) la delincuencia informática; e i) la delincuencia organizada, a las cuales el Consejo podrá agregar otras.

En cuanto al principal problema de este modelo de Derecho penal transnacional, lo encuentra en que su eficacia depende en gran medida de la voluntad soberana de los Estados, los cuales deben, en primer lugar, ratificar los Convenios y luego convertirlos en Derecho nacional. Además, si en un determinado momento se produce un cambio de criterios, siempre se puede denunciar el convenio en cuestión, o simplemente no aplicarlo, en cuyo caso

únicamente quedaría el recurso a las reglas de Derecho internacional sobre incumplimiento de obligaciones internacionales por parte de un Estado miembro.

2. El Estado frente al crimen organizado transnacional (COT)

Nadie duda a estas alturas, como refiere Piedrahita Bustamante (2), que el control de los Estados sobre el espacio y el tiempo se ha visto superado por los diferentes flujos globales de capital, bienes, servicios, tecnología, comunicación y poder, pero, paradójicamente, las respuestas de los Estados nación a su crisis siguen una doble vía de resistencia y flexibilización de su soberanía. De ese modo, los Estados nación terminan auto limitándose a partir de una escala espacio temporal que se ha impuesto durante los últimos doscientos años y que configuró una concepción político-ideológica que convirtió al Estado en la única y exclusiva fuente de derecho.

A la vez, explica el autor, si se analiza el contexto internacional sucede algo similar, pues el sistema occidental está compuesto por un orden jurídico basado en la concepción tradicional del Estado donde priman los conceptos de territorio y soberanía. De tal forma, los ordenamientos jurídicos del sistema internacional occidental presentan limitantes, motivo por el cual los tratados y convenciones están marcados por la "buena voluntad" de las partes contratantes, asunto que termina desconociendo la necesaria "plasticidad del derecho estatal moderno" como una forma de articulación entre los diferentes ordenamientos jurídicos nacionales para enfrentar una amenaza transnacional.

Considera que el Estado nación puede superar su crisis en la medida que se reconozca una soberanía fragmentada que permita no sólo la hibridación del derecho, sino la hibridación de las instituciones y funciones estatales en materia de seguridad y persecución del delito transnacional. Es decir, los Estados deben migrar a una operatividad en red, tal y como lo hacen los grupos asociados al crimen organizado transnacional. Un Estado jerárquico, vertical, nacional, aunque tenga las herramientas jurídicas, no posee la capacidad para enfrentar las redes del crimen global.

En ese orden, debe partirse del supuesto de que la conformación y estructura del crimen organizado en el orden mundial de posguerra fría, puede afirmarse como generalmente reconocido en su importancia y en la realidad de este fenómeno, atestiguado por abundantes datos, principalmente de informes periodísticos bien documentados y de las conferencias de las organizaciones internacionales. Se caracteriza por ejercicios de intimidación violenta y su capacidad de corromper a funcionarios de gobiernos o líderes de opinión de los países, sin fines ideológicos sino meramente económicos.

Entonces, concluye el autor, como salida política y jurídica al problema, además del Protocolo de Palermo y otros muchos instrumentos del Derecho Internacional referentes a los delitos asociados al COT, en el marco legal es necesario establecer mecanismos de control real y efectivo, enfatizando en la obligación de los Estados en la cooperación y la coordinación operativa, las actividades de análisis conjunto, la evaluación y el control, la transferencia de técnicas y métodos, la formación y el intercambio de expertos, así como las actividades de sensibilización y difusión.

En particular, es necesario deconstruir los instrumentos judiciales y los conceptos de jurisdicción y competencia para que efectivamente se sancionen estas conductas. Por esto es por lo que se afirma que la salida política al problema de la crisis del Estado pasa por una necesaria fragmentación de la soberanía. Es necesario que los Estados establezcan mecanismos de soberanía compartida, una hibridación del derecho y de los organismos de seguridad para enfrentar el delito.

Afirma la convicción de que los organismos de seguridad que funcionan como componentes de la aplicación de la justicia no pueden proceder solos, pues sin la acción judicial posterior es inocua su actuación. Pero tampoco puede descansar todo el peso del control criminal transnacional en las normas, las acciones policiales y el uso del derecho a la fuerza y a la sanción, sino que deben darse otro tipo de acciones estatales y de cooperación real de los Estados para combatir la delincuencia más allá de los lineamientos ideológicos de los gobiernos. Es el Estado como una totalidad el que debe responder al desafío a partir de una nueva forma de funcionamiento, no vertical; un funcionamiento en red entre Estados.

En esa línea, concluye, en el contexto de la crisis del Estado nación es necesario un nuevo modelo de organización social, teniendo en cuenta que la sociedad contemporánea se caracteriza por nuevas figuras de orden o de desorden, modelo aquél que supere la incapacidad constatada del derecho para producir normas a la altura de los desafíos de la globalización en la cuestión criminal y la cuestión penal, pensando en un sistema de globalización de los sistemas jurídicos que sea análogo al fenómeno ocurrido con el crimen. En definitiva, la adopción de una política en este sentido no podría pasar por lo que Ferrajoli denomina "la inflación del derecho penal" que ha llevado a la quiebra de la maquinaria judicial.

3. ¿Existe un sistema penal transnacional?

La catedrática Ana Isabel Cepeda (3), también denuncia la limitación del sistema judicial del Estado nación para combatir los delitos transnacionales, ya

que el derecho y la persecución penal están ligadas a la soberanía del Estado impedido de actuar fuera de sus fronteras por muy condenable que sea aun cuando se haya cometido justo detrás de la frontera y afecte a los ciudadanos nacionales.

Ante esta realidad, en el marco de la tradicional cooperación jurídica de la persecución penal, varios países han realizado acuerdos, tanto bilaterales como multilaterales, dentro del marco del derecho internacional público. Entre ellos, la Convención contra la delincuencia organizada transnacional de las Naciones Unidas y los convenios de Naciones Unidas en materia de lucha contra el terrorismo, corrupción, el tráfico de drogas y el convenio relativo a la profundización de la cooperación transfronteriza, en particular, en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal 2005.

Por su parte, en el ámbito de la Unión Europea expone la existencia de varios instrumentos, entre ellos, el más importante es la orden de detención europea Decisión Marco del Consejo del 13/6/2002, la que fue de avanzada porque prevé una larga lista de delitos, sin exigir la doble punibilidad de la conducta perseguida como se hacía hasta ese momento. Además, destaca la autora el art. 82 (TFUE), el cual conforme la Exposición de Motivos de la Ley 23/2014, conllevó un cambio radical en las relaciones entre los Estados miembros de la UE, al sustituir las antiguas comunicaciones entre autoridades centrales o gubernativas por la comunicación directa entre autoridades judiciales, suprimir el principio de doble incriminación en relación con un listado predeterminado de delitos y regular como excepcional el rechazo al reconocimiento y ejecución de una resolución, a partir de un listado tasado de motivos de denegación. Además, se ha logrado simplificar los procedimientos de transmisión de las resoluciones judiciales, mediante un formulario que deben completar las autoridades judiciales.

También, cabe citar como avanzada la propuesta de Reglamento estableciendo una Fiscalía Europea frente al fraude de intereses financieros de la UE, proyectada como una institución independiente que servirá de nexo entre los sistemas nacionales de los Estados de la Unión y los organismos de la UE que no pueden realizar investigaciones penales. Así las cosas, sostiene la autora que, analizando estos instrumentos podemos aproximarnos a una idea sobre el derecho penal transnacional, mediante un enfoque normativo de reglas creados específicamente para tratar asuntos criminales transnacionales, lo cual presupone un legislador tuvo como punto de referencia no sólo los Estados soberanos, sino las áreas judiciales comunes con un interés transnacional.

A su vez, se suma un enfoque empírico inductivo que abarca además las reglas de competencia y sobre la asistencia jurídica mutua en materia penal para la obtención de prueba transnacional y el uso de pruebas, en cuyo marco serán fundamental considerar los derechos y garantías del sospechoso o el acusado y las víctimas. No obstante, parece una obviedad percatarse de que en el ámbito internacional la amplia ratificación de diversos tratados sobre derechos humanos, hace que podamos hablar de ciertas reglas de procedimiento y garantías procesales que se aplican directamente en el ordenamiento jurídico de los Estados. Además, existe un consenso cada vez mayor en la ley internacional de derechos humanos.

A su vez, para facilitar el enjuiciamiento transnacional de estos y otros crímenes, los Estados han establecido instituciones, tales como ONUDD y Europol, han establecido mecanismos para la internacionalización de información e incluso se han concedido autoridad para llevar a cabo actos de investigación en su territorio a los agentes de otros estados.

Finalmente, si tuviéramos que delinear -siguiendo a Cepeda- los principios básicos que podrían formar un cuerpo completo de normas para los delitos transnacionales en el marco de las Naciones Unidas, en primer lugar, se invoca la regla de competencia universal, considerando los delitos transnacionales suponen siempre la concurrencia de jurisdicciones, aunque será menester aplicar el principio de subsidiariedad horizontal, propio del funcionamiento de la Corte Penal internacional, para limitarla a los casos en que habiendo iniciado un procedimiento el país en que se hubiera cometido el delito o de la nacionalidad del imputado, los tribunales y jueces podrán reservar su jurisdicción si el Estado que la ejerce no está dispuesto a llevar a cabo la investigación o realmente no puede hacerlo, porque no tiene la infraestructura técnica. Asimismo, desarrolla minuciosamente la autora los restantes principios básicos, que solo enumeraré por exceder el objetivo de este trabajo, entre los cuales se encuentran todos aquellos que emanan de los principios penales estatales tradicionales, tales como el principio de culpabilidad y el principio *ne bis in idem*, el principio de legalidad, así como también, de todas aquéllas garantías procesales que conforman las condiciones mínimas para conceder al acusado la posibilidad efectiva de acceder a un “juicio justo” bajo las reglas del debido proceso legal.

4. La Exposición de Motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal (4).

Ante todo, es importante destacar que esta Propuesta de Reglamento se redactó en el año 2018, es decir a más de quince años del Convenio sobre Ciberdelincuencia del Consejo de Europa de 2001, demostrando así que los mecanismos establecidos no resultan suficientes para los problemas que se suscitan en la actualidad. Así, se expone la problemática subyacente a la cooperación penal para la investigación de ciberdelitos más reciente, al afirmar que la utilización de las redes sociales, los servicios de correo electrónico y de mensajería y las aplicaciones para comunicarse, trabajar, crear lazos sociales y obtener información se ha convertido en algo habitual en la mayoría de las regiones del mundo.

Señala que estos servicios conectan entre sí a cientos de millones de usuarios y generan importantes beneficios para el bienestar social y económico de los usuarios en la Unión y fuera de ella. Sin embargo, también se pueden utilizar indebidamente como instrumentos para cometer o facilitar delitos graves, en particular atentados terroristas. Cuando esto sucede, dichos servicios y aplicaciones son a menudo el único lugar donde los investigadores pueden hallar pistas para determinar quién ha cometido un delito y obtener pruebas que puedan utilizarse ante los tribunales.

En ese marco, dado que internet no conoce fronteras, estos servicios pueden prestarse desde cualquier lugar del mundo y no exigen necesariamente una infraestructura física ni una presencia empresarial o personal en los Estados miembros en los que se ofrecen o en el mercado interior en su conjunto. Tampoco requieren una ubicación específica para el almacenamiento de los datos, que a menudo es elegida por el proveedor de servicios sobre la base de consideraciones legítimas como la seguridad de los datos, las economías de escala y la rapidez de acceso.

En consecuencia, en un número creciente de casos penales relativos a todo tipo de delitos, las autoridades de los Estados miembros necesitan acceder a datos que puedan servir como prueba y que están almacenados fuera de su país o por proveedores de servicios de otros Estados miembros o de países terceros. Para estas situaciones, en que las pruebas o el proveedor de servicios están ubicados en otro lugar, ya se desarrollaron hace varios decenios mecanismos de cooperación entre países.

A pesar de las frecuentes reformas, estos mecanismos de cooperación están sometidos a una presión creciente debido a la mayor necesidad de poder acceder rápidamente a pruebas electrónicas de forma transfronteriza. En respuesta, varios Estados miembros y países terceros han recurrido a la

ampliación de sus herramientas nacionales; la consiguiente fragmentación genera inseguridad jurídica y obligaciones contradictorias y plantea la cuestión de la protección de los derechos fundamentales y las garantías procesales de las personas afectadas por tales solicitudes.

En el ámbito de la UE, como expresa el documento citado, ya en el año 2016 el Consejo del Europa pidió acciones concretas basadas en un enfoque común de la para una asistencia jurídica mutua más eficaz a fin mejorar la cooperación entre las autoridades de los Estados miembros y los proveedores de servicios radicados en países no pertenecientes a la UE y para proponer soluciones al problema de la determinación y aplicación de la jurisdicción en el ciberespacio.

El Parlamento Europeo también puso de relieve los retos que el actualmente fragmentado marco jurídico puede suponer para los proveedores de servicios que desean dar cumplimiento a los requerimientos legales e hizo un llamamiento en favor de un marco jurídico europeo que incluya salvaguardias para los derechos y las libertades de los interesados.

En definitiva, el problema específico que se resalta se vincula al carácter volátil de las pruebas electrónicas y su dimensión internacional, frente a los desactualizados mecanismos de cooperación impropios de esta era digital. El desafío radica en ofrecer herramientas a las autoridades judiciales y policiales para abordar la forma en que los delincuentes se comunican en la actualidad, y para luchar contra las nuevas formas de delincuencia.

Se expresa en el instrumento del Consejo de Europa que tiene por objeto mejorar la seguridad jurídica para las autoridades, los proveedores de servicios y las personas afectadas, y mantener un nivel elevado por lo que respecta a las solicitudes de las autoridades competentes, asegurando así la protección de los derechos fundamentales, la transparencia y la responsabilidad. También acelera el proceso para obtener y asegurar pruebas electrónicas que estén almacenadas o que obren en poder de proveedores de servicios establecidos en otra jurisdicción.

5. El derecho informático y la cooperación penal internacional

Como señala Díaz Gómez (5), en materia de derecho informático como de cooperación internacional en general, la legislación europea se presenta como adalid indiscutible de las nuevas formas de colaboración entre Estados, existiendo multitud de acuerdos específicos en materia de cooperación en derecho penal, entre los cuales destaca el Convenio Europeo de Asistencia

Judicial en Materia Penal (2000) que “constituye la culminación de los esfuerzos para maximizar la asistencia judicial entre los juzgados de los países miembros”, al facilitar la ayuda judicial mutua entre las autoridades competentes de los Estados miembros (policía, aduanas y tribunales), con el fin de que la cooperación penal resulte más rápida y eficaz. Para este propósito se prevén soluciones concretas como son: intercambio de información, equipos de investigación conjuntos, transmisión de documentos, interceptación de comunicaciones, etc. Su incidencia en la persecución del ciberdelito queda, aún a falta de mayor explicación, bien acreditada.

Igualmente, deben recordarse otras expresiones más que notables de cooperación judicial en materia penal en el ámbito de la Unión Europea, como son la creación de la Red Judicial Europea y el Eurojust. La primera, se trata de una red de contactos judiciales entre los Estados miembros con el fin de facilitar la cooperación judicial, proporcionar información jurídica y práctica necesaria a las autoridades locales, participar y promover la organización de sesiones de formación en materia de cooperación, etc. Ello en el marco de la lucha contra formas de delincuencia grave (delincuencia organizada, corrupción, narcotráfico y terrorismo).

El Eurojust, por su parte, es un órgano que se encarga de realizar investigaciones y actuaciones relativas a la delincuencia grave que afecta al menos a dos Estados miembros, promoviendo la coordinación entre autoridades competentes de los distintos Estados miembros y facilitar la cooperación judicial entre ellos.

Conforme concluye el autor, si bien la regulación comentada no se refiere en particular a los delitos informáticos, la mayoría de sus previsiones pueden ser aplicadas a la comisión de éstos, acreditando así el fundamento de la exposición.

Explica que la cooperación, en abstracto, posee una estricta relación con la solidaridad intercultural, con la concurrencia recíproca de ideas y soluciones, con la ayuda mutua, así como con la apertura a otras formas de colaboración transversal que alcance nuevas disciplinas. Esta generalidad es precisamente su mayor ventaja, pero también un inconveniente. Ello por la complejidad y dificultad que supone articular procesos participativos que involucren a gran cantidad de Estados, cada uno de ellos con sus peculiaridades e intereses, así como concordar la gran cantidad de elementos en juego. Para ello será necesario salvar primero el importante escollo del inherente antagonismo diplomático de los países y forzar a los Estados a tomar decisiones conjuntas de los problemas que les afectan.

Dada la universalidad del delito informático y sus dificultades procesales, será muy importante conocer todos los datos acerca de los distintos elementos que configuran el ciberdelito en el tiempo y la forma adecuados. En este sentido la agilidad y rapidez en el intercambio de la información serán aspectos que beneficiarán inmensamente la persecución de los delitos informáticos. Igualmente, será muy importante para dotar de una mayor presteza a la investigación llevar a cabo una simplificación cualitativa de los medios de comunicación.

Propone el autor que la Red Judicial Europea descrita supra podría servir de modelo para la creación de una red de juristas de contacto entre diferentes países, en la línea seguida por el avanzado sistema I-24/7 de Interpol para intercambiar información sobre delincuencia informática entre sus países miembros. Pues, facilitar el intercambio de información a todos los niveles es quizás la más importante de las ventajas que puede proporcionar la cooperación internacional, dada su transversalidad, afectando tanto a la alta toma de decisiones como a la actividad administrativa y jurisdiccional común.

Destaca la importancia de la colaboración entre unidades policiales, encargadas de reprimir este tipo de delitos, de los distintos Estados. Dado nuevamente el carácter transfronterizo de los ciberdelitos, no se necesitan demasiadas explicaciones para percibir el modo en que la cooperación beneficia las actividades de las fuerzas y cuerpos de seguridad en la represión de dichos delitos.

Pudiendo distinguirse en este aspecto dos vías de cooperación penal, la que se realiza a través de los convenios internacionales, y una segunda que se sustancia mediante organizaciones internacionales ya consolidadas como Interpol. La primera vía, caracterizada por los convenios bilaterales entre Estados, es de acción limitada por su inevitable confinamiento a la negociación particular entre muy pocos países, hasta la aparición, claro está, del Convenio sobre Cibercriminalidad.

En cuanto a la segunda, destaca las bondades de la organización internacional Interpol, cuyo ámbito de acción es prácticamente universal, abarcando hasta 188 miembros, la cual realizará una importante labor en la lucha contra la cibercriminalidad dada su extensión mundial; más allá del mero intercambio de información antes aludido (sistema I-24/7), favorece enormemente la cooperación entre las fuerzas de seguridad de todo.

Asimismo, explica que, en el ámbito europeo, la cooperación policial alcanza cotas más altas con la presencia del llamado Protocolo Schengen y Europol. El primero es un acuerdo para la supresión real de las fronteras y los

controles interiores entre los países signatarios e incorpora medidas de colaboración policial y judicial y armonización de legislaciones en múltiples materias para la persecución de la delincuencia. En cuanto a Europol, dependiente de la Oficina Europea de policía, tiene por misión la coordinación de las policías europeas, proporcionar apoyo, facilitar intercambios de información, etc., en la lucha contra la delincuencia.

En relación con los ciberdelitos, se prevén específicamente tareas de recogida y análisis de información para contribuir a identificar las actividades delictivas facilitadas por internet o cometidas a través de internet. Especialmente conviene mencionar la importancia que ha supuesto la utilización de bases de datos para la persecución de determinados delitos a través de Internet, como son el fichero "Twins" y el archivo "Terminal".

Siguiendo al autor, entre los requisitos que debe investir una adecuada cooperación internacional en materia ciberdelictual pueden citarse: a) El "pensamiento universal" que obliga a abarcar el mayor número de Estados y para ello cosechar el mayor número de avenencias. b) Los "límites formales y materiales a la cooperación", porque la armonización conlleva el respeto a los Tratados Internacionales vigentes, que no tiene siquiera carácter de recomendación, sino de obligación, entre ellos, los principios de intervención mínima, principio de *non bis in ídem*, principio de culpabilidad, principio de humanidad de las penas, principio de legalidad, etc. Y c) La máxima "Pensar globalmente, actuar localmente y pensamiento realista", que opera como cláusula de cierre para señalar que nunca se debe perder de vista la realidad de los hechos; todas las acciones tomadas en el plano legislativo deben poder llevarse plenamente al escenario existente, pero además deben realizarse pensando siempre en las distintas comunidades a las que finalmente va a ser aplicada.

En este sentido, destaca que, para construir una adecuada cooperación internacional de cara a la persecución de los delitos informáticos, no basta con el recurso a los tratados Internacionales sino que la simplificación y la agilización de la cooperación no tiene lugar únicamente mediante la creación de instrumentos nuevos, sino en los fundamentos mismos de los órganos de la administración de justicia que han de colaborar mediante una infraestructura mejorada para el tratamiento de casos transfronterizos.

III. EL MÉTODO DE LA PRESENTE INVESTIGACION

Este trabajo de investigación, reitero, no tuvo por objeto profundizar en el desarrollo de ningún medio de prueba en particular ni en relación proceso

de obtención de prueba transnacional específico alguno, sino que se pone el enfoque en la evolución de la política criminal internacional en materia de cooperación penal para la investigación de ciberdelitos, a partir de los instrumentos legales que los Estados han ido suscribiendo en los últimos veinte años, culminando con el Segundo Protocolo Adicional al Convenio. Ello, a los fines de comprender cuáles fueron los aciertos y falencias del pasado, como así también, cuáles son los nuevos direccionamientos del presente para pronosticar, a partir de allí y de manera fundada, pronosticar cuáles son los mecanismo e instituciones de la cooperación del futuro, en el contexto

El trabajo presenta un enfoque *mixto cualitativo - cuantitativo* de tipo histórico-hermenéutico, desde el cual se analizan los instrumentos jurídicos desarrollados en el marco institucional de las relaciones internacionales; en particular los destinados a enfrentar el cibercrimen, como así también, las instituciones multilaterales en funcionamiento actualmente, las cuales tienen un componente de normativo, en sus actos fundacionales, pero también tienen un componente pragmático, en el ejercicio de su funcionamiento efectivo. Como veremos, estas prácticas se analizaron a través de las publicaciones actuales de las páginas oficiales en Internet que, entiendo, brindan información exhaustiva sobre los aspectos de su rol institucional efectivo y de sus experiencias prácticas.

Entonces, en parte el enfoque es cuantitativo en la medida que hubo una tarea de relevamiento objetivo de datos, esto es, de los instrumentos legales vigentes para la cooperación los cuales, en definitiva, son fenómenos externos. Además, el enfoque cuantitativo se manifestó en la pretensión de generalización de los resultados encontrados, tal como se verá al momento de efectuar las conclusiones, con el fin último explicar cómo será el futuro próximo de la cooperación penal. En ese aspecto, se ha utilizado la lógica del razonamiento deductivo.

Por otra parte, esta investigación tuvo un *componente cualitativo*, ya que necesariamente se introdujo un nivel interpretativo, no de tipo judicial, sino más bien a nivel de la política criminal del Estado parte, a partir del compromiso que asume al adherir al Segundo Protocolo Adicional, desentrañando cuáles son las autoridades nacionales que tienen atinencia y responsabilidad en la debida receptividad del Instrumento en el orden interno, y cuáles son parámetros y las decisiones que deben adoptar para la implementación de mecanismo efectivos que mejoren la cooperación en las investigaciones penales. Para ello, se han tomado elementos del institucionalismo propio de la Ciencia Política y del análisis del Derecho Internacional y el Derecho Penal.

En este punto, decimos que el enfoque fue cualitativo, ya que después de la recolección y el análisis de los datos, la acción indagatoria se movió entre los hechos y su interpretación en un proceso más bien circular. Es decir, hubo una inmersión inicial en el campo de estudio a fin de sensibilizarme con el contexto del estudio, identificando las fuentes que aportaron los datos, para luego compenetrarme con la situación de investigación y verificar la factibilidad del estudio. En ese sentido, la muestra, la recolección y el análisis fueron fases que se realizaron prácticamente de manera simultánea.

La actividad indagatoria se dividió, entonces, en dos etapas. En una primera etapa analicé los instrumentos de cooperación penal para la investigación de delitos transnacionales entre los años 1988 y 2001, especialmente, el Convenio sobre Ciberdelincuencia del Consejo de Europa (Budapest, 2001), las herramientas de cooperación allí contenidas. Paralelamente, se analizaron los criterios política criminal estatal que en ese momento el Estado nacional efectuó, concluyéndose que -a ese nivel- predominaron intereses nacionalistas restrictivos basados en anquilosadas concepciones de la soberanía territorial clásica, lo que impidió poner en funcionamiento de manera adecuada de los mecanismos diseñados en el Convenio.

En una segunda etapa, que se ubica entre 2013 y 2022, se analizaron las nuevas herramientas contenidas en el Segundo Protocolo Adicional, además, de otros instrumentos legales que fueron sus antecedentes inmediatos, como el Proyecto de Reglamento del Parlamento y el Consejo de Europa para las órdenes de conservación y entrega de prueba electrónica. Paralelamente, se analizaron los criterios de política criminal imperantes a nivel del Consejo de Europa, a partir del surgimiento de instituciones concretas que implementan procedimientos de cooperación efectivos, como es el European Cybercrime Center (EC3), y, en el mismo sentido, se analizaron los nuevos programas que ha incorporado Interpol para cooperar con los Estados en las investigaciones penales. Llegando así a la conclusión de la tendencia hacia la cooperación lo más amplia posible que presupone la flexibilización de los controles nacionalistas para dar lugar a una fragmentación necesaria de la concepción estricta de soberanía territorial. A partir de allí es que se pronostica que el Estado nacional mejorará su papel -en relación con la etapa anterior-, que actuará a la altura de las circunstancias a través de cada área asumiendo su responsabilidad internacional implementar de manera efectiva los mecanismos.

Es decir, se ha procedido dato por dato hasta llegar a una perspectiva más general, por lo que el objetivo central del trabajo se ha generado durante

el proceso. En este punto, el propósito del trabajo fue “reconstruir” la realidad, tal como los actores del sistema social competente en esos temas (Consejo de Europa) entienden que deben receptarse los instrumentos nuevos que ellos mismo van dictando. Entonces se trató de desentrañar la perspectiva interpretativa de los redactores y legisladores internacionales de esos documentos para que sean adecuadamente receptados por los destinatarios, que no son otros que los Estados.

Vale la pena aclarar que, tal como señala Hernández Sampieri (6), las aproximaciones cuantitativa y cualitativa no deben verse como enfoques rivales sino como diferentes aproximaciones al estudio de un fenómeno, que en este trabajo se utilizaron de manera complementaria, proporcionando el e*nfoque cuantitativo* rigurosidad, objetividad y certeza en el conocimiento obtenido, mientras que el *enfoque cualitativo* permitió una aproximación a la experiencia subjetiva de las instituciones analizadas desentrañando sus interpretaciones y vivencias.

Para concluir este acápite, resta mencionar que este trabajo presenta un “enfoque explicativo”, posibilitado por el evolucionado estado del conocimiento actual del tema de investigación que revela la revisión de la bibliografía y la perspectiva de este estudio, ya que existen numerosos estudios científicos con apoyo empírico suficiente sobre problemáticas muy similares. Podría decirse, como vimos, que la literatura expuesta revela la existencia de teorías que se aplican a nuestro problema de investigación, aunque se enfocan en las falencias del sistema de cooperación internacional penal para la investigación de delitos transnacionales distintos de los delitos informáticos.

IV. ANÁLISIS DE RESULTADOS: LOS INSTRUMENTOS JURÍDICOS Y LAS INSTITUCIONES INTERNACIONALES DE COOPERACION PENAL EN LA INVESTIGACIÓN DE CIBERDELITOS

Del análisis de los convenios multilaterales de cooperación penal vigentes en la actualidad, surge que durante la última década del siglo pasado y los primeros años del corriente, los Estados, preocupados por la expansión y el daño ocasionado a nivel global por los nuevos fenómenos delictivos organizados transnacionales, comienzan a redactar y suscribir los primeros instrumentos multilaterales para comprometer a las Partes a colaborar de una manera más amplia y efectiva, despojados de antiguas concepciones restrictivas basadas en los principios de soberanía territorial y orden público interno.

No obstante, a pesar de estos avances, en el sentido de haberse conseguido la homogeneización de la legislación sustantiva a los fines de la tipificación penal nacional de los delitos, en lo relativo a las investigaciones transnacionales, y en particular, para la obtención de pruebas trasnacionales, aquellos instrumentos se mostraron ser insuficientes, dando lugar así a una segunda etapa, que se inicia alrededor del año 2013, con el surgimiento de nuevos instrumentos legales, mecanismos de cooperación y la instauración de instituciones a ese fin. Así, pueden visualizarse dos etapas bien marcadas, a partir de los instrumentos legislativos que se exponen a continuación:

1. Primera Etapa, entre 1992 y 2001:

. 1.1. En lo relativo a la Delincuencia Organizada Transnacional

En este acápite realizaré un breve repaso de la Convención contra la delincuencia organizada trasnacional y sus Protocolos, por su semejanza con la problemática planteada en este trabajo, pues el instrumento tuvo por finalidad promover la cooperación para prevenir y combatir más eficazmente la delincuencia organizada transnacional, dando lugar a la implementación de herramientas de avanzada, en ese momento, similares a las del Convenio sobre cibercriminalidad.

El objeto de la Convención fue la lucha contra “grupos delictivos organizado”, estructurados por tres o más personas con cierta duración y concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la Convención, con miras a obtener un beneficio económico u otro beneficio de orden material. Entre los delitos, se contempla el blanqueo de capitales de origen delictivo, y el delito de corrupción y contiene, además, el Protocolo para Prevenir, Reprimir y Sancionar la Trata de Personas, especialmente Mujeres y Niños. Serán considerados de carácter transnacional si se cometen en más de un Estado, o si se cometen dentro de un solo Estado, pero una parte sustancial de su preparación, planificación, dirección o control se realiza en otro Estado. También en caso de que se cometan en un Estado, pero tiene efectos sustanciales en otro Estado.

En lo que aquí interesa, respecto de la extradición y la asistencia judicial, establece una amplia colaboración internacional respecto a las actividades delictivas transnacionales donde el componente económico resulta primordial, esto es la asociación delictiva con miras a obtener beneficios por la comisión de delitos graves.

La regla de competencia recepta el principio de jurisdicción universal, característico de los convenios contra delitos transnacionales, tal como lo hace también el Convenio sobre ciberdelincuencia de 2001, ya que un Estado Parte podrá establecer su jurisdicción cuando se cometa contra uno de sus nacionales; cuando se trate de delitos fuera de su territorio con miras a la comisión de un delito grave dentro de su territorio; o cuando se trate de uno de los delitos vinculados al blanqueo de capitales de origen delictivo y se cometa fuera del territorio con miras a la comisión, dentro de su territorio. También, cuando el presunto delincuente se encuentre en su territorio y el Estado Parte no lo extradite por el solo hecho de ser uno de sus nacionales.

En materia de cooperación penal internacional, surge el principio de la máxima cooperación posible entre los Estados respecto de investigaciones, procesos y actuaciones judiciales relacionadas con los delitos comprendidos en la presente Convención. En esa línea, la asistencia judicial recíproca podrá solicitarse a fines de recibir testimonios o tomar declaración a personas, presentar documentos judiciales, efectuar inspecciones e incautaciones y embargos preventivos, examinar objetos y lugares; facilitar información elementos de prueba y evaluaciones de peritos, entregar copias de documentos y expedientes pertinentes, incluida documentación pública, bancaria y financiera o social y mercantil de sociedades comerciales, entre otras.

Además, las autoridades competentes de un Estado parte podrán, sin que se les solicite previamente, transmitir información relativa a cuestiones penales a una autoridad competente de otro Estado parte, si creen que esa información podrá ayudar a la autoridad a emprender o concluir con éxito indagaciones y procesaos penales. En esa dirección, los Estados parte no invocarán el secreto bancario para denegar la asistencia judicial recíproca ni podrán negarse a prestar cooperación salvo cuando el Estado requerido considere que el cumplimiento de lo solicitado podría menoscabar su soberanía, su seguridad, su orden público u otros intereses fundamentales. Tampoco podrá denegarse porque se considere que el delito también entraña asuntos fiscales.

Lo importante es que la denegatoria debe ser debidamente justificada y la solicitud deberá cumplirse lo más rápido posible y tendrá en cuenta los plazos que sugiera el Estado requirente, debiendo antes de denegar una solicitud el Estado requerido formular consultas al Estado requirente sobre si es posible cumplirla bajo ciertas condiciones que imponga.

A su vez, cada Estado parte designará a una autoridad central encargada de recibir solicitudes de asistencia judicial recíproca, que velarán por el rápido y adecuado cumplimiento o transmisión de las solicitudes recibidas y, en circunstancias urgentes, cuando los Estado parte convengan en ello, por conducto de la Organización Internacional de Policía Criminal (INTERPOL) se procurará imprimirle la más rápida diligencia. Otro aspecto de avanzada de la Convención son las medidas tendientes a que los Estados adopten técnicas de avanzada en materia de investigación, entre ellas, la entrega vigilada, la vigilancia electrónica y las operaciones encubiertas con el objeto de combatir la delincuencia organizada. El Convenio sobre Ciberdelincuencia del Consejo de Europa.

1.2. El Convenio sobre Ciberdelincuencia del Consejo de Europa

El Convenio (ETS N° 185) fue adoptado en la ciudad de Budapest, República de Hungría, el 23 de noviembre de 2001, al que adhirió la República Argentina mediante Ley N° 27.411 varios años después. Para comenzar, vale destacar la importancia que ya en ese entonces se le asignó a la necesidad de establecer un sistema de cooperación penal amplio entre los Estados Parte para las investigaciones penales a los fines de la obtención de prueba transnacional, ya que se dedicaron las dos terceras partes del total de las normas a la regulación de dicha cuestión.

Los preparativos comenzaron en el mes de noviembre de 1996, por medio de la decisión CDPC/103/2111196, el Comité europeo para los problemas criminales, estableció un comité de expertos encargado de los delitos informáticos, basado en la razón fundamental de los “rápidos desarrollos en el campo de la tecnología de la información … La integración de los sistemas de las telecomunicaciones y de información, que posibilitan el almacenamiento y la transmisión de todo tipo de comunicaciones, sin tener en cuenta la distancia.”

El Convenio fue el primero en el mundo en abordar la problemática y el Comité europeo ya en ese tiempo explicó que esos desarrollos se vieron “potenciados por la aparición de las redes y las superautopistas de la información, incluida Internet, a través de las cuales todas las personas pueden tener acceso a cualquier servicio de información electrónica, creando una especie de espacio común, denominado ciberespacio, que es utilizado con fines legítimos, pero que también puede ser objeto de un uso impropio” (7).

Se consagró el principio general relativos a la “colaboración”, según el cual las Partes acordarán llevar a cabo una *colaboración mutua lo más amplia*

posible al objeto de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o al de recoger pruebas electrónicas de una infracción penal. A ese fin, establece que las Partes designarán una o varias "*autoridades centrales*" encargadas de tramitar las "demandas de colaboración", de ejecutarlas o de transferirlas a las autoridades competentes para que éstas ejecuten. Asimismo, prevé que las autoridades centrales se comunicarán directamente las unas con las otras y que las Partes comunicarán al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas, debiendo el crear y actualizar un registro.

A su vez, la asistencia solo podrá ser rechazada por el Estado requerido si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o; si el Estado requerido estima que, de acceder a la colaboración, se pondría en peligro su soberanía, seguridad, orden público u otro interés esencial.

En caso de urgencia, las autoridades judiciales del Estado requirente podrán dirigir directamente a las autoridades homólogas del Estado requerido las demandas de asistencia y las comunicaciones. En tales casos, se remitirá simultáneamente una copia a las autoridades del Estado requerido con el visado de la autoridad central del Estado requirente y podrán ser tramitadas a través de la Organización Internacional de Policía Criminal (INTERPOL).

En cuanto al acceso a datos informáticos almacenados, cualquier Estado podrá solicitar a otro el registro o acceso de otro modo, el decomiso u obtención por otro medio, o la comunicación de datos almacenados en un sistema informático que se encuentre en su territorio. Se establece que la demanda deberá ser satisfecha lo más rápidamente posible cuando existan motivos para sospechar que los datos solicitados son particularmente vulnerables por existir riesgo de pérdida o modificación.

En lo referido a la Asistencia para la recolección en tiempo real de datos de tráfico, las Partes podrán acordar colaborar en la recolección, en tiempo real, de datos de tráfico, asociados a concretas comunicaciones llevadas a cabo en sus territorios, a través un sistema informático. A ese fin, se tendrá en cuenta que aquellas infracciones penales para las cuales la recolección en tiempo real de datos de tráfico se solicita, se encuentre prevista en su derecho interno en situaciones análogas.

Instituye el sistema de la Red 24/7, según el cual las Partes designarán un punto de contacto localizable las 24 horas del día, y los siete días de la semana,

con el fin de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recolección de pruebas electrónicas de una infracción penal. Esta asistencia comprenderá facilitar la aplicación directa de las siguientes medidas: aportación de consejos técnicos; conservación de datos según lo dispuesto en los artículos 29 y 30; y recolección de pruebas, aportación de información de carácter jurídico y localización de sospechosos.

Para concluir esta exposición, cabe reiterar, tal como lo hiciera al plantear el problema de este trabajo, que el Convenio sobre Cibercriminalidad del Consejo de Europa de 2001 sí se ocupó, especialmente, de establecer mecanismos de cooperación penal internacional que en la teoría se percibieron de avanzada en ese momento, sobre todo, con la utilización de la figura de la Autoridad Central que cada Estado parte debía designar ante el Secretario General, con la función específica de tramitar las solicitudes de cooperación en los términos del acuerdo de manera directa y ágil. Igualmente, se consideró un avance el establecimiento del Sistema de la Red 24/7 para emergencias, a cuyo fin cada Estado parte debía designar un Punto de Contacto disponible en todo momento para la atención de las solicitudes.

Ahora bien, no obstante ello, con el transcurrir de los años hasta la fecha, la insuficiencia de este sistema de cooperación para la investigación penal y la obtención de prueba transnacional diseñado en el Convenio en la práctico, se hizo evidente a partir de la cantidad y diversidad de reglamentaciones, acuerdos e instituciones que fueron emergiendo en el ámbito mismo del Consejo de Europa, con el objeto claro de superar las deficiencias y las demoras que presenta la investigación de ciberdelitos cuando hasta llegar a la redacción del Segundo Protocolo Adicional al Convenio sobre cooperación reforzada.

Al respecto, la pregunta que se impone será porqué habrían fracasado -por decirlo de alguna manera- aquellas medidas del Convenio de 2001 si en sí mismas se presentan como mecanismos idóneos para acelerar las solicitudes y entrega de información, datos y prueba, sobre todo comparado con los antiguos mecanismos de cooperación. Ante la pregunta, entiendo que la única explicación plausible debe encontrarse, entonces, fuera de la legislación en sí misma, en dos aspectos de la realidad. Por un lado, en la evolución de los fenómenos informáticos y tecnológicos y en consecuencia de la complejidad de los delitos informáticos transnacionales que volvieron insuficientes esos procedimientos. Pero, por otro lado, existe un componente de responsabilidad política que es atribuible a la inacción de las autoridades nacionales con atinencia en la implementación efectiva de los mecanismos, que no asumieron

la responsabilidad internacional que les competía con la fuerza y el compromiso político al momento de contribuir para hacer efectivos los mecanismos. Es decir, sin la voluntad política del Estado parte no hay posibilidad de que funcione ningún mecanismo internacional de cooperación por bien orquestado que se encuentre, porque toda norma internacional presenta un fuerte componente de voluntarismo del Estado nacional. En este punto, dable es suponer que, más que por razones de desidia, habría dominado en la decisión gubernamental nacional la concepción restrictiva de la soberanía nacional en protección de supuestos intereses de orden público interno que ya no requieren, como veremos, esa tutela.

2. Segunda Etapa, entre el 2013 y 2022.

Los instrumentos que se analizan a continuación revelan que, el ámbito de la cooperación penal para la investigación de delitos informáticos, la normativa existente, y las instituciones creadas a través de ella –Autoridad Central y Punto de Contacto de la Red 24/7-, resultaban inidóneas para la obtención de pruebas transnacionales en el extranjero o la identificación de víctimas y sospechosos con el nivel de eficacia requerido.

2.1. El surgimiento de European Cybercrime Center (EC3)

A mediados del año 2013, la UE creó un centro asociado a Europol llamado European Cybercrime Center (EC3) en el marco de la Estrategia de Seguridad Interior de la Unión europea, hacia un modelo europeo de seguridad vinculada al Programa de Estocolmo desde el año 2010 y al cumplimiento a su vez del Convenio de Cibercrimen del Consejo de Europa del 2001 (8).

El EC3 a través de Europol es un buen ejemplo para crear una especie de servicio de inteligencia coordinado en la lucha contra el cibercrimen en la UE, ya que contribuye a la ciberseguridad y ciberdefensa desde una concepción futurista, pensada en investigar delitos cibernéticos de nueva generación y que, a su vez, funcione como una especie de plataforma con ramificaciones conectada con agencias de seguridad nacionales y operadores jurídicos o policiales que se dediquen a lo misma en cada uno de los países de los estados miembros.

Además de esto, Europol a través del EC3 realiza una acción coordinada en materia de diligencias de investigación a través de la potenciación de equipos conjuntos de investigación entre diversos estados. Es decir, operadores policiales de distintos países que colaboran en operaciones cibernéticas con

componente transfronterizo para investigar ciberdelitos de alta tecnología, pornografía infantil, fraude electrónico, etc.

En todo caso, el inconveniente que plantea esta labor se vincula a la desarmonía legislativa a nivel de diligencias de investigación tecnológica en la UE, como el uso de la interceptación de las comunicaciones o de otras más avanzadas como la inclusión de virus espías o la infiltración de agentes encubiertos en Internet, por lo cual, se tiene que actuar bajo el principio de garantismo preventivo absoluto con el fin de no poner en peligro el resultado de la investigación.

Una de las operaciones más conocidas coordinadas por el EC3 a través de equipos conjuntos de investigación fue el caso de Sweetie, aplicando inteligencia artificial como diligencia de investigación. En el caso, la organización holandesa a favor de los derechos humanos de los niños Terre des hommes y Europol, a través de una niña creada por inteligencia artificial, se logró atraer a más de 20 mil pedófilos en todo el mundo entre 2013 y 2014, resultado de una estrategia coordinada gracias al EC3. Fue un caso de agentes encubiertos en Internet con el objetivo de recabar pruebas electrónicas válidas para probar un determinado ciberdelito con pretensión de validez de diversos Estados miembros.

Así, partimos de que cada país tiene su propia regulación en el uso de las diligencias de investigación, sus principios rectores para su autorización y una modalidad de ejecución particular, así como características para la concesión de resoluciones judiciales para su concesión y un largo etcétera que debe ser validado para que la prueba surta efecto y se puedan respetar los principios suficientes que aseguren una obtención válida.

Es por ello interesante explorar la medida de los Equipos Conjuntos de Investigación (ECI), en el que los Estados involucrados a través de sus agencias policiales autorizadas realizan un acuerdo previo y un acto de constitución del alcance de las medidas de investigación a adoptar. El EC3 realiza una importante labor de inteligencia e información criminal y ayuda igualmente a través de un análisis operacional y de coordinación personal e instrumental entre los estados. En definitiva, facilita la conexión ente las agencias encargadas de cumplir la ley, la academia, el sector privado y otros grupos de interés que se ocupan de la seguridad de la Red, al tiempo que ofrece y apoya programa *de training* para construir capacidades cibernéticas y poner al servicio de los mismos asistencia técnica y digital forense destinadas a apoyar investigaciones.

Por último, se destaca el valor de lo J-CAT (Join Cybercrime Action Task Force o Grupo de Trabajo conjunto de Acción contra el Cibercrimen) que surgen como complemento de los ECI con el fin de ayudar en investigaciones de gran complejidad, mediante un acuerdo de colaboración operacional de las agencias policiales con el EC3 de Europol, compartiendo de datos o mediante el desarrollo de planes conjuntos de actuación, en tanto cada equipo de trabajo será dirigido por el país que ha llevado el caso al EC3 y se atenderá al marco legal de dicho Estado para dirigir las posibles pesquisas, con el fin de dotarlas de mayor garantismo posible.

Los J-CAT nacen además con un afán de estabilidad, y se afirma que hasta el momento los resultados son fructíferos ante ciberdelitos de componente transfronterizo. Son unidades de apoyo que velan por la colaboración entre países, teniendo en cuenta los límites marcados por el principio de exclusividad de la jurisdicción de cada país, pero que sirve para identificar a través de una labor colaborativa, los instrumentos técnicos, personales e instrumentales que hacen falta para abordar un delito informático que traspasa la jurisdicción de un único estado.

Un enfoque clave de este grupo de trabajo es el traspaso de información a los fines de investigación, para lo cual Convención del Cibercrimen da cobertura legal mediante lo indicado en su art. 26 al referirse a la “información espontánea”. El precepto indica que “dentro de los límites de su derecho interno, y sin petición previa, una parte podrá comunicar a otra Parte información obtenida en el marco de sus propias investigaciones cuando considere que la revelación de dicha información podría ayudar a la Parte receptora a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en el presente Convenio o podría dar lugar a una petición de colaboración”.

2.2. Los Equipos Conjuntos de Investigación (ECI).

Conforme surge de la Guía de Cooperación Penal Internacional del Ministerio Público Fiscal de la Nación (9), los Equipos Conjuntos de Investigación son instrumentos de cooperación que permiten compartir la información y documentación en forma directa con los integrantes sin necesidad de otras solicitudes oficiales de asistencia, configurando un marco de cooperación estable que posibilita evitar la multiplicidad de pedidos de asistencia jurídica y permite la ejecución de medidas de prueba o actos procesales en todas las jurisdicciones intervinientes, lo que facilita la investigación.

Lo interesante de esta modalidad radica en que fue articulada para actuar en situaciones de urgencia en la obtención o transmisión de determinada información útil para las investigaciones, para superar la lentitud de los mecanismos formales de asistencia jurídica internacional, propiciando la comunicación directa entre autoridades judiciales. Se considera que para ello existen dos instrumentos útiles, la cooperación interinstitucional y la remisión espontánea de información.

Claro está que los funcionarios de cualquiera de las Partes que integren esos equipos actuarán con la venia de las autoridades competentes de la Parte en cuyo territorio se ha de llevar a cabo la operación y en todos esos casos, la Parte de que se trate velará por que se respete plenamente la soberanía de la Parte en cuyo territorio se ha de realizar la operación.

Si analizamos el marco jurídico multilateral de los ECI, puede verse que esta modalidad viene siendo contemplada desde hace casi tres décadas, en la Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional adoptada en Palermo el 15 de octubre de 2000, aprobada por ley 25.632, en la Convención de Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas (1988) promulgada por la Ley 24.072; y en la Convención de las Naciones Unidas contra la Corrupción, adoptada en Nueva York (2003), promulgada por la Ley 26.097, entre otras.

En el marco del Mercosur y países asociados y en el ámbito iberoamericano, el Estado argentino viene formando parte de una serie de instrumentos que le permitirían integrar equipos conjuntos de investigación desde el año 2010.

Entre ellos, el Acuerdo Marco de Cooperación entre los Estados Parte del Mercosur y Estados Asociados para la Creación de Equipos Conjuntos de Investigación, celebrado en San Juan, República Argentina, el 2 de agosto de 2010, aprobado mediante Ley N° 26.952 (10). Este Acuerdo Marco celebrado Brasil, Paraguay, Uruguay (Mercosur), y Bolivia y el Ecuador (Estados asociados), expone la preocupación por delitos como el tráfico de estupefacientes, la corrupción, el lavado de activos, la trata de personas, el tráfico de migrantes, el tráfico de armas y todos aquellos que integran la llamada delincuencia organizada transnacional, así como los actos de terrorismo, o delitos cuyas características hagan necesaria la actuación y combate coordinados de más de una Parte.

Por su parte, los Ministerios Públicos de Iberoamérica en el marco de la Asociación Iberoamericana de Ministerios Públicos (AIAMP) (11), han suscripto

el Convenio de Cooperación Interinstitucional entre los Ministerios Públicos y Fiscales Miembros de la Asociación Iberoamericana Ministerios Públicos, el 6 de septiembre de 2018, integrado por Argentina y otros veintitrés países. La Asociación cuenta con siete Redes Permanentes de Fiscales Especializados en distintos delitos: Red contra la Trata de Personas y Tráfico Ilícito de Migrantes; Red de Ciberdelincuencia; Red de Fiscales Antidroga; Red contra la Corrupción; Red de Cooperación Penal Internacional; Red Protección Ambiental; Red Especializada en Temas de Género.

A su vez, en materia de cibercrimen, CiberRed (12) es la red de Ministerios Públicos iberoamericanos especializados en ciberdelito creada por la XXIV Asamblea General de la AIAMP celebrada en Lisboa en octubre de 2016. Se trata de una red de procuradores fiscales especializados en la investigación y persecución penal de los ciberdelitos, con puntos de contacto en los diversos países integrantes. Los objetivos de la red son los de promover y mejorar la información disponible; potenciar el intercambio de conocimientos y experiencias; crear y difundir buenas prácticas y especialmente optimizar y agilizar la cooperación institucional y las solicitudes de cooperación penal internacional.

En el Plan de Actividades de CiberRed para el 2021, se explicitó que, a pesar de que muchos de los sistemas jurídicos del espacio iberoamericano tienen ya marcos normativos específicos de derecho penal sustantivo en el ámbito de la ciberdelincuencia, la conclusión es más pesimista en lo que se refiere a las normas relativas a la obtención de pruebas digitales, existentes solamente en un pequeño número de países iberoamericanos. A fin de afrontar estas dificultades, se dio continuidad al plan en una segunda reunión en Santiago de Chile el 25 de junio de 2019, donde se discutieron los concretos problemas surgidos en las investigaciones y la necesidad de capacitación y especialización del Ministerio Público en las áreas del ciberdelito y obtención de la prueba digital.

A su vez, en el mes de febrero de 2017, los Ministerios Públicos y Fiscalías Generales de once países firmaron la Declaración de Brasilia sobre Cooperación Jurídica Internacional contra la Corrupción.

Finalmente, no puede soslayarse el ámbito de la Unión Europea donde más se han trabajado y desarrollado los ECIs para optimizar la coordinación de las autoridades judiciales, fiscales y policiales competentes. Ya en Consejo Europeo de Tampere, el 19 de octubre de 1999, luego recogido en el artículo 13 del Convenio para la asistencia judicial en materia penal del 29 de mayo del

2000. Sobre esta base, el Consejo de la Unión Europea tomó la Decisión Marco de 13 de junio de 2002, respecto a la creación de equipos conjuntos de investigación, con el fin de propiciar que los distintos Estados miembros adoptaran sus respectivas leyes nacionales que permitieran su funcionamiento anticipado.

De suma importancia es el "mecanismo de cooperación internacional mediante el cual las autoridades competentes de un Estado remiten información a las autoridades competentes de otro Estado, sin que la misma haya sido solicitada previamente, cuando en el marco de una investigación tome conocimiento sobre hechos que podrían tener relevancia penal en el otro Estado, a los fines que se inicie una investigación o, en su caso, esa información sea aportada a una investigación en curso".

Al respecto, el Acuerdo de Cooperación Interinstitucional entre los Ministerios Públicos y Fiscales miembros de la AIAMP en la cláusula sexta prevé que "Los Ministerios Públicos o Fiscalías promoverán el intercambio de información cuando tomen conocimiento sobre hechos que pueden ser investigados en otro país. Dicha información será enviada sin perjuicio de las investigaciones que se lleven adelante en el país que remite la información, y sin afectar la reserva que deben guardar las mismas".

2.3. La propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal - 2018/0108 (COD).

He seleccionado este instrumento porque resulta elocuente al momento de exponer los problemas que subsistían a ese año de su redacción (2018), es decir a más de 15 años del Convenio sobre Ciberdelincuencia de 2001, en los mecanismos para obtener y conservar pruebas para investigaciones penales en la Unión Europea. Aunque, el documento emana del parlamento europeo, claramente, evidencia una problemática que se comparten la totalidad de los Estados que integran el Convenio de 2001, y aun los que no lo integran.

Este Proyecto fue impulsado como consecuencia de los atentados terroristas de Bruselas y las conclusiones del Consejo del 9 de junio de 2016, donde se subrayó la importancia creciente de las pruebas electrónicas en los procesos penales, y la necesidad de proteger el ciberespacio de abusos y las actividades delictivas, dotando a las autoridades policiales y judiciales de herramientas eficaces para investigar y enjuiciar los actos delictivos relacionados con el ciberespacio. Se afirma que los procesos actuales a veces

no logran adaptarse a la velocidad de los ciberataques, lo que crea una necesidad concreta de una cooperación transfronteriza ágil.

Se explica que atento que los servicios basados en la red pueden prestarse desde cualquier lugar y no requieren infraestructura física, instalaciones o personal en el país en cuestión, las pruebas pertinentes a menudo se almacenan fuera del Estado investigador o por un proveedor de servicios establecido fuera de dicho Estado. Entonces, con frecuencia no existirá ninguna otra conexión entre el caso investigado en el Estado en cuestión y el Estado del lugar de almacenamiento o de establecimiento del proveedor de servicio.

Debido a ello, las solicitudes de cooperación se remiten frecuentemente a Estados que acogen a un gran número de proveedores de servicios sin relación con el asunto en cuestión. Además, el número de solicitudes se han multiplicado debido al mayor uso de servicios de red, que por su naturaleza no tiene fronteras. En consecuencia, la obtención de pruebas electrónicas utilizando canales de cooperación judicial a menudo lleva mucho tiempo, más del tiempo que en podrían estar disponibles los indicios.

Por ese motivo, se declara la necesidad de establecer un marco jurídico europeo relativo a las pruebas electrónicas que obligue a los proveedores de servicios a responder directamente a las autoridades sin la intervención de un órgano judicial del Estado miembro del proveedor de servicios. A ese fin, las órdenes deberán remitirse a los representantes legales de los proveedores de servicios designados para al fin, remarcándose que este mecanismo solo puede funcionar con un alto nivel de confianza mutua entre los Estados miembros, en el marco de respeto de los derechos fundamentales a la libertad, seguridad, respeto de la vida privada y familiar, protección de datos personales, derecho de propiedad, tutela judicial efectiva, debido proceso, entre otros.

Se destaca que los proveedores de servicios más importantes a los efectos de recabar pruebas para procesos penales son los de comunicaciones electrónicas y de la sociedad de la información, que facilitan específicamente interacción entre usuarios. Incluyen los servicios de vos, sobre IP, los servicios de mensajería instantánea y los servicios de correo electrónico. Entre los segundos, incluye aquéllos que cuentan con almacenamiento de datos como componente esencial al usuario, en particular, las redes sociales, los mercados en línea y otros servicios de alojamiento de datos, inclusive los que prestan servicio a través de la nube.

A su vez, los proveedores de servicios de infraestructuras de internet relacionadas con los registros de nombres, números, como los registradores de dominio, como los proveedores de servicios de privacidad y representación, o los registros regionales de direcciones de protocolos de internet (IP) revisten especial importancia para la identificación de quienes están detrás de las páginas maliciosas.

Resulta muy ilustrativa la categorización de los datos que contiene el Reglamento, distinguiendo entre los datos de los abonados, los datos relativos al acceso y de transacciones (categorías denominadas “sin contenido”), así como los datos de contenido. Los dos primeros, se buscan para identificar al usuario subyacente, y el nivel de interferencia de los derechos fundamentales es similar. Los datos de transacciones, por su parte, suelen buscarse para obtener información sobre los contactos y el paradero del usuario, y para establecer el perfil de un individuo. Se explica que mientras los datos de los abonados y los relativos al acceso son útiles para obtener los primeros indicios de la investigación sobre la identidad del sospechoso, los datos de transacciones y los datos de contenidos son más relevantes con material probatorio, señalándose asimismo que las condiciones para obtener unos u otros son distintas debido al distinto grado de injerencia en los derechos fundamentales.

Finalmente, entiendo que son muy importantes los criterios que se emplean para establecer cuando un proveedor de servicios “ofrece servicios en la Unión”, habilitando así al Estado a imponerle obligaciones. Estos criterios son de avanzada porque deconstruyen concepciones estrictas de soberanía territorial y dan muestras de la fragmentariedad de los nacionalismos estrictos que imposibilitaban una cooperación penal eficaz en la comunidad global, donde los individuos, las empresas y las instituciones de gobernanza ya no están ligadas a hegemonías políticas territoriales de un Estado sino en base a otros parámetros.

Entonces, se evaluará si el proveedor permite a las personas físicas o jurídicas que se encuentren en una o más Estados miembros utilizar sus servicios. No obstante, como la mera accesibilidad de una interfaz en línea considerada aisladamente no es suficiente, será necesario establecer si el proveedor tiene un establecimiento en la Unión. A falta de establecimiento, deberá evaluarse la estrecha vinculación sobre la base de un número significativo de usuarios en uno o más Estados miembros, o la orientación de actividades hacia uno o más Estados miembros.

Dicha orientación, puede determinarse en función de factores como el uso de la lengua o una moneda utilizada generalmente en ese Estado miembro, o la posibilidad de encargar bienes o servicios. También puede derivarse de la disponibilidad de una aplicación móvil en la tienda de aplicaciones nacional, de la publicidad local o la publicidad en la lengua utilizada en dicho Estado miembro, o de la gestión de las relaciones con los clientes, como la prestación de servicios en la lengua comúnmente utilizada en tal Estado.

En cuanto a las órdenes, el reglamento prevé una orden europea de conservación que se emitirá para cualquier infracción con el objetivo de evitar la eliminación, supresión o modificación de los datos en situaciones en las que pudiera llevar más tiempo conseguir la entrega de esos datos, por ejemplo, cuando se utilicen los canales de comunicación judicial y el proveedor deberá conservarlos por 60 días. Y una orden europea de entrega y conservación que directamente requiere los datos almacenados.

Estas órdenes serán emitidas directamente al destinatario por la autoridad emisora, la autoridad judicial, con lo cual vemos aquí un antecedente de la norma de similar contenido del Segundo Protocolo Adicional que se analizará luego. Además, es importante porque se imponen plazos acotados y razonables para la información solicitada que deberá transmitirse a las autoridades en un plazo de 10 máximo, debiendo el proveedor respetar plazos más breves en casos urgentes, imponiéndose al proveedor que se vea dificultado a entregar la información a que lo informe directamente a la autoridad emisora a fin de ofrecer las justificaciones oportunas.

Para culminar, cabe destacar la importancia del sistema de sanciones para el proveedor incumplidor que se prevé, ya que, en caso de incumplimiento injustificado, la autoridad emisora podrá trasladar la orden completa al Estado miembro en que el proveedor esté establecido el destinatario. Este Estado deberá ejecutarla conforme con su legislación nacional, debiendo preverse sanciones pecuniarias efectivas, proporcionadas y disuasorias en caso de incumplimiento de las obligaciones del presente reglamento. Recordemos que la autoridad de ejecución solo podrá negarse a ejecutar la orden por motivos específicos ligados a privilegios e inmunidades con arreglo a su legislación nacional, o si la revelación puede afectar intereses fundamentales, como la seguridad o la defensa nacionales.

En definitiva, como veremos a continuación, este documento configura un antecedente en varios aspectos de la nueva regulación que se receptó luego

en el Segundo Protocolo Adicional al Convenio de 2001 sobre cooperación reforzada.

2.4. El sistema reforzado de cooperación internacional en el Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia

El Comité del Convenio sobre la Ciberdelincuencia (T-CY), en la sesión plenaria de redacción del Protocolo del T-CY de fecha 12 de abril de 2021, redactó este protocolo relativo al "refuerzo de la cooperación y de la divulgación de pruebas electrónicas" (13).

En la conferencia de apertura a la firma organizada en el marco de la presidencia italiana del Comité de ministros del Consejo de Europa (14), la Secretaria General señaló: "La ciberdelincuencia crece y evoluciona a un ritmo cada vez mayor. Lo perturba todo, incluyendo a las empresas, los hospitales y las infraestructuras críticas de las que todos dependemos. Hoy estamos haciendo una importante contribución al esfuerzo mundial en la lucha contra la ciberdelincuencia … El segundo Protocolo Adicional, por tanto, responde a la necesidad de una cooperación mayor y más eficaz entre los Estados, y entre éstos y el sector privado, aclarando los casos en los que los 'proveedores de servicios' podrán facilitar datos que posean directamente a las autoridades competentes de otros países. La relevancia de este Protocolo es una esperanza para las víctimas de la ciberdelincuencia".

El contenido del video de presentación del Protocolo en español explica: "Antes los delitos se cometían en un solo país, las víctimas y los autores estaban en el mismo lugar y los investigadores podían resolver el caso investigando el lugar del hecho físico. Ahora, la delincuencia se ha trasladado a internet, las pruebas dispersas para identificar a los delincuentes pueden estar en lugares extranjeros cambiantes y desconocidos. Sin embargo, los investigadores están limitados a su propio territorio y los medios tradicionales de obtener prueba en jurisdicción ajena no suelen ser eficaces. Esto significa que solo se atrapa una parte de los delincuentes y que rara vez se hace justicia con las víctimas…"

Y continúa: "Gracias al Consejo de Europa, luego de haber celebrado el primer convenio del mundo en la materia, ahora más de 600 expertos de 75 países han creado una nueva herramienta para luchar contra la ciberdelincuencia sin fronteras. El Segundo Protocolo Adicional viene a reforzar el Convenio. Por primera vez las fuerzas del orden podrán obtener directamente de los proveedores de servicios de otros países la información

que necesitan para dar con los ciberdelincuentes, además de establecer procedimientos para la asistencia mutua de emergencia".

La República Argentina participó del Grupo de Redacción del Protocolo a través de las Direcciones Nacionales de Cooperación Internacional y de Investigación Criminal dependientes del Ministerio de Seguridad de la Nación. También participó la Unidad Fiscal Especializada en Ciberdelitos del Ministerio Público Fiscal de la Nación y el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto.

El texto normativo define que se entenderá por "autoridad central" aquella designada por una Parte en virtud del párrafo 2.a del artículo 27 del Convenio, que en el caso de la República Argentina se asignó -como vimos- a una Secretaría dependiente del Ministerio de Relaciones Exteriores (art. 3). Agrega la noción de "autoridad competente" como toda *autoridad judicial*, administrativa u otra autoridad encargada de hacer cumplir la ley, que esté facultada por el derecho interno para ordenar, autorizar o llevar a cabo la ejecución de medidas en virtud del presente Protocolo con el fin de obtener o presentar pruebas en relación con investigaciones o procedimientos penales específicos.

Se consagran Principios Generales de las Medidas de cooperación reforzada, en el art. 5, entre ellos "el mayor esfuerzo posible para cooperar", lo que implica que no pueden negarse sin especificar las razones que, a su vez, pueden ser consideradas por el Estado solicitante para reformular su pedido. Por ello, cuando se permita a la Parte requerida condicionar la cooperación a la existencia de doble incriminación, se considerará cumplida esta condición, independientemente de que su legislación incluya el delito en la misma categoría de delitos o lo denomine con la misma terminología que la Parte requirente, si la conducta constitutiva del delito para el que se solicita la asistencia es un delito penal en virtud de su legislación.

Entre las novedades se destacan:

a. El procedimiento para mejorar la cooperación directa con proveedores y entidades de otras Partes. Así, para la "Solicitud de información sobre el registro de nombres de dominio", cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes (judiciales) para emitir una "solicitud a una entidad que preste servicios de nombres de dominio en el territorio de otra Parte" para obtener la información que esté en posesión o bajo el control de la entidad, con el fin de *identificar o ponerse en contacto con el titular de un nombre de dominio*. A su

vez, cada Parte adoptará las medidas para permitir que una entidad en su territorio divulgue dicha información en respuesta a una solicitud de aquel tipo.

En caso de falta de cooperación por parte de una entidad descrita, se activará un sistema de consultas. Así, la Parte requirente podrá pedir a la entidad que explique la razón por la que no divulga la información solicitada y solicitar consultas con la Parte en la que se encuentre la entidad, con miras a determinar las medidas disponibles para obtener la información. Para ello, se comunicará al Secretario General del Consejo de Europa la "autoridad designada" para los fines de consulta. Estas autoridades podrán coincidir o no con las "autoridades centrales" del art. 27 del Convenio.

b. El Procedimiento de divulgación de la información de los abonados, presenta una regulación similar a la de obtención de nombres de dominio. Igualmente,

A su vez, los firmantes podrán solicitar que cuando se emita una orden en los términos señalados a un proveedor de servicios de su territorio, se le haga una notificación simultánea, en todos los casos o en circunstancias determinadas. También podrá exigir que el proveedor de servicios le consulte sobre la posibilidad de divulgación. Las autoridades notificadas o consultadas podrán exigir al proveedor de servicios que no divulgue la información si puede perjudicar las investigaciones o procedimientos penales en ese territorio.

Si un proveedor de servicios informa a la autoridad que no divulgará la información sobre el abondado solicitada, o si no divulga la información en un plazo de 30 días a partir de la recepción de la orden o del plazo estipulado en el párrafo 4.d, las autoridades competentes de la parte emisora podrán solicitar la ejecución de la orden únicamente a través del procedimiento previsto en el artículo 8vo., u otras formas de asistencia mutua.

c. El Procedimiento entre autoridades para la divulgación de datos informáticos almacenados, conforme al artículo 8vo., establece que cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para *facultar a sus autoridades* competentes para emitir una orden que se presentará como parte de una solicitud a otra Parte con el fin de obligar a un proveedor de servicios en el territorio de la Parte requerida a presentar información específica y almacenada sobre los abonados y sobre los datos de tráfico, que sean necesarios para las investigaciones o procedimientos penales. A su vez, cada Parte adoptará las medidas necesarias para dar efecto a dicha orden de una Parte requirente.

En cuanto a los plazos, a partir de la recepción de la notificación con la información adicional, la Parte requerida hará esfuerzos razonables para notificar al proveedor de servicios en un plazo de 45 días a más tardar, y ordenará la devolución de la producción a más tardar en 20 días para la información de los abonados y en 45 días para los datos de tráfico. A su vez, dispondrá la devolución de la información obtenida a la Parte requirente sin demora indebida. Si hay demora adicional debe comunicarle a la Parte requirente a la mayor brevedad.

La Parte requerida podrá negarse a ejecutar una solicitud por los motivos establecidos en el Convenio de 2001, o podrá imponer condiciones que considere necesarias. Podrá también aplazar la ejecución de las solicitudes por esos motivos. Recordemos que estos motivos están ligados al resguardo de investigación en curso en la Parte requerida, o por motivos de protección del orden público interno o de intereses nacionales que se pondrían en riesgo con la provisión de la información.

Si la Parte requirente no puede cumplir una condición impuesta por la Parte requerida, se lo informará inmediatamente, para que reconsidere si a pesar de ello facilitará o no la información solicitada. Si la Parte requirente acepta la condición, quedará obligada a cumplirla. Al momento de la firma cada parte dará la información de contacto de las autoridades designadas para presente artículo.

d. El procedimiento de Divulgación Acelerada de datos informáticos almacenados en caso de emergencia, establece que Parte adoptará las medidas legislativas y de otra índole que sean necesarias para que su Punto de Contacto para la Red 24/7 pueda, en caso de emergencia, transmitir una solicitud a un Punto de Contacto de otra Parte y recibir una solicitud de éste, para obtener de un proveedor de servicios en el territorio *la divulgación acelerada* de determinados datos informáticos almacenados que estén bajo control de ese proveedor, sin necesidad de asistencia mutua. A su vez, cada Parte adoptará las medidas necesarias para permitir que sus autoridades puedan recabar datos de un proveedor de servicios en su territorio; y que un proveedor de servicios en su territorio divulgue los datos solicitados a sus autoridades. También, que sus autoridades faciliten los datos solicitados a la Parte requirente.

e. Los Procedimientos relativos a la asistencia mutua en caso de emergencia, establecen que cada Parte podrá solicitar asistencia mutua de manera rápida cuando considere que hay *una emergencia*. A ese fin, cada parte garantizará que una persona responsable de responder a las solicitudes de

asistencia mutua esté disponible las 24 horas los 7 días de la semana. Las autoridades responsables de ambas Partes podrán determinar de común acuerdo que los resultados de la ejecución de estas solicitudes, podrá facilitarse a la Parte requirente por un cauce alternativo.

Además, cada Parte podrá declarar que las solicitudes también podrán ser enviadas directamente a sus autoridades judiciales, o a través de los canales de la Organización Internacional de Policía Criminal (INTERPOL) o a su Punto de Contacto 24/7 establecido en virtud del art. 35 del Convenio de 2001. En cualquier caso, se enviará simultáneamente una copia a la Autoridad Central de la Parte requerida a través de la Autoridad Central de la Parte requirente.

Finalmente, resta destacar la implementación de los Equipos Conjuntos de Investigación, evidenciándose con esto la gran utilidad de este instrumento. Se establece que, de mutuo acuerdo, las autoridades competentes de dos o más Partes podrán crear un equipo conjunto de investigación. Estas autoridades acordarán los procedimientos y condiciones que regirán el funcionamiento de los equipos conjuntos de investigación, tales como sus fines específicos, composición, funciones, duración y prórrogas, ubicación, organización, requisitos aplicables a la recopilación, transmisión y utilización de información o pruebas, cláusulas de confidencialidad y condiciones para la participación de las autoridades participantes de una Parte en las actividades de investigación que tengan lugar en el territorio de otra Parte.

Dichas autoridades competentes y participantes se comunicarán entre sí directamente y cuando sea necesario adoptar medidas de investigación en el territorio de una de las Partes, las autoridades participantes podrán solicitar a sus propias autoridades que adopten dichas medidas sin que las otras Partes tengan que presentar una solicitud de asistencia mutua.

Si el acuerdo no fija condiciones para denegar o restringir el uso de la información, las Partes podrán usar la información o las pruebas proporcionadas: a) para los fines contemplados en el acuerdo; b) para la detección, investigación y enjuiciamiento de delitos distintos de aquellos contemplados en el acuerdo, con la autorización previa de las autoridades que proporcionen la información o las pruebas, y c) para prevenir una emergencia.

2.5. La importancia creciente de Interpol para la investigación de ciberdelitos

Hablamos de la importancia creciente porque si bien la organización fue fundada hace más de cien años, su intervención se ha vuelto fundamental,

especialmente, al momento de investigar delitos transnacionales que han proliferado en los últimos años como consecuencia de los avances tecnológicos, económicos y sociológicos, tales como la ciberdelincuencia y el tráfico ilícito de personas.

Cabe recordar que entre el listado de crímenes que son de su competencia, se destacan los delitos de corrupción, falsificación de moneda y documentos de seguridad, delitos contra menores, delitos contra el patrimonio cultural, ciberdelincuencia, tráfico de drogas, delitos contra el medio ambiente, delincuencia financiera, trata de personas, tráfico de armas de fuego, delitos marítimos, delincuencia organizada, tráfico ilegal de migrantes, terrorismo, delincuencia relacionada con los vehículos, crímenes de guerra. De la sola nomenclatura parece evidente que la materia de su actuación está conformada por delitos de naturaleza transnacional.

En su estructura orgánica, cuenta con un Centro de Mando y Coordinación (CCC), primer punto de contacto de cualquier país que requiera ayuda urgente de la Secretaría General o de otro país. Los miembros de su personal pueden asistir en distintos idiomas a policías nacionales de diferentes zonas horarias que requieran ayuda en materia de investigación.

Bajo la premisa “apoyo policial en tiempo real”, la organización recibe y evalúa los mensajes policiales llegados a través del sistema I-24/7, red mundial de comunicación policial protegida. Además, coordina la comunicación entre las Oficinas Centrales Nacionales de Interpol (OCN) en cada país, Oficinas Regionales y las unidades de delincuencia en la Secretaría General. También realiza comprobaciones instantáneas en las bases de datos de la organización y responde a consultas urgentes, publica notificaciones o alertas sobre delitos inminentes o potenciales y asume la función de gestión de crisis tras sucesos graves.

A su vez, cabe destacar el intercambio de Información a nivel mundial, ya que brinda a sus países miembros acceso inmediato y directo a una amplia gama de bases de datos policiales. Se trata de un sistema que presenta condiciones de adaptación al usuario a través del panel de mandos del sistema I-24/7 (portal de Internet de acceso restringido), excepto a la de imágenes de explotación sexual de niños.

Estas bases contienen datos nominales sobre más de 225.346 registros de delincuentes internacionales, personas desaparecidas y cadáveres, con sus correspondientes historiales delictivos, fotografías, huellas dactilares; como así también cuenta con unos 226.000 perfiles de ADN provenientes de 87 países

que pueden servir para resolver casos y establecer la identidad de cadáveres y víctimas. A su vez, contiene unas 220.000 fichas dactilares y más de 17.000 huellas latentes, procedentes del lugar de los hechos, remitidas por los países miembros, ya sea por vía electrónica o por correo postal. En cuanto a las Imágenes de explotación sexual de niños, se cuenta con la Base de Datos Internacional de Interpol sobre Explotación Sexual de Niños (ICSE), cuyas imágenes han permitido a los investigadores la identificación de 21.458 víctimas, así como a 9.698 delincuentes, cifras estas válidas a 31 de diciembre de 2019 (15).

En materia de ciberdelitos presta una tarea de colaboración a las fuerzas del orden de todo el mundo para entender esta nueva forma delictiva y su investigación, considerando el uso de las tecnologías que aseguran el anonimato del usuario en aumento, se asignan recursos al tratamiento de criptomonedas virtuales y la red oscura a la que solo se puede acceder mediante un software especializado, y que, más allá de sus ventajas, pueden facilitar el tráfico ilegal de drogas, armas y explosivos, la trata de personas, el blanqueo de capitales, las actividades terroristas, y la ciberdelincuencia.

En la actualidad Interpol colabora con el proyecto Titanium financiado por la Unión Europea, participando en el desarrollo de GraphSense, una herramienta de análisis de cadenas de bloques que permite rastrear las transacciones realizadas con criptomonedas, que permite la ubicación de direcciones, etiquetas y transacciones de criptomonedas con las que identificar los clústeres en torno a una dirección permitiendo “seguir el rastro del dinero” para avanzar en sus investigaciones.

A su vez, ha desarrollado herramienta analítica denominada Darkweb Monitor para recopilar datos sobre actividades delictivas en la red oscura con los que luego se generará una información policial que facilitará las investigaciones de casos en todo el mundo- Entre los datos a recabar se encuentran direcciones de criptomonedas; claves PGP; direcciones IP; nombres de usuario y alias; direcciones electrónicas; dominios de los mercados de la red oscura; foros de la red oscura e historial de datos recopilados en la red oscura desde 2015.

Además, la organización cuenta con un Equipo Especial sobre la Red Oscura y las Criptomonedas que está elaborando una taxonomía mundial de las criptomonedas, esto es, un conjunto de clasificaciones para determinar qué categorías de datos de transacciones sospechosas con criptomonedas deben recopilarse, que se difundirá a escala global como una guía estandarizada. Se

prevé seguir un procedimiento similar al del etiquetado de fotografías digitales a la que se agrega una etiqueta con la localización geográfica de la imagen, la fecha en la que fue tomada y el tipo de cámara utilizada. Organizado esto en torno a tres categorías de información: a. Entidades: particulares, organizaciones y entidades digitales; b. Servicios: mercados de la red oscura, plataformas de intercambio de criptomonedas, facilitadores de mensajes y otros proveedores de servicios relacionados con la transacción; y c. Tipos de delitos: delitos con los que está relacionada la transacción, tales como el comercio ilícito en línea de drogas o armas, abusos sexuales de menores, terrorismo o ciberdelitos.

Entre sus proyectos en desarrollo se encuentra también CapaCT, financiado por el Ministerio de Asuntos Exteriores de los Países Bajos, destinado a la investigación en línea del terrorismo encontrándose en elaboración un manual dirigido a las fuerzas del orden del Sudeste Asiático para combatir el uso indebido de la red oscura y las criptomonedas por parte de los terroristas. En esa misma línea, junto con el Ministerio de Justicia del Estado de Baviera, han creado el Grupo de Trabajo sobre la Red Oscura y las Criptomonedas en el que los especialistas que lo integran comparten información sobre metodologías y herramientas para la identificación de delincuentes.

2.6. La importancia creciente de organismos multinacionales como NCMEC.

El Centro Nacional para Menores Desaparecidos y Víctimas de Explotación Sexual, es una ONG estadounidense que tiene convenio con las fuerzas de seguridad de Estados Unidos y con las principales empresas de Internet para monitorear el contenido que circula por la web y detectar potenciales situaciones de pedofilia. Si bien fue creado en el año 1998 con la ayuda de una donación privada y después del alarmante aumento de los informes relacionados con la explotación sexual de niños, recién en el año 2013, el Ministerio Público Fiscal de la Ciudad de Buenos Aires firmó un acuerdo para recibir reportes de distribución de contenidos con pornografía infantil y posibles casos de grooming en Internet procedentes de IPs ubicadas en el país. Los reportes de NCMEC son recibidos por el Cuerpo de Investigaciones Judiciales de la Fiscalía de la Ciudad (CIJ), que da curso al fiscal que corresponda según la competencia territorial y material en cualquier punto del país (16).

Estos reportes tienen cuatro categorías. La primera, identificada formalmente con el número 1, refiere a que hay un menor en situación de peligro, es decir, cuando se detecta que el niño está siendo abusado en un video en vivo. La segunda, advierte que hay un menor al alcance del denunciado, cuando, por ejemplo, toda la pornografía que se detecta proviene de un mismo menor o cuando existe información de que el menor es parte del entorno familiar. La tercera, implica que las características de las imágenes son de factura amateur y no profesional, pero que en principio no hay datos ciertos de que ese menor tiene un contacto con el pedófilo. Finalmente, la cuarta categoría (identificada con la letra E) significa que hay denuncias de las prestadoras de contenidos de internet, NCMEC no las analiza, pero sí las envía al país correspondiente.

Lo importante es que cada uno de los reportes especifica la IP a través de la cual fueron enviadas las imágenes, tras lo cual, el CIJ verifica a qué proveedor de Internet pertenece esa IP y se comunica con el proveedor para que le aporte datos del usuario. Cuando el fiscal considera que tiene las pruebas suficientes, solicita el allanamiento de todos los domicilios involucrados y, eventualmente, la detención de los imputados. También se solicita al juez la protección de los menores en riesgo. Se estima que, actualmente, el CIJ está procesando algo así como 50.000 denuncias al año.

En relación con los proveedores de servicios, NCMEC tiene convenios con todas las empresas 2.0 propietarias de todas las plataformas y redes sociales del mundo y para detectar la distribución de material que contiene pornografía infantil, se recurre a programas que utilizan inteligencia artificial para analizar grandes cantidades de información. Con esos softwares, grandes empresas como Facebook, Google y Dropbox puedan rastrear diariamente los millones de archivos que intercambian sus usuarios. Esta aplicación funciona convirtiendo cada archivo (texto, fotografía o vídeo) en un “hash” o código alfanumérico de veinte caracteres.

De esta manera, cuando alguien copia o difunde alguno de los archivos considerados peligrosos, hay una base de datos específica de pornografía, surge una alerta instantánea. Las compañías informáticas trasladan estas informaciones al NCMEC y es la ONG quien eleva una denuncia al Departamento de Seguridad Nacional de Estados Unidos. En el caso de que la IP sea extranjera, el organismo de Seguridad Nacional estadounidense deriva el caso al país en el que se registró la IP.

Por su parte, se cuenta con un Programa de identificación de Víctimas Infantiles que comenzó en 2002 después de que los analistas de NCMEC vieran repetidamente imágenes de los mismos niños víctimas en sus revisiones y comenzaran a rastrear qué víctimas habían sido identificadas previamente por la policía, habiéndose identificado hasta el momento más de 19.100 niños, a lo que se suma la tarea de ayuda a localizar información sobre las víctimas infantiles aun no identificadas para rescatarlas (17).

V. CONCLUSIONES.

Así las cosas, ha llegado el momento de efectuar las inferencias de los resultados de la investigación, para luego proceder a la contrastación del objetivo propuesto a los fines de establecer la verificación del cumplimiento del objetivo propuesto.

Las principales inferencias del Segundo Protocolo Adicional son las siguientes:

1. Refleja un cambio de paradigma de las relaciones internacionales para la cooperación penal internacional. Es decir, se ha plasmado con fuerza que el interés de los Estados en combatir de manera eficiente el flagelo del cibercrimen supera otros intereses que históricamente se consideraron primordiales en las relaciones internacionales tales como los de protección del orden público interno y de la soberanía territorial de un Estado. Por lo pronto, de esto mismo, ya puede inferirse que surge una responsabilidad internacional para el Estado parte de aplicar políticas internas en ese sentido.

2. Se concede protagonismo a las autoridades judiciales en la cooperación penal, empoderándolas para actuar directamente tanto al momento de solicitar pruebas como de remitirlas. El Estado asume así el compromiso de permitir canales de comunicación directos entre las autoridades judiciales de la investigación (fiscales, policías, jueces) y las entidades privadas proveedoras de servicios ubicadas en territorios de otros Estados parte. A su vez, compromete a los Estados parte que tiene localizados en su territorio esas entidades provean lo necesario para brindar la asistencia y cooperar con la entrega de la información. Desde ya se considera esto una evolución pues ningún organismo se encuentra en mejor posición para la cooperación que los propios operadores judiciales que realizan las investigaciones.

A diferencia el Convenio de 2001, este Protocolo concede un papel central a los jueces, fiscales y policías, estableciendo por definición que la

“autoridad competente” puede ser una autoridad judicial, administrativa u otra autoridad encargada de hacer cumplir la ley, que esté facultada por el derecho interno para ordenar, autorizar o llevar a cabo la ejecución de medidas en virtud del presente Protocolo con el fin de obtener o presentar pruebas en relación con investigaciones o procedimientos penales específicos.

Esto significa, entiendo que, desde la adhesión de la República Argentina al Segundo Protocolo, los operadores judiciales podrán actuar de conformidad a estos preceptos, sin necesidad de legislación interna previa, ya que el instrumento deja abierta la opción de la legislación o demás medidas que estime necesarias para ello. De esta manera, sí se requerirá una tarea política criminal acorde y adecuadas de parte de la cabeza de los Ministerios públicos Fiscales -Fiscalías Generales- instruyendo a los subordinados con lineamientos en este sentido.

3. Si bien el proveedor de servicios puede negarse a cooperar voluntariamente, solo podrá hacerlo cuando los datos pudieran perjudicar otras investigaciones que se llevan a cabo en su territorio, o en caso de afectación de cuestiones de orden público interno o de soberanía territorial, tal como ya se preveía en el Convenio de 2001, lo cual restringe la arbitrariedad. Además, frente a la negativa, la Parte requirente contará aun con varias posibilidades más ya que podrá pedir la intervención de la autoridad de la Parte del territorio donde se ubica el ente, la cual sí tendrá facultades para obligar al mismo a suministrar esa información.

4. Si bien la Parte requerida, a su vez, podría denegar la solicitud, tiene las mismas exigencias de justificar la negativa con motivos tasados. A su vez, resulta un avance que, para el trámite, ya no necesariamente deberá tratarse de una “autoridad central” en los términos del Convenio de 2001, por lo cual, nada impide que dicha autoridad se trate de un funcionario judicial.

Además, frente a la negativa, aun la parte requirente contará con más opciones en aras de conseguir su pedido, ya que se podrá llevar a cabo un sistema de consultas mutuas entre los Estados involucrados para evitar el rechazo sin más, como una suerte de negociación con fines de lograr la cooperación, en la que eventualmente se pedirá al requirente que modifique algún aspecto de su solicitud inicial.

5. En los casos de emergencia, se establece la obligatoriedad de adoptar medidas que permita la “divulgación acelerada de determinados datos”, a cuyo fin los Puntos de Contacto de cada Parte designados a los fines de la Red 24/7 deberán estar siempre disponibles, con lo cual, el nuevo documento viene a

ratificar la importancia del rol institucional de esos funcionarios. Aquí, es importante destacar que se está dirigiendo una directiva clara a las autoridades estatales de las que depende el Punto de Contacto, en el caso de las República Argentina el poder ejecutivo a través del Ministerio de Justicia y Derechos Humanos, quienes deberán disponer una reglamentación adecuada a la altura de las circunstancias y demuestre la voluntad real de hacer efectivo este procedimiento.

6. Otro avance se observa al haberse facultado a los Estados parte para la obtención de testimoniales en el extranjero mediante videoconferencia, otorgando amplias atribuciones a la Parte requerida para la adopción de medidas coercitivas en caso de falsedad o inasistencia del testigo, promoviéndose las consultas mutuas entre ellos la manera de garantizar el debido proceso, el tratamiento de reclamaciones de privilegios de inmunidad, el tratamiento de objeciones a preguntas o respuestas, etc. La Parte requerida podrá adoptar los medios necesarios para obligar a un testigo o perito a comparecer e imponer sanciones por falso testimonio.

7. Resulta de suma importancia que a partir de ahora, en la cooperación en casos de emergencia, se compromete a los Estados firmantes a la adopción de las medias legislativas o de otra índole que sean necesarias para que celebren acuerdos caso por caso o generales tendientes a que las solicitudes sean enviadas directamente a sus autoridades judiciales a través de Interpol o de su punto de Contacto 24/7, lo cual agiliza exponencialmente cualquier procedimiento internacional al prescindir del exhorto internacional con intervención de cancillería.

Nuevamente aquí, surge una directiva clara para las autoridades estatales con competencia, de dictar los reglamentos, directivas y procedimientos necesarios para hacer efectivo ese mecanismo. En el caso de la República Argentina, además del Ministerio de Justicia y DDHH de la nación, será incumbencia también del Ministerio de Seguridad de la Nación que tiene a su cargo la policía federal y mantiene interacción con la oficina en el país de Interpol.

Esta incumbencia no es arbitraria sino surge como un mandato claro del nuevo instrumento. La gravedad de la situación internacional por el avance de la criminalidad cibernética transnacional denunciada en el Preámbulo del Segundo Protocolo y en su video de presentación, ya no deja lugar a duda sobre la interpretación de la naturaleza jurídica que tiene ese mandato para los Estados parte: no se trata de una simple recomendación sino de una auténtica

obligación que asume el Estado susceptible de acarrearle responsabilidad internacional.

Se infiere también la importancia creciente de Interpol, en los últimos años, como organismo multilateral de lucha contra el cibercrimen, a partir de numerosos programas y proyectos de colaboración, instrucción y participación con las fuerzas policiales de los distintos Estados que la integran para hacer frente a este nuevo fenómeno.

De hecho, el origen mismo de la Organización Internacional de Policía y su devenir histórico, es una muestra muy representativa de voluntarismo político en aras de la cooperación penal para combatir el delito que comenzó en 1914, cuando policías y abogados procedentes de veinticuatro países se reunieron para debatir sobre técnicas de identificación y captura de fugitivos. Dejando de lado pruritos derivados de recelos nacionalistas y de protección interna, durante más de 100 años policías de todo el mundo han cooperado para prevenir y luchar contra la delincuencia. Tan necesaria fue que, mediante el Estatuto del 13 de junio de 1956 dictado en la 25° Asamblea General Celebrada en Viena, se creó la Organización, tal como la conocemos hoy, conformada por más de cincuenta países fundadores, entre los cuales se encontraba la República Argentina, contando para el año 1967 cien países miembros, pasando a tener ciento noventa y cinco en el año 2001.En la actualidad, como vemos por su propia naturaleza y funciones, configura una herramienta indispensable para combatir delitos transnacionales.

Es decir, la historia de las relaciones internacionales a los fines de la cooperación penal viene dando muestras de la necesidad constante de generar instituciones e instrumentos, cuyo efectivo funcionamiento se ha vuelto un interés primordial más que nunca en los últimos años. Por ello, puede concluirse, sin exagerar que, ante tanta evidencia y los claros parámetros que emergen, el Estado nacional ya no tiene margen para desatender los compromisos asumidos sin incurrir en responsabilidad internacional.

Así ocurrió con el European cybercrime Center (EC3) ya referido, otra experiencia más que puede encontrarse en la historia de las relaciones internacionales para la cooperación penal, que no deja lugar a duda acerca de las obligaciones de todo Estado nación que se considere parte de la comunidad del derecho internacional público, como evidentemente lo es la República Argentina por su membresía en las principales organizaciones internacionales del mundo, más aún por su adhesión al Convenio de cibercriminalidad de Budapest.

Aquella nueva obligación del Estado de la que hablamos, impone ante todo una toma de conciencia del sentido y la importancia de mecanismos como éste, para luego aplicar políticas acordes en el territorio. Así, en lo relativo al EC3, las autoridades competentes de la República Argentina procurarán contactarse con los miembros y conseguir el apoyo de este Centro, que se plantea como una plataforma cooperativa sobre esta materia que funciona principalmente a través de Europol pero que puede ayudar a otras instituciones ya apuntadas como Eurojust. Tiene también una cierta función pedagógica o divulgativa sobre la materia, a través de la creación de guías de buenas prácticas, estudios estadísticos, recomendaciones, contribuyendo a la creación progresiva de un *corpus de soft law* destinado a guiar y a formar jurídicamente tanto a operadores jurídicos como a la sociedad en general, al encontrarse en dominio abierto.

En este sentido, la República Argentina tiene la obligación de sumarse a la política criminal de la UE, estableciendo mecanismo concretos para concertar acuerdos con las instituciones existentes destinadas a luchar contra delitos cibernéticos por su propio perfil transfronterizo, poniendo el acento en la fase de investigación, a sabiendas del peligro de anonimato y la amplia difusión a través de Internet hacían necesaria una respuesta no solo preventiva, sino que atajara el problema en sus inicios a través de agentes policiales especializados en cibercriminalidad y que al mismo tiempo estuvieran interconectados en sus diferentes estados miembros.

8. El Segundo Protocolo recupera la figura de los Equipos Conjuntos de Investigación, ya previstos en otras normas internacionales, en una demostración de la utilidad de este mecanismo que, además, había venido siendo implementando a lo ancho y lo largo de todo el mundo desde la cabeza del Ministerio Publico Fiscal de la nación argentina pero también de diversos países, tanto en el ámbito del Mercosur, como en el ámbito Iberoamericano y de la Unión Europea, a través de los acuerdos para la investigación de delitos generalmente con un componente transfronterizo.

Conforme al Segundo Protocolo, los procedimientos y condiciones que rijan el funcionamiento de los equipos conjuntos de investigación -tales como sus fines específicos; composición; funciones; duración; organización; las condiciones de recopilación, transmisión y utilización de la información o de las pruebas; etc.-, serán los acordados entre dichas autoridades competentes (judiciales).

Lo cual demuestra, una vez más, el lineamiento de política criminal del nuevo sistema de cooperación reforzado, tendiente al empoderamiento de los órganos judiciales de la investigación, a los cuales se conceden potestades suficientes para adoptar políticas de cooperación internacionales y tomar iniciativas para la conformación de Equipos con otros pares del extranjero.

La profusa actividad de concertación que el MPF de la Nación ha venido realizando en este sentido en la última década que se ha analizado supra, demostraba la insuficiencia de los procedimientos existentes en el Convenio de 2001 pero sobre todo denunciaban la falta de acompañamiento político de los otros poderes del Estado, en particular del poder ejecutivo a través de los ministerios que hemos señalado, que ninguna actividad realizaron y omitieron el dictado reglamentaciones, directivas o procedimientos tendientes a hacer efectivos mecanismos adecuados de cooperación.

Paralelamente, la extendida receptividad de este mecanismo en todo el mundo evidenciaba una concepción generalizada de parte de los operadores judiciales, quienes mejor posición tienen para evaluar esto, sobre sus bondades como práctica útil y eficaz para la investigación de delitos transnacionales.

Ahora, con la incorporación de este mecanismo en el Segundo Protocolo surge evidente la obligación del Estado argentina en impulsar y promocionar su utilización, más allá de la legislación interna que deba dictarse. Esta obligación incumbe, por un lado, a la cabeza de los MPF tanto provinciales como nacional con competencia para fijar la política criminal. Dicha política debe articularse partiendo del supuesto de que, ante todo, el adecuado funcionamiento de este tipo de mecanismos se sustenta en la confianza mutua entre los Estados y sus actores judiciales. De ese lugar, tal como indica la experiencia común y las reglas de la psicología, como no puede haber confianza sin conocimiento previo entre los actores, es decir, sin haberse en entablado una relación, lo principal será establecer una agenda tendiente a identificar a los jueces o fiscales con competencia y autoridad por lo pronto de los países adheridos al Convenio de Budapest, para luego tomar de contacto efectivo, procurar entrevistas y reuniones.

Esta política de relación exterior entre funcionarios judiciales solo puede ser articulada por la cabeza política de los MPF tanto locales como de la nación con competencia para diseñar la política criminal (Fiscalías Generales), tal como se ha visto en los numerosos ejemplos de acuerdos concretados a esos fines por la nación. No obstante, tal como se ha venido sosteniendo, el poder ejecutivo también tiene aquí su cuota de competencia y será su

responsabilidad promover estos mecanismos, por lo pronto, agregando entre las funciones de la Autoridad Central del Ministerio de Relaciones Exteriores y del Punto de Contacto del Ministerio de Justicia la de colaboración activa en este proceso de interrelación, promoviendo el conocimiento mutuo y los encuentros de los jueces y fiscales con sus pares en el extranjero, dado que, además, son ellos quienes mejor posición tienen para esa tarea por su vinculación y acceso directo a las Autoridades Centrales y los Puntos de Contacto de todos los países del Convenio. En esa misma línea, será responsabilidad del poder ejecutivo a través del Ministerio de Seguridad encarar una tarea similar a través de Interpol, cuya oficina en la República Argentina configura un medio idóneo como punto de salida para extender contactos a las demás oficinas citas en otros países de interés y a través de ellas a las autoridades judiciales de dichos lugares.

En definitiva, si bien los Equipos se conforman en principio a los fines de investigaciones determinadas, todo indica la conveniencia de avanzar más allá, implementando políticas de relaciones exteriores a priori con los principales actores, entablado previos contactos, ofreciendo ayuda y colaboración y poniéndose a disposición. Además, para contribuir al proceso de confianza mutua, será fundamental adoptar una actitud de ofrecimiento basada solo en la buena voluntad, a cuyo fin el instituto de la remisión espontánea de información prevista en el Segundo Protocolo configura un buen ejemplo. Es decir, si se pretende es suscitar círculos de confianza mutua, el fiscal o el juez local que lleva a cabo una investigación que se encontrare con información o datos que pudieran ser de interés para un par en el extranjero, proceder a compartirla sin más es una buena manera de iniciarlo. El objetivo final será en un futuro próximo que la información fluya entre las jurisdicciones sin mayores restricciones ni controles.

En esa línea, para identificar información de utilidad para fiscales extranjeros, habrá de considerarse la información sobre el posible origen o destino extranjero de sustancias estupefacientes, material de contrabando, remesas ilícitas, armas ilegales, víctima en delito de trata de personas; la información sobre bienes muebles o inmuebles en el extranjero que formen parte de una investigación; la posible mención de funcionarios públicos extranjeros en investigaciones por corrupción; constatación de reiterados viajes sin razón justificable al extranjero de personas investigadas; la presencia de documentos extranjeros falsificados; información sobre el giro de divisas o constitución de empresas en el extranjero de personas investigadas; identificación de lazos con organizaciones criminales extranjeras; o demás

datos concretos sobre delitos cometidos en otro país que se dejan de prueba documental o testimonial.

9. El proyecto de reglamento sobre una orden europea de conservación y una orden europea de solicitud de pruebas electrónicas de 2018, destaca que actualmente se utilizan datos electrónicos en el 85% de las investigaciones penales, lo que seguramente seguirá en aumento en el futuro. Mientras que la solicitud propia de pruebas electrónicas de un país a otro está presente en la mitad de los casos que intentan esclarecer.

Dicho Proyecto de Reglamento del Parlamento y del Consejo de Europa, del año 2018, brinda parámetros que deben emplearse para interpretar el Segundo Protocolo Adicional, puesto que fue su antecedente. Este documento en su momento configuró una declaración política en contra de la ineficacia del sistema de cooperación existente, motivada, lamentablemente, por los atentados terroristas ocurridos en Bruselas. En ese sentido, nuevamente, cabe resaltar los Estados deben hacerse eco de estas medidas y, aunque la República Argentina no forme parte de la UE, es de competencia de los distintos poderes del Estado asumir esas políticas como directrices para diseñar la política interna y, en particular, al momento de adherirse al Segundo Protocolo Adicional que configura una continuidad de aquella normativa.

Entonces, cuando se afirma que los distintos poderes del Estado tienen incumbencia y responsabilidad, implicará para la cabeza de los MPF tanto locales como nacional, considerar una instrucción que habilite a los fiscales para pedir datos de naturaleza electrónica directamente a un proveedor de servicios o su representante legal en otro Estado miembro, pudiendo hacer uso de los plazos reducidos de 10 días, e incluso en solo 6 horas en caso de necesidad o extrema urgencia. Si bien podría objetarse que esos plazos no están cubiertos por el Segundo Protocolo Adicional, debe reiterarse que esta reglamentación deriva del mismo órgano político -Consejo de Europa y Parlamento europeo-, que ordenó la redacción del Segundo Protocolo, que podría interpretarse como una base legal que proporciona un piso mínimo, pero nada obsta que los Estados vayan más allá si se trata de conseguir la tan deseada eficacia.

Además, el enfoque de la Comisión a través de ese proyecto adquiere una proyección mundial y se intenta progresar en una etapa de internacionalización global de la medida en junio de 2019. Estas negociaciones se concretan en una autorización para que la Comisión Europea negocie este acuerdo con EEUU y se pudiera llegar a un acuerdo con ello en aplicación de las

órdenes de acceso transfronterizo a pruebas electrónicas, sobre todo, considerando que en la actualidad el traspaso de este tipo de información electrónica entre EEUU y Europa tarda una media de 10 meses en hacerse efectiva, lo que acabaríamos acortando a un plazo máximo de 10 días o inferior en casos de ciberataques terroristas.

A su vez, puede verse el surgimiento de otra directiva clara para el poder ejecutivo, quien a través del Ente Nacional de Comunicaciones conjuntamente con la Dirección de Ciberseguridad de la Jefatura de Gabinete de Ministros del gobierno nacional, deberá establecer reglamentos o directivas tenientes obligar a los proveedores de servicios a designar representante legal en la República Argentina, pudiendo obligarlos a remitir la información bajo sancione pecuniarias razonables y proporcionadas. En contraprestación gozarán de mayores garantías de seguridad jurídica y tendrán relación directa con las agencias policiales europeas. Estos representantes legales tendrán además responsabilidad solidaria en caso de incumplimiento

Recordemos que se utiliza el criterio de la estrecha vinculación, cuando el proveedor tenga un establecimiento en el país, o sobre base de un número significativo de usuarios en uno o más Estados miembros, o en función de la orientación de actividades hacia uno o más Estados miembros, en virtud de factores como el uso de la lengua o una moneda utilizada generalmente en ese Estado miembro, o la posibilidad de encargar bienes o servicios. También, puede derivarse de la disponibilidad de una aplicación móvil en la tienda de aplicaciones nacional, de la publicidad local o la publicidad en la lengua utilizada en dicho Estado miembro, o de la gestión de las relaciones con los clientes, como la prestación de servicios en la lengua comúnmente utilizada en tal Estado, entre otros.

VI. REFLEXIÓN FINAL: RECOMENDACIONES Y PLANTEAMIENTOS PARA FUTURAS INVESTIGACIONES

A partir de todo lo dicho y en función de estas inferencias, cabe concluir que están dadas las bases jurídicas y las instituciones necesarias para la implementación de todos aquellos mecanismos de cooperación novedosos que se han explicitado, de manera que, solo se trata, ahora -a partir de la adhesión de la República Argentina al Segundo Protocolo Adicional al Convenio en el corriente año-, que cada área gubernamental que tenga incumbencia en los diferentes asuntos, asuma con seriedad la competencia que se le ha asignado procediendo al dictar la reglamentación, las directivas y procedimientos necesarios para hacer efectivos esos mecanismos, sin perjuicio de la legislación

interna que deba sancionarse. Entonces, como dijimos, no se trata de una simple recomendación que surge de la normativa internacional, sino que ha emergido para el Estado argentino una auténtica obligación susceptible de generar responsabilidad internacional en caso de incumplimiento.

Desde ese lugar, se ha demostrado el objetivo central de este trabajo, en el sentido de que, para encontrar una salida política y jurídica al problema planteado, los instrumentos legales más recientes, como son el Proyecto de Reglamento del Parlamento europeo y del Consejo de Europa 0108/2018 y, fundamentalmente el Segundo Protocolo Adicional al Convenio de 2001, proporcionan herramientas útiles que ya pueden ir implementando los operadores judiciales locales -sin perjuicio de la legislación interna que deberá dictarse- a partir del compromiso asumido por la República Argentina con su adhesión.

Se ha demostrado que instrumentos están destinados a empoderar a las autoridades judiciales locales para actuar directamente hacia el exterior sin pasar por órganos de cancillería nacionales. Por lo que será esencial, para comenzar, que los altos mandos de los MPF provinciales y nacional -Fiscalías Generales- tomen conciencia y asuman su competencia con toda la confianza de la potestad que se le ha asignado para luego impartir las instrucciones necesarias a sus subordinados. Entre los aspectos que incluirá las nuevas directivas, además de la habilitación para actuar directamente solicitando o remitiendo datos electrónicos, estará la de habilitarlos a conformar Equipos Conjuntos de Investigación y procurar acciones para establecer vínculos activos y sostenidos en el tiempo con instituciones de la cooperación penal internacional de relevancia en la actualidad, como lo es Interpol y el EC3.

También se ha demostrado que, para la efectiva implementación de esos mecanismos, se requiere el accionar conjunto de todos los poderes del Estado, en sintonía política con la nueva tendencia internacional para la cooperación penal, fundamentalmente en razón de las importantes incumbencias que tiene el poder ejecutivo a través del Ministerio de Relaciones Exteriores y Culto, del Ministerio de Justicia y Derechos Humanos, del Ministerio de Seguridad y del Ente Nacional de comunicaciones en conjunto con la Dirección de ciberseguridad dependiente de la Jefatura de Gabinete de Ministros, en cuyos ámbitos actúan la Autoridad Central y el Punto de Contacto de la Red 24/7 en cumplimiento del Convenio de 2001, como así también, se tramitarán las relaciones con la oficina nacional de Interpol y bajo cuya órbita (ENACOM) deben controlarse los proveedores de servicios de comunicaciones electrónicas. Pues, todos estos organismos configuran engranajes

fundamentales en la logística necesaria para implementar los mecanismos avanzados de cooperación.

Se ha demostrado, entonces, que más allá de los lineamientos jurídicos para los operadores judiciales que emergen del Segundo Protocolo Adicional, el instrumento impone una serie de obligaciones adicionales tácitas que recaen, también, en otros poderes del estado y les demandan un alineamiento con las políticas de máxima cooperación. Tan es así, que surge evidente que sin ese apoyo político del Estado en sus distintas funciones, ninguna chance de éxito tendrán los nuevos mecanismos implementados. Las denuncias y exclamaciones de preocupación por el flagelo de los delitos transnacionales potenciados por las nuevas tecnologías de la investigación que se realizan en el Preámbulo del Segundo Protocolo y en su video de presentación, entre otros, deja en evidencia que el Estado parte no podrá desatender esas políticas.

Sobre este aspecto, vale aclarar que ciertos intereses que se han ligado históricamente al concepto de soberanía territorial para justificar criterios estrictos de proteccionismo, tales como la protección de las garantías judiciales y derechos fundamentales de los connacionales o del orden público interno o de los intereses nacionales, en la actualidad han perdido contendido real, porque la proliferación de tratados internacionales de derechos humanos y de otra naturaleza suscriptos por la mayoría de los Estados de la tierra, demuestra que existe un núcleo duro de respeto a ciertos intereses esenciales para los Estados que son compartidos por la mayoría de las naciones de la sociedad global, que, además, integran distintas organizaciones internacionales humanitarias. A su vez, como contracara han emergido intereses superiores y fundamentales para la comunidad internacional entre los cuales está el de combatir eficazmente contra los delitos transnacionales.

En definitiva y para concluir, la directriz interpretativa que obliga a los distintos poderes del Estado como parte de la comunidad internacional y del Convenio de 2001, consiste en receptar debidamente el mandato de deconstruir los instrumentos judiciales y los conceptos de jurisdicción y competencia para que efectivamente se sancionen estas conductas, bajo la idea clara de que la actuación del Estado en este aspecto, hoy, pasa por una necesaria fragmentación de la soberanía. Es necesario que los Estados establezcan mecanismos de soberanía compartida, una hibridación del derecho y de los organismos de seguridad para enfrentar el delito.

Como bien se expone en el Preámbulo del Segundo Protocolo Adicional, son los gobiernos los responsables de proteger a la sociedad y a las personas

contra la delincuencia no sólo respecto de los delitos tradicionales sino también sobre aquello que sucede cibernéticamente, siendo conscientes que cada vez más las pruebas de los delitos se almacenan en forma electrónica en sistemas informáticos incluso en jurisdicciones extranjeras, múltiples o desconocidas.

Para apoyar esta idea, como no invocar las Recomendaciones del 12 de septiembre de 2017 de la Comisión Europea a los Estados miembros para mejorar la ciberseguridad en la Unión (), como consecuencia de los ataques terroristas ocurridos recientemente facilitados por las nuevas tecnologías, en donde se pone especial énfasis en la cooperación entre los Estados, entre ellas, la que señala que el Marco de respuesta a la crisis de ciberseguridad de la UE debe identificar en especial a los agentes, instituciones de la UE y autoridades de los Estados miembros que sean pertinentes, a todos los niveles necesarios (técnico, operativo y estratégico político) y elaborar, en caso necesario, procedimientos de trabajo normalizados que definan cómo han de colaborar en el contexto de los mecanismos de gestión de crisis de la UE, debiendo hacerse hincapié en permitir el intercambio de información, sin demoras indebidas, y en coordinar la respuesta durante incidentes y crisis de ciberseguridad a gran escala.

Entonces, si el principal problema del modelo de derecho penal transnacional, común a todo el derecho internacional público, se encuentra en el hecho de que su eficacia depende en gran medida de la voluntad soberana de los Estados, ha llegado el momento de ejercer una voluntad firme porque la comunidad internacional está alertando que ya no hay tiempo para dilaciones en la lucha contra la ciberdelincuencia.

REFERENCIAS

1. SERGIO ROMEO MALANDA; "*Un nuevo modelo de Derecho penal transnacional: el Derecho penal de la Unión Europea tras el Tratado de Lisboa*"; Estudios Penales y Criminológicos, Vol. XXXII (2012), ISSN 1137-7557:313-386 - Universidad de Las Palmas de Gran Canaria; publicado en Google académico el 19/7/2022.

2. PEDRO PIEDRAHITA-BUSTAMANTE; *"Local y global: el Estado frente al delito transnacional*", Revista Derecho del Estado n° 46, Bogotá, Colombia, 2020, págs. 137-160, Versión Impresa ISSN 0122, 9893, publicada en scielo.org.co el 19/7/2022.

3. ANA ISABEL CEPEDA; "*¿Existe un Sistema Penal Transnacional?" publicado en "Globalización, Delincuencia organizada, Expansionismo Penal y Económico en el Siglo XXI - Libro Homenaje al Dr. Juan María Terradillos Basoco*"; Cuba; Editorial UNIJURIS (Unión de Juristas Cuba); Junio del 2015; Recuperado de Google Académico el 19 de julio de 2022.

4. COMISIÓN EUROPEA, Estrasburgo,17.4.2018, COM (2018) 225 final, 2018/0108(COD); publicado en https://ec.europea.eu el 23/7/2022.

5. DÍAZ GÓMEZ, A.; "*El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest*", *REDUR* 8, diciembre 2010, págs. 169-203. ISSN 1695-078X; publicado en https://scholar.google.es

6. ROBERTO HERNÁNDEZ SAMPIERI, "Metodología de la Investigación", Ed. Mc Graw Hill Education/ Interamericana Editores S.A. del C.V., Méjico DF, 6ta Edición, publicado en https://www.uca.ar.cr el 20 de octubre de 2022.

7. Ley N° 25.362 de aprobación de la Convención Internacional Contra la Delincuencia Organizada Transnacional (B.O. 29 de agosto de 2002)"; InfoLEG Información Legislativa Ministerio de Justicia y Derechos Humanos Presidencia de la Nación; recuperado el 1/5/2022, de http://servicios.infoleg.gob.ar

8. INFORME EXPLICATIVO DEL CONVENIO SOBRE LA CIBERDELINCUENCIA - Consejo de Europa, publicado en https://rm.coe.int el 7 de junio de 2022.

9. FEDERICO BUENO DE MATA, "*La transformación digital de la cooperación jurídica penal internacional*" – Dirección: Leticia Fontestad Portalés, 2021, Thomson Reuters, publicado en google académico el 1° de julio de 2022.

10. DIRECCIÓN GENERAL DE COOPERACIÓN REGIONAL E INTERNACIONAL (DIGCR); "*Guía de Cooperación Penal Internacional del MPF de la Nación"*; publicado en https://www.mpf.gob.ar el 29 de mayo de 2022.

11. DIRECCIÓN GENERAL DE COOPREACIÓN REGIONAL E INTERNACIONAL DEL MPF DE LA NACIÓN; "*Equipos conjuntos de Investigación - Estrategias de Trabajo Articulado para Investigar y Perseguir el Crimen Organizado*"; publicado en https://www.mpf.gob.ar el 31 de mayo de 2022.

12. ASOCIACIÓN IBEROAMERICANA DE MINISTERIOS PÚBLICOS - AIAMP, "Página oficial - ¿Quiénes Somos?"; recuperado de https://www.aiamp.info el día 29 de mayo de 2022.

13. RED IBEROAMERICANA DE MINISTERIOS PÚBLICOS ESPECIALIZADOS EN CIBERDELITO - CiberRed; recuperado de https://www.aiamp.info, el 1 de junio de 2022.

14. COMITÉ DEL CONVENIIO SOBRE LA CIBERDELINCUENCIA (T-CY); "*Segundo Protocolo adicional al Convenio sobre Ciberdelincuencia, relativo al refuerzo de la cooperación y de la divulgación de las pruebas electrónicas*"; Versión 2 del 12 de abril de 2021; publicado en www.coe.int/cybercrime el 23 de marzo de 2022.

15. PORTAL DE NOTICIAS DEL CONSEJO DE EUROPA; "*Mejora en la cooperación y la divulgación de pruebas electrónicas: 22 países firman el nuevo Protocolo al Convenio sobre Ciberdelincuencia*"; 12 de mayo de 2022; publicado en https://www.coe.int, el 25 de mayo de 2022.

16. INTERPOL. "*Intercambio de Información a nivel mundial*"; Página oficial INTERPOL; Recuperado el 29 de mayo de 2022 de "GI-04_Databases_Factsheets_ES_2020-03.pdf".

17. Nota publicada en el periódico "Página 12" online "Cómo se descubre la distribución de pornografía infantil en internet | Las investigaciones internacionales que detectan los intercambios y entre quiénes suceden | Página12 (pagina12.com.ar)", publicado el 11 de junio de 2022.

18. Hogar (missingkids.org); "*Las investigaciones internacionales que detectan los intercambios y entre quiénes suceden. Cómo se descubre la distribución de pornografía infantil en internet*" - 31/6/2019; publicado el 11 de junio de 2022.

19. ANGUITA OSUNA, JOSÉ ENRIQUE; "Análisis histórico – jurídico de la lucha contra la ciberdelincuencia de la Unión Europea", 2017, recuperado de https://scholar.google.es

BIBLIOGRAFÍA

SAIN, GUSTAVO; "*Evolución histórica de los delitos informáticos*"; recuperado el 4/4/2021 de http://www.pensamientopenal.com.ar.

SAIN, GUSTAVO; "*Cibercrimen y Delitos Informáticos Suplemento Especial*"; Ed. Erreius; 2018; recuperado de http://www.pensamientopenal.com.ar

SAIN, GUSTAVO Y AZZOLIN, H.; "*Delitos informáticos: investigación criminal, marco legal y peritaje*"; Ed. BdF; 2017; Buenos Aires Argentina.

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DE LA NACIÓN, "Una aproximación a la estadística criminal sobre delitos informáticos"; 2016; CABA – Argentina; recuperado de https://docplayer.es/33190704-Una-aproximacion-a-la-estadistica-criminal-sobre-delitos-informaticos-primer-muestreo-de-denuncias-judiciales-de-la-republica-argentina.html

CONSEJO DE EUROPA, "*Guía de prueba Electrónica - Guía básica para Fuerzas y Cuerpos de Seguridad, Jueces y Fiscales*" - Version 1.0. - CyberCrime@IPA EU/COE Joint Project on Regional Cooperation against Cybercrime; recuperado de https://www.coe.int el 10/6/2022.

CASTELLS, MANUEL, "*La era de la información – Prólogo: La red y yo*"; Revista Economía, sociedad y cultura – Vol. 1; México; 1996.

MANSILLA Y MEJÍA, MARÍA ELENA; "*Temas de Derecho Internacional*"; 1ra. edición; septiembre de 2006, Secretaría de Gobernación - Dirección General de Compilación y Consulta del Orden Jurídico Nacional, recuperado el 25/5/22 de http://www.gobernacion.gob.mx, http://www.ordenjuridico.gob.mx

RASKIN, PAUL D.; "*Un Cambio en el Sistema: El Viraje hacia la Sostenibilidad", publicado en "BBVA - Hay Futuro. Visiones para Un Mundo Mejor"*; España; TF Editores; 2012; recuperado el 13/11/21 de https://www.bbvaopenmind.com/wp-content/uploads/2013/01/BBVA-OpenMind-Libro-Hay-futuro_visiones-para-un-mundo-mejor

Al-RODHAN, NAYEF; "*El futuro de las relaciones internacionales: una teoría del realismo simbiótico*" - Hay Futuro Visiones para un Mundo Mejor BBVV Francés; recuperado el 13/11/2021 de https://www.bbvaopenmind.com/wp-content/uploads/2013/01/BBVA-OpenMind-Libro-Hay-futuro_visiones-para-un-mundo-mejor