Revista Digital de Ciencias Penales de Costa Rica, número 1 (32) (13) . Homenaje al Prof. Dr. Daniel González Álvarez. Año 1. ISSN **pendiente**. RDCP-UCR. 2021.
https://revistas.ucr.ac.cr/index.php/RDMCP

UNA POLÍTICA CRIMINAL INFORMÁTICA PARA AMÉRICA LATINA

AN INFORMATION TECHNOLOGY CRIMINAL POLICY FOR LATIN AMERICA

Prof. Dr. Alfredo Chirino Sánchez[1]

1. Introducción

Desde la primera comunicación enviada a través Internet en 1969, se ha producido un descomunal desarrollo de las tecnologías que han permitido el aumento, la diversificación y velocidad del tráfico de datos en el mundo. Apenas la descripción de los cambios tecnológicos que se han producido en la última parte del siglo XX y las primeras dos décadas del siglo XXI, alcanzarían para dar una idea del tamaño y profundidad de las transformaciones económicas, sociales y políticas que la presente Era de la Información ha permitido.

Las bases tecnológicas que dieron lugar a la "red de redes" (World Wide Web), entre ellas, los protocolos TCP/IP[2], el lenguaje HTML, los buscadores de información, los correos electrónicos, pero después las redes sociales, el uso de redes neuronales cada vez más complejas, el almacenamiento de información en la nube, la WEB 2.0 y la promesa de que la Internet no olvidará, las Wikis o bibliotecas públicas, el Internet de las Cosas, los "*blockchains*", han sido posibles gracias a la articulación de los esfuerzos, hasta ahora descentralizados y arbitrarios, que promovieron todo este progreso a pasos agigantados. Aun cuando enfrentamos una pandemia[3]

[1] Decano y Catedrático de Derecho Penal. Facultad de Derecho. Universidad de Costa Rica.

[2] En los años setenta del siglo pasado se sentaron las bases para el "Transmission Control Protocol" y el "Internet Protocol" (TCP/IP) que permitieron la intercomunicación entre diversos tipos de computadores, independientemente de sus características, tamaño, marcas o sistemas operativos. Con ello se alcanzaría la garantía para el intercambio de datos a un nivel antes desconocido. Desarrollos posteriores, como la amplia distribución y comercialización de los computadores del hogar y en el trabajo en los años ochenta, y, después, las "laptop" hacia finales de esa década y los años noventa, sentarían las bases para que el uso de ordenadores se integrara en la cultura general, preparando el camino para el uso cada vez más intensivo de la Internet y sus diversos servicios. fuera popularizados tanto en el trabajo como la Internet y sus servicios se hicieran materia común, de tal manera que se integrarían en los servicios disponibles en todo computador comercializado Cfr. Schwarzenegger, Christian, "Die Internationalisierung des Wirtschaftsstrafrechts und die schweizerische Kriminalpolitik: Cyberkriminalität und das neue Urheberstrafrecht", en: ZSR 2008 II, p. 405, disponible en: https://www.ius.uzh.ch/dam/jcr:00000000-5624-ccd2-0000-00003bba68ae/ZSRII2008BeitragSchwarzenegger.pdf

[3] Este artículo se ha terminado de escribir en el mes de noviembre de 2020, cuando han transcurrido nueve meses de diversas etapas de confinamiento producto de las medidas sanitarias para atender la pandemia provocada por la enfermedad del COVID-19. Se ha observado a lo largo de este largo periodo un papel trascendental de las

de alcances mundiales, con efectos económicos, sociales y políticos de incalculables proporciones, y que ha obligado a las personas a adaptarse a nuevas formas de comunicación y de interacción social, más de 1100 millones de usuarios[4] y cerca de 63 millones de páginas en línea, acompañan a una humanidad en confinamiento. Justo en esta coyuntura histórica tan delicada, la inversión en computación periférica (*edge computing*), inteligencia artificial y en la tecnología de *blockchain*[5] está atisbando las nuevas etapas de la evolución de la Internet, que aseguran escenarios de mayor velocidad de acceso, de más confiabilidad en las interacciones y en la generación de los contextos para la revolución industrial 4.0 que promete, ya, transformaciones revolucionarias en el mundo del trabajo. La velocidad de los cambios responde a la así denominada "Ley de Moore", la cual establece que el número de transistores por unidad de superficie se duplica cada 18 meses, y que se ha mantenido en su velocidad inalterable en las últimas décadas, parece indicar que los cambios y transformaciones del ambiente de la información seguirán intensificándose de la mano de cada vez más pequeños aparatos de

tecnologías de la comunicación y de la información, cuyo uso e incidencia en la vida cotidiana solo se ha fortalecido. La distancia entre trabajo, vida familiar y ocio se ha trastocado con la llegada abrupta del teletrabajo. De la misma manera, se han disparado los delitos cibernéticos al tener tantas personas conectadas por más tiempo, e interactuando virtualmente de una manera mucho más intensa que antes. Dicho papel de las tecnologías en tiempos de la pandemia requiere, por supuesto, un análisis más detallado, que no es posible hacer en este momento, sin embargo, algunas de sus consecuencias pueden ser estudiadas en el reciente trabajo del joven filósofo croata Srećko Horvat, discípulo de Žižek, cuyo título "Poesía del Futuro" es suficientemente sugestiva (Paidós, 2020).

[4] Solo en comparación, para 1995 se consideraba que había 53 millones de usuarios de Internet y se proyectaba para el año 2000 un número aproximado de 250 millones. Cfr. Stegbauer, Christian, Euphorie und Ernüchterung auf der Datenautobahn, Frankfurt am Main, dipa-Verlag, 1996, p. 19.

[5] Por su denominación en inglés, y en su forma más conocida, la "cadena de bloques" o "blockchain" hace alusión, en la mayoría de los casos, a las criptomonedas, pero su uso es mucho más amplio, sobre todo en servicios de Internet de las Cosas (IoT) y en algunas aplicaciones para instituciones financieras donde la seguridad criptográfica es especialmente necesaria. El blockchain es, en realidad, un registro único que es consensuado y distribuido en varios nodos en la red. Para las criptomonedas, el blockchain sería como el libro de registro contable donde se asientan las diversas transacciones. Los bloques contienen así, una cantidad de registros o transacciones válidas, información referente a es bloque, y, por supuesto, información sobre el vínculo con el bloque anterior y el bloque siguiente a través de un "hash" de cada bloque, que a su vez no es más que un código único que sería como la huella de trazabilidad digital de ese bloque. Con esa vinculación de códigos es que es posible que no se pierda la trazabilidad de esos bloques y la pertenencia de unos a otros, y todos los participantes de la red conservan una copia exacta del bloque. Conforme se realizan nuevos registros, el sistema verifica la validez y son validados también por los nodos de la red y se añade al nuevo bloque que se enlaza, entonces, a la cadena. Lo anterior, garantiza la disponibilidad de la información en todo momento y la seguridad, pues cualquiera de los nodos de la red, si está activo, contiene la información necesaria para recuperar el historial de los bloques. Esto último tiene una especial importancia, pues si un ciberdelincuente quiere atacar la infraestructura del blockchain tendría que atacar los nodos y modificar la cadena, para que la información sea dañada. La garantía de seguridad es tan grande, que se ha pensado su uso para brindar seguridad en el proceso probatorio civil, por ejemplo, cfr., con más detalles: Melo, Letícia, "Régimen Jurídico de Blockchain: una prueba atípica", en: Revista Bioética y Derecho, Barcelona, No. 46, 2019, disponible en: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872019000200007

procesamiento y el abaratamiento de las tecnologías disponibles[6]. El futuro parece descansar en dispositivos cada vez más pequeños, donde la nanotecnología y los sistemas "incrustados" ("*embedded systems*") prometen aun más incidencia de la interconexión permanente y ubicua, y, por ende, a más posibilidades de lesión a la privacidad y a la autodeterminación informativa.

En esta "nueva normalidad" medra un conjunto muy importante de fenómenos constituido por acciones delictivas de alcance nacional y global que ponen en peligro muchas de las conquistas que esta revolución informativa ha originado. Se trata de una criminalidad con características muy específicas, que ha evolucionado de meros delitos cuyo objeto material es el computador mismo (delitos por computadoras o delitos informáticos), a hechos criminales que ahora utilizan las facilidades de interconexión facilitadas por Internet: los ciberdelitos[7].

La arquitectura de los sistemas informáticos, basada en un control centralizado, es la parte más débil de la cadena, pues puede ser objeto de ataques de la ciberdelincuencia. Es aquí, entonces, donde resulta imprescindible comprender no sólo el contexto tecnológico en que se ha desarrolla el actual ambiente de la información mundial, sino también los riesgos y peligros implícitos a su estructura, arquitectura y forma de uso.

Conceptos tales como "ciberseguridad", "ciberespacio", contacto "virtual", redes sociales, son determinantes para comprender el espectro de problemas que focalizarán las decisiones de los Estados a la hora de enfrentar manifestaciones de una criminalidad al mismo tiempo sutil y poderosa. Los escenarios criminales en los que se desenvolverá esta criminalidad, requieren un análisis del legislador, para que, junto a la complejidad casuística de este fenómeno, los conceptos normativos utilizados tengan algún acercamiento técnico a los precisos conceptos involucrados en estas tecnologías. No se trata simplemente de la suplantación de identidades en redes sociales y en transacciones bancarias, o la propagación de virus y otras formas de malware en la Web, o de la pornografía infantil o de mecanismos articulados a través de criptomonedas para el financiamiento del terrorismo, sino que estamos hablando de todo un conjunto de nuevas acciones que ponen en peligro la integridad de los sistemas informáticos a nivel nacional e

[6] Cfr. Hansen, Markus & Fabian, Benjamin & Möller, Jan & Spiekermann, Sarah. (2006). Szenarien des Ubiquitous Computing, disponible en https://www.researchgate.net/publication/262563325 p.15.
[7] Barrio Andrés, Moisés, Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos, Madrid, Wolter Kluwer, 2018, pp. 33-37. Con detalles a los desarrollos en Alemania, cfr. Wassmer, Martin Paul, "Delitos Informáticos (Cybercrimes)", en: Revista Penal, No. 40, julio 2017, Valencia, Tirant Lo Blanch, pp. 250.

internacional, así como también afectan la seguridad económica y social de los países.

2. El ciberespacio y la ciberseguridad como modeladores de las condiciones en la política criminal

Desde que el autor de ciencia-ficción, William Gibson, acuñó el término "ciberespacio" muchas cosas han sucedido desde la perspectiva tecnológica. La idea de un espacio virtual donde podrían suceder cosas que afectarían la realidad de sus personajes, en 1984 aun no era posible. Sin embargo, en las décadas subsiguientes se generarían importantes cambios tecnológicos que serían el epítome de lo que Gibson buscaba al describir ese concepto del "ciberespacio". La gran cantidad de conexiones a la Internet, la convivencia cotidiana con servicios de toda índole: compras, comunicaciones, envíos de dinero, imágenes, comparaciones de datos en cantidades simplemente inconmensurables. Baste pensar que para el año 1996 había 500 mil servidores en servicio en todo el mundo, con 30 millones de páginas disponibles y con casi 75 millones de usuarios. Para el año 2019, se estimaba que el número de usuarios de Internet llegaba a 4.021 millones, es decir, el 53% de la población mundial. En otras palabras, más de la mitad de la población del mundo está presente en la "Red de Redes", interactuando de mil maneras, y provocando una cantidad de información que es casi imposible de poner en números: según estimaciones de Eric Schmidt[8], CEO de Google, hasta 2003 la humanidad había generado cinco exabytes de información a lo largo de toda su historia, comenzando desde los albores de la civilización. Ya para el año 2007, se había generado 281 exabytes, según las investigadoras Hardy y Williams[9], y apenas cuatro años más tarde alcanzamos los 1.800 exabytes (un exabyte equivale a 10^{18} bytes). En esa cantidad monstruosa de datos hay tuits, mensajes de correo, videos, películas, memes, llamadas telefónicas, fotografías, canciones. Hoy la producción de información puede estimarse en más de 5 exabytes al día, es decir toda la información que había sido producida solo en el año 2003, y la cuenta sigue creciendo. La

[8] Este impresionante dato lo dio Schmidt durante su alocución en la conferencia "Techonomy" en el Lago Tahoe, en los Estados Unidos, en agosto de 2010. La afirmación que hizo fue mucho más radical: "*From the dawn of civilization to 2003, five exabytes of data were created. The same amount was created in the last two days*." En ello va implícita, por supuesto, toda la información que es generada por los usuarios, lo que involucra fotografías, mensajes instantáneos y tweets, entre otros datos. La pregunta que ello conlleva, es que las compañías como Google pueden lidiar con tales dimensiones de datos haciendo con ellos múltiples operaciones y comparaciones, manteniendo algoritmos de búsqueda que le dan sentido, pero se pregunta el señor Schmidt, ¿deberían estas compañías estar facultadas para ello? Cfr. https://www.huffpost.com/entry/google-ceo-eric-schmidt-p_n_671513

[9] https://www.htcnexus.com/cuanta-informacion-se-genera-al-ano-en-el-mundo/

expansión de Internet ha excedido hasta las predicciones más generosas de los expertos, y ha arrojado un enorme interés de los ciberdelincuentes que encuentran en ella todas las condiciones para expandir sus actividades criminales alrededor del globo terráqueo. Desde la revisión de los datos financieros y bancarios que viajan hoy libremente en los paquetes de datos de Internet, hasta la revisión e interceptación de información privilegiada (propiedad intelectual, secretos industriales, música y videos protegidos, etc.), son de las acciones criminales más temidas en la Web, junto a la suplantación de identidad, y la distribución indiscriminada de virus y amenazas de malware.

Es por todo esto que resulta indispensable que en la reconstrucción de la política criminal se ponga un especial énfasis en el estudio y comprensión de las estructuras tecnológicas que han hecho posible este panorama de la información, con explicaciones que conecten estos desarrollos con las condiciones que han sido clave para que Internet sea el escenario para una criminalidad sofisticada, técnicamente compleja y con tentáculos y expansión en todo el mundo.

3. La ciberdelincuencia como criminalidad organizada

Los ciberdelitos han evolucionado de conductas individuales cometidas por personas aisladas y con grandes conocimientos técnicos, a conductas que se inscriben dentro de las formas de comisión organizada. Se trata de una maduración de los afanes humanos tradicionales de obtener riqueza e influencia por medios ilícitos, ahora acompañados de los pasos agigantados que las tecnologías de la comunicación y de la información han dado en las últimas décadas, y de la apertura económica que la mundialización ha permitido. El interés de los ciberdelincuentes se ha movido del ataque a los sistemas informáticos como tales, con el fin de causar daños o imponerse de data útil, para ahora utilizarlos como medio para asegurar los resultados económicos de sus emprendimientos. Sus acciones son ahora de gran envergadura, y no dudan en utilizar las diversas posibilidades técnicas disponibles para ocultar u obtener las ganancias de sus hechos criminales. En una Internet de las Cosas, donde multitud de objetos, máquinas y otros elementos de nuestra vida cotidiana se comunican entre sí, los cibercriminales ven la oportunidad para hacer más multifacéticas sus propuestas delictuosas, y esa es un área donde es esperable aun nuevos fenómenos delictivos.

Dentro de estos cambios del comportamiento criminal en el ciberespacio se manifiesta,

especialmente, el surgimiento de organizaciones criminales que cometen este tipo de conductas. Se trata de organizaciones integradas por personas jóvenes. En un estudio del año 2013, conducido por las Naciones Unidas (Estudio Comprensivo sobre Ciberdelincuencia), se logró determinar que el 60% de todos los usuarios de Internet se encuentran en los países en desarrollo y con un 45% de todos lo usuarios con un rango de edad inferior a los 25 años. Este dato de la edad es importante, porque refleja que muchas de las organizaciones criminales dedicadas a la delincuencia informática están conformadas por subculturas de personas jóvenes, nacidas en tiempos de avances tecnológicos vertiginosos y acostumbrados a interactuar en diversos ambientes donde la tecnología tiene un papel esencial. Se ha logrado identificar, al menos en los Estados Unidos, grupos concretos provenientes de células criminales rusas que se trasladaron a los Estados Unidos luego de la caída de la Unión Soviética, agrupaciones provenientes de países africanos que se han concentrado, primariamente, en delitos con esquemas financieros y tráfico de estupefacientes, así como grupos pertenecientes a grupos criminales asiáticos (Yakuza japonesa, Tongs chinos y otros grupos), así como sociedades criminales que operan en Rumania, Hungría y otros países del Este europeo. El estudio de tendencia demuestra que estos grupos han empezado a colaborar entre sí, lo que cambia definitivamente el perfil tradicional del delincuente informático. La potencialización de la ciberdelincuencia mediante el uso de los instrumentos de la organización criminal, ha llevado a nuevos niveles de complejidad la investigación y persecución de los cibercriminales.

Como lo describió el ya fallecido (1925-2017) y afamado sociólogo Zygmunt Bauman, habita en nuestro mundo una élite global, que no depende de la soberanía de los Estados ortodoxos, controlados por alambradas y puestos de migración, y que opera de manera transnacional, y transestatal (Bauman, La sociedad sitiada, 2007), en una palabra, lo hace en el ciberespacio, donde despliega una activa vida económica y social, con posibilidades infinitas como bien lo percibía Giovanni Sartori, "…para bien y para mal" (Homo Videns, 2012). No en vano el Prefacio a la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional apunta, en palabras de Kofi Annan, a que la criminalidad no ha perdido el tiempo, echando mano a las ventajas de una economía mundializada y a la tecnología sofisticada que la acompaña. En una palabra, el crimen organizado utiliza desde hace bastante tiempo todos los avances tecnológicos que han permitido la sociedad altamente virtual que hemos ido

construyendo.

El crimen organizado apertrechado tecnológicamente ha incursionado en la World Wide Web para involucrarse en el fraude informático y en atentados varios contra la banca electrónica, principalmente, pero introduciendo nuevas formas de afectación a bienes jurídicos en la forma de terrorismo cibernético, financiamiento de grupos yihadistas, pornografía infantil y explotación sexual, tráfico de personas y órganos, y una singular variedad de nuevos hechos que afectan a todos los países. Se calcula el impacto económico de estos cibergrupos en cifras que van de un trillón de dólares hasta cálculos conservadores en 12.5 billones de dólares (cfr. FBI, Organized crime Overview). Estos inmensos daños son facilitados por diversos factores, algunos dependientes de la fragilidad de las redes y de su arquitectura de software, y en otros casos gravemente influenciados por la ingenuidad de los propios usuarios de los servicios bancarios y financieros en red. El comercio electrónico, en especial, se ha convertido al mismo tiempo en la piedra del toque para un despertar económico global y también en la puerta de acceso para estas nuevas conductas delictivas en la "Red de Redes", y propone dificultades asombrosas para el combate de estas organizaciones ilícitas. Es, por lo tanto, indispensable, que los legisladores regionales tengan claridad de estas nuevas formas de interacción grupal de las organizaciones delictivas, que echan mano de los beneficios tecnológicos de la Internet, para vender información, facilitar el ciberespionaje, provocar caídas de redes informáticas, y hacerse con vital información financiera de los internautas. Es así que habrá que estudiar a los grupos que hacen el "*phishing"*, mediante spam, correos engañosos, así como en la réplica o construcción de páginas Web falsas, pero también como estos interactúan con los así denominados "cibermulas", que se encargan de entrar a las cuentas y obtener el dinero, luego lo transmiten por canales seguros a otras organizaciones criminales que a su vez lo utilizan con diversos fines y para financiar ulteriores actividades criminales. Estas operaciones, muchas veces deslocalizadas y en diversos momentos, se realizan por grupos muy diversos, lo que dificulta su seguimiento y la comprensión de su papel en una actividad criminal en fases y en diversos territorios. Comprender estas interacciones, los fines globales que se persiguen, como esta metodología incide en la aplicación de la ley penal y procesal, permitirá a los legisladores la construcción de una política criminal adecuada a las circunstancias en las que se mueve la ciberdelincuencia.

4. Delitos informáticos vs. Ciberdelincuencia: La necesaria evolución del derecho penal cibernético

Ha habido un tránsito importante desde la antigua delincuencia informática, principalmente orientada a los sistemas informáticos y el computador y sus periféricos, a una delincuencia apertrechada tecnológicamente, que ha expandido la capacidad de los infractores, y ha confrontado a la sociedad con diversos problemas que van directamente unidos a condiciones que han hecho posible el avance de la humanidad en diversos ámbitos. La tecnología ha creado medios inusitadamente poderosos para ampliar la acción de los delitos más allá de los territorios de los Estados Nacionales, convirtiendo a los cibercriminales en actores de un nuevo escenario global. La sociedad actual se ha hecho dependiente de los recursos tecnológicos para hacer posible su comercio, el intercambio de conocimiento, el desarrollo de la educación, para crear nuevas conexiones sociales y de comunicación y para asegurar un "valiente nuevo mundo", lleno de fragilidades en su seguridad y en la consistencia de sus contactos.

Los delitos de la primera etapa de la evolución de la criminalidad informática, construidos a partir de los tipos penales tradicionales contra la propiedad y el patrimonio, han empezado a evolucionar de maneras absolutamente inimaginables hace apenas unas décadas, integrándose con el estado de la técnica, y la creciente organización de los grupos que los cometen. Como resultado de ello, la empresa criminal informática propone nuevos retos al derecho penal que este apenas empieza a entender, precisamente cuando ya hay condiciones tecnológicas que abren puertas a adelantos aún más difíciles de adecuar a las nuevas prescripciones penales.

Un acercamiento político-criminal implicará, así las cosas, analizar tanto los tradicionales delitos informáticos, así como la moderna ciberdelincuencia, para ver los puntos de conexión, comprender los tránsitos metodológicos entre unos y otros, los particulares adelantos tecnológicos que los han promovido y, por supuesto, la forma en que la legislación penal nacional e internacional los ha ido incorporando dentro del corpus iuris del derecho penal. Ejemplificativos de esas tendencias lo son, por supuesto, el fraude y la estafa informática, pero también el sabotaje informático, pero también los virus, el malware, la pornografía infantil en Internet, y la suplantación de identidad.

Con el estudio de estas figuras penales será posible comprender los diversos factores que han promovido el movimiento internacional[10] hacia un derecho penal intercultural en la materia, provocar un interés de los legisladores en el estudio de la visión corporativa de estos hechos criminosos, y establecer con claridad las tendencias de la moderna ciberdelincuencia en el estado actual de la técnica.

Conforme el advenimiento de la Edad de la Información somete a las sociedades occidentales y las marca con su signo tecnológico, es indudable que el computador como punto de entronque para todo tipo de actividad humana, ha transformado nuestra vivencia con la tecnología, haciéndola omnipresente, y al ser humano un esclavo de sus designios y posibilidades. América Latina no ha sido una excepción en ese desarrollo, con una impresionante penetración celular, que hace que la mayor parte de conexiones a Internet se realicen desde dispositivos telefónicos. El ancho de banda telefónico de acceso a Internet se ha incrementado exponencialmente, y los dispositivos que le permiten ese acceso a la tecnología son cada vez más rápidos, más sofisticados y disponen de memorias cada vez más grandes. Al mismo tiempo que se abarata el acceso y la memoria disponible en los aparatos, se multiplican los servicios de pago, de comercio electrónico, de obtención de información en línea y, por supuesto, de uso y abuso de todo tipo servicios de entretenimiento en línea, siendo especialmente prometedores los servicios de televisión, música y transporte, para citar los más trascendentes en el espacio informativo de la región. Este enorme cambio en las costumbres de consumo del ha motivado nuevas conductas criminales de suplantación de identidad, que le han permitido a delincuentes informáticos obtener pingües ganancias.

Con el fin de examinar estos cambios en el paisaje de la criminalidad, y la capacidad de imputación que la legislación regional permite, resulta esencial pasar revista a los delitos recientemente incorporados en la legislación, y examinar su capacidad de rendimiento frente a fenómenos tales como la criminalidad corporativa, económica, el lavado de dinero, el uso de criptomonedas y otras acciones dañosas, examen que no podemos realizar con detalle en este

[10] Sieber plantea, con razón, la necesidad de un eficaz derecho penal "transnacional", pues los retos más claros de esta criminalidad están asentados en su extraterritorialidad. Por ello, habría que integrar instrumentos legales que permitan la implementación de investigaciones con efectos extraterritoriales desde el propio derecho penal nacional y, además, de investigaciones que puedan ser realizadas ya propiamente en el ciberespacio. Cfr. Sieber, Ulrich, Straftaten und Strafverfolgung im Internet, Gutachten C zum 69. Deutschen Juristentag, C.H. Beck, München, 2012, p. 139.

momento.

Como podrá fácilmente comprenderse, resulta fundamental pasar cumplida revista a la forma en que el legislador ha incorporado en la legislación penal todas las acciones que hoy día tienen tantas repercusiones en las oportunidades de desarrollo individual y social, así como para el futuro económico de los países. El legislador debe estar en la capacidad de conocer la completa variedad de figuras existentes, su orientación punitiva, sus fuentes de política criminal, sus elementos y dependencias tecnológicas y, por supuesto, las eventuales dificultades que ofrecen para ser aplicados en contextos donde las exigencias de un panorama tecnológico en constante transformación, retan a los aplicadores de justicia a cada instante.

5. La Convención de Budapest como una forma de construcción de un derecho penal intercultural en materia de ciberdelincuencia.

Uno de los retos más importantes propuesto por el carácter global de la ciberdelincuencia lo constituye, sin duda alguna, la persecución internacional de estos hechos delictivos. En la investigación de este tipo de delincuencia resulta fundamental una vigorosa cooperación internacional en materia penal, no sólo para aunar esfuerzos nacionales para obtener prueba, realizar seguimientos de personas y grupos conectados con la actividad organizada, sino también para otorgar capacidad suficiente a los diversos intervinientes en la investigación para superar obstáculos como las diferencias legislativas, las diversas jurisdicciones y criterios de intervención, así como también las siempre presentes diferencias y muy limitadas capacidades tecnológicas de los órganos del control penal para dar una adecuada atención a los diversos métodos y herramientas de comisión de los hechos delictivos de ciberdelincuencia[11]. La duplicación de esfuerzos en jurisdicciones que se yuxtaponen y se intersecan en la investigación es uno de los problemas más complejos que deben atenderse a la hora de emprender una intervención global en acciones que han sido pensadas, precisamente, para aprovechar las dificultades que tienen los países para lograr un efectivo y eficaz trabajo mancomunado. La información clave para asegurar el éxito de una investigación puede ser trasladada de manera transfronteriza aprovechando las interconexiones y redes que estos grupos tienen, así como también por las facilidades que la misma Internet ofrece de almacenamientos masivos en la

[11] Sieber, op. cit., p. 139.

"nube", así como la ubicuidad del procesamiento de datos en computadores remotos que tienen toda o parcialmente la información que serviría para asegurar un golpe a estos grupos. Las autoridades del control penal podrían encontrarse que necesitan cooperación en un país donde esa conducta que investigan, en concreto, no ha sido incorporada como un delito, o no tiene las connotaciones de gravedad que permitirían, por ejemplo, dictar medidas precautorias o decisiones de intervención policial técnica[12]. Adicionalmente a ello, la anonimidad garantizada por la propia Internet, pero también por la utilización de diversas herramientas de software, les permite a estos delincuentes actuar con cierta impunidad tanto en el nivel nacional como internacional.

De cara a los problemas de la ciberdelincuencia, su conexión abierta a las disponibilidades de una economía global y la no poco frecuente dificultad de cooperación internacional, se ha venido produciendo una importante actividad internacional de construcción de una normativa internacional. Quizá el antecedente más relevante es el así denominado Convenio sobre la Ciberdelincuencia conocido como "Convenio de Budapest" del Consejo de Europa de 2001. Este texto se ha convertido, al mismo tiempo, en guía legislativa o "ley modelo" para la comunidad internacional y también en un "acuerdo marco" que orienta las acciones en el contexto de las normativas nacionales. Al encontrarse abierto a la suscripción de Estados que no pertenecen al Consejo de Europa, ha ido permitiendo, poco a poco, una armonización normativa, al menos en lo que se refiere a la descripción de los tipos penales, aun cuando, en muchos casos, las diferencias y déficits en otras materias, como las garantías penales y la protección de derechos humanos siguen siendo un óbice importante para una acción concertada y equilibrada entre las diferentes naciones. El Convenio de Budapest busca, en primera instancia, la incorporación en la normativa interna de una serie de figuras penales y, en segundo lugar, la dotación a las autoridades penales de facultades e instrumentos procesales que habiliten una investigación efectiva de estos hechos, tanto en el área de acumulación de inteligencia como en la vigilancia constante, decomiso e incautación de equipos e instrumentos de comisión, monitoreo de actividades en línea, intervención de comunicaciones, transferencia de datos, entre otras. Aun cuando el listado de delitos corresponde a una época de desarrollo

[12] Hilgendorf, Eric; Frank, Thomas; Valerius, Brian, Computer- und Internetsstrafrecht. Ein Grundriss, Berlin, Heidelberg, Springer Verlag, 2005, Nm. 65 y 66, p. 19.

tecnológico relativamente viejo (2001) algunas de ellas tienen relevancia aun en la actualidad (fraude y falsificación informáticos) y otros han adquirido una perniciosa tendencia al alza en la Internet (pornografía infantil, violación a derechos de autor, delitos contra la confidencialidad y la privacidad). Desde esa perspectiva, la orientación al legislador nacional resulta pertinente y adecuada. El problema se suscita con las habilitaciones procedimentales para la investigación, vigilancia y control de las actividades tecnológicas que posibilitan esta ciberdelincuencia. Lo anterior requiere, como bien lo reconoce el artículo 15 del Convenio de Budapest, un equilibrio detallado entre las garantías del debido proceso y las facultades de investigación que se le concederán a los equipos de trabajo. Reflexiones sobre esta materia resultan fundamentales, sobre todo en una época espiritual donde tales equilibrios resultan cada vez más difíciles, por la supervivencia de un discurso antigarantista y la búsqueda de una punición a ultranza, sobre todo en los diversos poderes legislativos de la región latinoamericana, amén de actos constitutivos de delito consumados por muchos Estados, como la vigilancia de ciudadanos sin control y con abuso, lesiones al derecho a la autodeterminación informativa de poblaciones en específico, la videovigilancia en espacios privados con fines de control ideológico, entre otras posibles amenazas de los Estados contra sus ciudadanos, de los que América Latina, no escapa, y que deben ser mantenidos en la mesa de discusión y análisis. La misma acción de organismos internacionales obliga a un control cruzado de garantías en materia de la punición de la ciberdelincuencia, como sucede, por ejemplo, con la Resolución 68/17 de la ONU sobre el derecho a la privacidad en la era digital, la cual, entre otros elementos, señala la preocupación de la comunidad internacional por el equilibrio entre el uso intensivo de las tecnologías de la información y la comunicación , con la capacidad de los gobiernos y de las personas de llevara adelante actividades de vigilancia, interceptación y recopilación de datos, lo que podría conducir, en últimas, a graves transgresiones a los derechos humanos. Una punición de la ciberdelincuencia, sobre todo en sectores cercanos a la protección de datos personales, lleva a difíciles acciones y levanta suspicacias en términos de la validez de las acciones preventivas del Estado en estos delicados contextos.

En general, el proceso de incorporación de normativas internacionales en materia de ciberdelincuencia, revela importantes aspectos positivos, en especial, en materia de cooperación judicial en la investigación, la obtención de evidencia en hechos que por su naturaleza son

volátiles y dependientes de la dimensión del tiempo, que involucra un proceso penal que tiene ser ágil y eficiente. Alcanzar esta meta es un trabajo que implica conocimiento de los instrumentos internacionales, sus contenidos y sus diversos compromisos en términos de trabajo cotidiano del aparato penal.

Dadas las características del actual proceso de armonización normativa internacional, resulta muy importante para el legislador latinoamericano conocer las tendencias, movimientos, condicionantes y, en última instancia, los procesos de incorporación de normativas internacionales en el derecho nacional. Esto les pondrá en una posición ventajosa al conocer dichos movimientos, pero también comprender los compromisos normativos asumidos, y las eventuales dificultades constitucionales y legales que estos procesos incorporan. El debate sobre la temática involucra no sólo una reflexión sobre la supervivencia de principios de radical importancia para el derecho penal nacional, como el de legalidad y culpabilidad, pero también de los principios que orientan la acción legislativa como el de lesividad, estricta legalidad, *lex certa* y *lex stricta*, y el de protección de bienes jurídicos. Estos principios revelan su capital relevancia en el proceso de aplicación e implementación de los delitos que llegan a la legislación costarricense, sobre todo cuando la apertura de los Convenios Internacionales, y su vocación de respetar la soberanía legislativa de los países, puede dejar elementos de los tipos delictivos sin una adecuada precisión que a la postre puede convertir en "letra muerta" la legislación así construida. Vocablos como "acceso ilegítimo", "sistema informático", "posesión", "integridad de los datos", "uso de datos no auténticos", podrían llevar a interpretaciones de los elementos típicos que podrían resultar excesivas o abusivas, y, en general, incompatibles con un uso racional de los mecanismos de interpretación a disposición del juzgador, si no se comprende en su justa perspectiva y si no se tiene en cuenta su siempre indispensable contexto tecnológico. La política criminal está invitada, pues, a hacer un análisis de los movimientos de integración internacional, los retos normativos que ofrece, los eventuales escenarios de aplicación e interpretación, así como los eventuales compromisos en garantías que la adopción de estos instrumentos internacionales tienen para la región latinoamericana.

6. Los problemas que deben ser atendidos en una política criminal informática

Como bien lo postula Ulrich Sieber, al analizar el problema de la ciberdelincuencia para

la 69 Reunión de Juristas de 2012[13], uno de los retos más importantes de una política criminal en materia de ciberdelincuencia es la de poner su acento en la cooperación internacional, y en la implementación de regla en el derecho nacional que permitan una efectiva acción en escenarios delictivos transfronterizos[14].

Reflexionar sobre la relación entre los principios del Estado de Derecho y el derecho penal resulta, si se lo observa sin cuidado, quizá innecesaria, pues damos por sentado que la relación existe sin cuestionamiento y que la misma contribuye, en definitiva, para dar legitimidad al *ius puniendi* estatal. No obstante, esta relación no se puede dar por automática, tomando en cuenta las circunstancias por las que discurre el derecho penal en la actualidad. El derecho penal moderno, donde el derecho penal informático abreva desde sus inicios, recoge muchas de las características de aquél, principalmente la técnica legislativa de "fórmulas generales", conceptos técnicos normativos, construcciones típicas poco claras y demasiado dependientes de las coyunturas tecnológicas. Esos elementos contribuyen a hacer de la interpretación y aplicación de los tipos penales informáticos una tarea particularmente difícil y compleja, que confronta al aplicador del derecho con las antípodas del derecho penal.

Es por ello que, repensar los límites del derecho penal y de las facultades estatales de castigo en el momento presente implica, entonces, dar una segunda mirada a la necesidad de proteger la libertad en el Estado de Derecho. Establecer límites para la persecución de los delitos, para la descripción de nuevas figuras penales o para concebir nuevas relaciones de protección, es tan solo una parte de las difíciles tareas teóricas que están implícitas en el quehacer científico del penalista, pero también son una parte esencial del esfuerzo teórico y reflexivo que acompaña la tarea del legislador, sobre todo ahora frente al avance cada vez más intensivo del así denominado "derecho penal de prevención". En un derecho penal de "prevención" es evidente que estas relaciones de limitación al poder estatal caen. El objetivo, a

[13] Sieber, Ulrich, Straftaten und Strafverfolgung im Internet, Gutachten C zum 69. Deutschen Juristentag, C.H. Beck, München, 2012.

[14] No descarta tampoco Sieber, que el derecho penal material se interese por completar los tipos penales de peligro abstracto agregando una característica específica del peligro para que en caso de la comisión de un hecho penal pueda tomarse en cuenta la eventualidad de realización de un resultado, lo que tendría la ventaja, según Sieber, de ampliar la cobertura del tipo penal de peligro abstracto allende las fronteras nacionales, así como eventualmente considerar especificidades de la situación legislativa internacional. La solución es, en todo caso, interesante, pues implica, de suyo, la especificación de los delitos de peligro abstracto mediante características que aludan a un específico resultado alcanzado. Cfr. Sieber, op. cit., p. 141.

diferencia del derecho penal del Estado de Derecho, es la de construir figuras penales que permitan un control de las organizaciones y de las decisiones individuales, de manera que se reduzca la complejidad de diversas decisiones, incluso de aquellas que no necesariamente implican una acción punible. Se trata de un derecho penal que echa mano del "peligro" y del "riesgo vital" de acciones, de previsiones humanas y hasta de "cálculos de oportunidad" que podría generar situaciones conflictivas. Las formas de castigo de estas anticipaciones punitivas son cada vez más rigurosas, al tiempo que las descripciones de estos riesgos y peligros se hacen cada vez más vaporosas y menos discernibles.

En el derecho penal informático hay necesidad de referenciar estos problemas, y abarcarlos en el análisis interpretativo de las figuras penales que lo integran, pues es indudable que el derecho penal seguirá teniendo un papel en la punición de graves conductas que hagan suyo el instrumental tecnológico de las Tecnologías de la Comunicación y la Información, como también de aquellas que apertrechadas tecnológicamente provoquen daños en bienes jurídicos personales y supraindividuales en la sociedad contemporánea.

En tiempos de un "*Ubiquitous Computing*", es decir, de un ecosistema donde las interacciones con los equipos y los programas informáticos, con las redes sociales y con el procesamiento de datos en todos los niveles (en teléfonos móviles, laptops, vehículos provistos de diversos niveles de procesamiento de información, aparatos provistos con tecnología RFID, Internet de las Cosas, etc.) es cuestión cotidiana, corresponde actuar en dos niveles: por un lado, a nivel de un ambiente de ciberseguridad, donde se garantice la interacción con todos esos niveles de procesamiento con una tutela de la identidad virtual del ciudadano y con adecuada anonimidad[15].

La tendencia será útil para pasar revista a diversos problemas dogmáticos que surgen a la hora de interpretar y aplicar los diversos tipos penales vinculados a la ciberdelincuencia. Aparece como esencial, y, por supuesto, como punto de arranque la permanente discusión sobre los bienes jurídicos tutelados en la ciberdelincuencia, muy especialmente en los delitos usualmente calificados como "informáticos" por su contenido, así como también resulta

[15] Cfr. con más detalles, Hansen, Markus & Fabian, Benjamin & Möller, Jan & Spiekermann, Sarah. (2006). Szenarien des Ubiquitous Computing, disponible en https://www.researchgate.net/publication/262563325

trascendente pasar revista a los elementos que podrían arrojar alguna conclusión sobre el ente protegido en la ciberdelincuencia 2.0, posterior a los hechos punibles incorporados en Costa Rica, por ejemplo, luego de la suscripción del Convenio de Budapest. Resultan trascendentes aquí los bienes jurídicos de la confidencialidad, la privacidad y la autodeterminación informativa, pero también los tradicionales bienes jurídicos patrimoniales, en especial en el contexto del "phishing", el "pharming" o mediante el uso de programas "sniffers" y espías. Pero también la infraestructura informática en sí misma cuando es objeto, por ejemplo, de ataques directos por "virus", "bombas lógicas", "caballos de troya", "gusanos", y recientemente por los programas DoS o ataques de denegación de servicio, o por sustitución de páginas WEB legítimas por páginas que suplantan contenidos, etc. Al respecto, se estudiará al "sistema de información" como un ente protegido, de características especiales, que debe comprenderse con el fin de captar el sentido de la prohibición jurídico-penal.

La construcción de delitos de deber y de peligro abstracto, como metodologías propias del derecho penal moderno, deben ser objeto de crítica, con el fin de determinar la oportunidad y pertinencia de algunas formas delictivas del derecho nacional e internacional, a partir de esa lógica punitiva.

Aquí es indispensable, en suma, ofrecer oportunidad suficiente para establecer los principales problemas de legalidad involucrados y hacer referencias oportunas que permitan al aplicador e intérprete de estos tipos penales formas para adecuar sus tareas a las prescripciones constitucionales aplicables.

Como ya se ha mencionado en las secciones anteriores, la investigación de la ciberdelincuencia enfrenta una serie de dificultades de mucha complejidad. En concreto, la vertiginosa revolución tecnológica que ha impulsado los intercambios de información a nivel global y el enorme entramado de redes que han posibilitado la evolución exponencial de la Internet, ha sido el caldo de cultivo para una delincuencia que no se ha detenido en sus esfuerzos por conquistar esta "Red de Redes". Los múltiples escenarios de la comunicación, ahora incrementados por millones de teléfonos inteligentes, redes WLAN, y conexiones WIFI desperdigadas por los continentes y los países, son la puerta abierta para las intromisiones en la privacidad de los internautas, y para obtener enormes beneficios mediante el apoderamiento de

claves, números de tarjeta de crédito, contenidos de correos y secretos industriales. La anonimidad de los contactos, la posibilidad de simular direcciones IP, y la posibilidad de realizar ataques transfronterizos, proponen a las autoridades penales dificultades enormes para alcanzar con éxito la detección de las actividades ilícitas, sus autores, y, por supuesto, la localización de sus ganancias. Primero los hackers, pero luego delincuentes informáticos de todo nivel de experiencia y capacidad, pueden acceder con facilidad a la multitud de computadores del hogar conectados constantemente a Internet por medio de banda ancha, utilizarlos para realizar sus ataques y disimular su ubicación, provocando sospechas en ciudadanos inocentes que no saben que están siendo utilizados para cometer hechos penales de gran impacto dañoso. El Big Data que ha surgido con la promesa de hacer más "inteligentes" a las redes, y recolectar data de diversa índole para la toma de decisiones, se ha convertido en un inmenso reservorio de informaciones, datos, imágenes, sonidos, cualquier cosa que pudiera tener interés, y de esa manera ser unido para obtener perfiles de consumo, respuesta a las necesidades de orientación política entre los electores, organización del tráfico y orientación a los conductores en tiempo real, entre otros usos. Aparte de la cuestión de saber de dónde viene esta información y cómo es comparada, analizada y almacenada, el problema está en el uso que se le dará[16]. El Big Data, mediante herramientas de software como Hadoop, podrían permitir otra visión a las investigaciones penales en materia de ciberdelincuencia. La observación y seguimiento de gran número de equipos, bases de datos, personas, por largos periodos de tiempo, requiere del uso de infraestructuras de datos muy complejas que permitan derivar conclusiones en tiempo real que permitan orientar las investigaciones y las acciones de los equipos de detección tanto en línea como físicamente. Esto va a requerir, claramente, la preparación y entrenamiento de equipos de técnicos, investigadores, policías, fiscales y jueces, que puedan atender las investigaciones.

Así las cosas, en primer lugar, la capacitación y el incremento de la capacidad técnica de los equipos de investigación, tareas que deben ser constantes y llevar el ritmo de los cambios tecnológicos y de las infraestructuras informáticas disponibles, y el aumento de la capacidad

[16] En nuestro tránsito por una sociedad global, dejamos huellas de nuestras apetencias, de quienes somos y qué pensamos. Esto hace que los datos que hay sobre nosotros sean tan importantes, tanto para los privados como para los Estados. Es por ello que la protección de la persona frente al posible abuso de sus datos es un requerimiento básico para toda sociedad democrática. Cfr. Lane, Julia; Stodden, Victoria; Bender, Stefan; Nissenbaum, Helen (Editores), Privacy, Big Data and the Public Good. Frameworks for Engagement, New York, Cambridge University Press, 2014, pp. 195-196.

instalada de los órganos de investigación, son tareas de indudable urgencia. El éxito de una investigación en ciberdelincuencia es directamente proporcional a los conocimientos, capacidades y experiencia de los equipos técnicos involucrados. Los escenarios son múltiples: desde delitos muy focalizados y donde los autores pueden ser fácilmente detectados, hasta escenas criminales múltiples y, por supuesto, investigaciones en red. Todas ellas requieren niveles de coordinación diferentes, pero la piedra angular de cualquier indagación depende de hacer bien las labores de seguimiento, recolección y detección. Diferentes técnicos deben intervenir, desde investigadores, analistas digitales, hasta especialistas en materias específicas, cuando el tema lo requiera. Temas tales como el aseguramiento de la escena, su valoración, la recolección y preservación de la evidencia, la cadena de custodia, su almacenamiento, son los elementos con los que puede construirse una investigación exitosa.

En la época actual, donde solo es esperable una escalada de la ciberdelincuencia de la mano del incremento de la capacidad tecnológica de las redes criminales, es cuando resulta más esencial la reflexión sobre el tema de ciberseguridad y de la preparación de los equipos técnicos de investigación.

Aun cuando esta temática resulte introductoria a un análisis que habrá de hacerse con más detalle en un estudio posterior, en donde habrá que profundizar en el tema de la investigación y la evaluación forense de evidencia en delitos informáticos, resulta trascendente cerrar este primer paso de análisis de la problemática político-criminal con algunos rudimentos relacionados con la investigación criminal de estos nuevos hechos penales que involucran, además de herramientas tecnológicas de primer nivel, conocimientos y formas de comisión que proponen dificultades de gran calado, donde la experticia y el entrenamiento táctico de los equipos resulta clave. Desde un nivel básico, en que los policías deben ser entrenados para revisar e incautar computadores, teléfonos, dispositivos de memoria externos como evidencia, hasta un nivel más complejo, donde las habilidades deben incluir, pero no se reducen, a comprender el entorno en red en que sucede el proceso comunicacional en la actualidad. La recolección de "ciberevidencia" requiere cuidados especiales, así como el manejo y obtención de los equipos computacionales y sus periféricos, otro escalón indispensable de una investigación exitosa. El conocimiento sencillo de que mucho del procesamiento de datos interesante se hace no localmente sino en la "nube"

requiere de los órganos del control penal conocimiento de cómo entender las redes, hacer auditoría de datos, interceptar comunicaciones, seguir transmisiones inalámbricas, y otros aspectos técnicos de diversa complejidad. Todo ello requiere experticia que va cambiando con el tiempo y que exige de los especialistas constante entrenamiento y capacitación. La combinación de un entrenamiento jurídico, pero al mismo tiempo técnico, nos provee de especialistas híbridos indispensables para asegurar éxitos en la investigación de ciberdelincuencia.

7. Conclusiones

Luego de este rápido recorrido por el ambiente actual de la información y de determinar los diversos escenarios de riesgo, es posible construir algunos elementos que permiten dibujar las características de una política criminal informática viable en el momento presente.

Es evidente que los esfuerzos político criminales asumidos hasta el momento no han permitido mantener el ritmo de los cambios que se han venido produciendo en las tecnologías de la comunicación y de la información, ni han logrado abarcar normativamente los nuevos escenarios de riesgo que están involucrados en la ciberdelincuencia. Por más que se pueda describir estos escenarios como la fuente de nacimiento de un nuevo ámbito jurídico: el "derecho penal cibernético", aun no hay regulaciones suficientes que permitan demostrar el correcto análisis jurídico penal de problemas tales como los generados por las redes sociales, los riesgos y peligros de la Internet profunda, las amenazas provocadas por la computación ubicua y, por supuesto, la creciente utilización de sistemas de procesamiento permanente como los involucrados en la Internet de las Cosas y el big data. Es cierto que en todos estos ámbitos estamos hablando de una fotografía del momento tecnológico presente, pero sin duda algunos de sus desarrollos se proyectarán al futuro con indudables consecuencias penales, tanto en materia de nuevas afectaciones a bienes jurídicos tradicionales, como también a bienes jurídicos inmateriales y supraindividuales.

Hará bien la política criminal en tomar en cuenta estas circunstancias tecnológicas, para unir y plantear de manera integral diversas cuestiones jurídicas que tienen que ver con principios y reglas de interpretación del derecho penal nuclear y que siguen profundamente unidos a principios propios de la Ilustración, como el principio de legalidad, de lesividad y de culpabilidad.

Es por lo anterior, que la política criminal informática, como una disciplina propia, con sus principios y reglas, debe mantenerse bajo el manto de protección de los principios derivados del Estado de Derecho. Desde este punto de vista, principios tales como el de tipicidad, el de protección de bienes jurídicos y, en especial, el de lesividad, deben orientar la construcción de los tipos penales, sobre todo en aquellos casos, donde el legislador decididamente había proyectado dejar casi todas las incriminaciones en la forma de delitos de peligro abstracto.

Al respecto de la esencia de los fines de tutela, cumple un papel muy importante la protección del flujo de informaciones. No es casualidad que se defina hoy en día la diferencia entre los antiguos delitos informáticos y los nuevos ciberdelitos a partir de la característica de estos últimos de estar vinculados a los flujos de información, ya sea en redes sociales o en centros de intercambio y procesamiento de datos, como también en el procesamiento de datos a nivel global. Es ese flujo de información lo que facilita la comunicación y el comercio, pero también es la base para entender por qué es tan trascendental el cambio de un grupo de delitos que se construyó a partir de la idea de que era el computador el objeto de casi todas las conductas criminales hacia un énfasis en la afectación de las condiciones que facilitan o explican una sociedad marcada por el intercambio de informaciones: la sociedad de la información.

La conexión con los datos es tan intensa que bien podría hablarse de un verdadero "derecho penal sobre los datos", sin embargo, por más que el intercambio de datos caracterice nuestra sociedad y nuestra relación con otros seres humanos y con nuestro ecosistema de información, aun hay cuestiones abiertas al debate que tienen que ver con la puesta en peligro de otros elementos fundamentales de la convivencia como lo son, por ejemplo, bienes jurídicos como la propiedad, el patrimonio, y la misma seguridad del comercio, y hasta el intercambio económico a partir de monedas virtuales.

Para la política criminal latinoamericana, pero también para los esfuerzos en otras latitudes, resulta de primera necesidad la consideración de los pasos legislativos seguidos en el ámbito nacional como internacional. Esto último no sólo es indispensable a los efectos de una más eficaz cooperación para la investigación y persecución de la ciberdelincuencia, sino también de cara a la construcción de un derecho penal intercultural planteado a partir de una verdadera tutela global de la información y su procesamiento. Es en esta dirección que muy probablemente

tendrán que incentivarse esfuerzos para que se produzcan más convenios de cooperación en materia penal, inspirados en el principio de justicia universal y de prolongación del principio de territorialidad, que junto a tareas conjuntas de investigación y de obtención de evidencia, también faciliten la utilización de esa evidencia en procesos penales instaurados en diversas administraciones de justicia. La pieza que falta en ese rompecabezas legislativo yace allí donde siempre debió buscarse: en un capítulo bien desarrollado sobre cooperación en asuntos penales en las legislaciones procesales de los países, que minimice los problemas de articulación en tareas de policía de cooperación y en investigaciones de carácter global. Esto último será la garantía definitiva para el éxito de las investigaciones, algo en lo que ya la Convención de Budapest ha avanzado mucho, pero que aún requiere un esfuerzo nacional más intenso.

La política criminal informática será posible cuando se comprenda que será una política criminal de la Internet, en la medida que es en ese ámbito que se cometen los hechos que han de perseguirse, pero que también es el ámbito donde, principalmente, se investigará a la ciberdelincuencia. Aquí se plantean cuestiones muy complejas relacionadas con la soberanía de los países, y con las tareas que los órganos del control penal cumplen en el plano nacional. Es indudable que aquí se plantea, como lo ha señalado con razón Sieber, un análisis concienzudo de las decisiones normativas que se pueden plantear desde del derecho internacional. Esta última es una consecuencia de una delincuencia que es global, tanto por el medio donde se comete (Internet) como por los efectos que produce. Junto a ello, un tema adicional que ha de subrayarse suficientemente: la ciberdelincuencia es también una forma de crimen organizado, no sólo porque ahora se comete de manera sistemática por grupos deslocalizados geográficamente, sino porque actores de otros tipos de criminalidad (terrorismo, por ejemplo) utilizan los medios usualmente vinculados en su comisión para financiar actividades de un más amplio espectro, agravando la sensible situación de seguridad de los Estados.

Finalmente, la política criminal informática debe construirse de la mano de un vigoroso debate en pro del derecho de la protección de datos personales. Si es posible pensar en un Budapest 2.0, lo es a partir de un compromiso decidido con la autodeterminación informativa, y, al mismo tiempo, con regulaciones que presten especial atención a los límites que el Estado de Derecho establece para las investigaciones de amplio espectro en materia de ciberdelincuencia.

No todo lo que es posible técnicamente debe ser autorizado jurídicamente, un principio que tuvo especial relevancia en las primeras generaciones de leyes sobre protección de datos, pero que se ha venido haciendo más importante de cara a los retos de un combate global de una criminalidad al mismo tiempo sutil, incruenta e increíblemente lesiva. esto conduce a un debate sobre la correlación de principios en el combate de la ciberdelincuencia, y es en una convención de derecho penal cibernético donde deben contemplarse las reglas del juego para el futuro posible de este nuevo derecho penal que estamos construyendo. La suerte está echada para la definición de un camino que permita asegurar las condiciones para la libertad y la seguridad en una sociedad global profundamente marcada por el signo tecnológico.

8. Bibliografía

Barrio Andrés, Moisés, Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos, Madrid, Wolter Kluwer, 2018.

Bedecarratz Scholz, Francisco, "Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal", en: Revista chilena de Derecho y Tecnología, Santiago de Chile, Vol.7 No.1, junio 2018, disponible en: http://dx.doi.org/10.5354/0719-2584.2018.48515

Hansen, Markus & Fabian, Benjamin & Möller, Jan & Spiekermann, Sarah. (2006). Szenarien des Ubiquitous Computing, disponible en https://www.researchgate.net/publication/262563325

Hilgendorf, Eric, "Die Strafrechtliche Regulierung des Internet als Aufgabe eines modernen Techniksrechts", en: JZ/17, 2012, pp. 825-832.

Hilgendorf, Eric; Frank, Thomas; Valerius, Brian, Computer- und Internetsstrafrecht. Ein Grundriss, Berlin, Heidelberg, Springer Verlag, 2005.

Leuthardt, Beat, Leben online. Von der Chipkarte bis zum Europol-Netz: Der Mensch unter ständigem Verdacht, Frankfurt am Main, Rowohlt Taschenbuchverlag GmbH, 1996.

Melo, Letícia, "Régimen Jurídico de Blockchain: una prueba atípica", en: Revista Bioética y Derecho, Barcelona, No. 46, 2019, disponible en: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872019000200007

Pérez Cepeda, Ana Isabel (Directora), Política Criminal ante el Reto de la Delincuencia Transnacional, Valencia, Ediciones Universida de Salamanca, Tirant Lo Blanch, 2016.

Schwarzenegger, Christian, "Die Internationalisierung des Wirtschaftsstrafrechts und die schweizerische Kriminalpolitik: Cyberkriminalität und das neue Urheberstrafrecht", en: ZSR 2008 II, disponible en: https://www.ius.uzh.ch/dam/jcr:00000000-5624-ccd2-0000-00003bba68ae/ZSRII2008BeitragSchwarzenegger.pdf

Sieber, Ulrich, Straftaten und Strafverfolgung im Internet, Gutachten C zum 69. Deutschen Juristentag, C.H. Beck, München, 2012.

Stegbauer, Christian, Euphorie und Ernüchterung auf der Datenautobahn, Frankfurt am Main, dipa-Verlag, 1996.

Lane, Julia; Stodden, Victoria; Bender, Stefan; Nissenbaum, Helen, Privacy, Big Data and the Public Good. Frameworks for Engagement, New York, Cambridge University Press, 2014.

Taylor, Robert; Fritsch, Eric; Liederbach, John; Saylor, Michael; Tafoya, William L., Cybercrime and Cyberterrorism, New York, Pearson, 2019.

Wassmer, Martin Paul, "Delitos Informáticos (Cybercrimes)", en: Revista Penal, No. 40, julio 2017, Valencia, Tirant Lo Blanch, pp. 250-255.