REVISTA CHILENA DE DERECHO Y TECNOLOGÍA
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO • UNIVERSIDAD DE CHILE
ISSN 0719-2576 • VOL. 1 NRO. 1 (2012) • PÁGS. 221-238 • DOI 10.5354/0719-2584.2012.24030

La Convención sobre Cibercrimen del Consejo de Europa[1]

The Convention on Cybercrime

SUSAN W. BRENNER
School of Law, University of Dayton

RESUMEN La Convención sobre Cibercrimen (de 23 de noviembre de 2001) reconoce y asume la posibilidad de eludir conductas delictivas tras las fronteras del país de comisión del delito. La Convención propone una teoría funcionalista del derecho penal para fundamentar la imposición de la pena a través de una persecución también garantista de los derechos fundamentales. El autor da cuenta de lo inadecuado de los sistemas tradicionales para perseguir delitos informáticos, pero, de todos modos sostiene que la Convención equipara el cibercrimen a la delincuencia habitual y exige a los Estados partes un trato de afrenta al Estado-nación, siguiendo los tradicionales parámetros criminológicos. A los Estados partes se les requiere la adopción de un determinado diseño de investigación (evidencia electrónica, incautación a través de sistemas informáticos, recolección de datos de tráfico, entre otras). No excluida de críticas, la Convención es rechazada por atentar contra la privacidad.

1. Artículo originalmente publicado en Jack M. Balkin, James Grimmelmann, Eddan Katz, Nimrod Kozlovski, Shlomit Wagman y Tal Zarsky (editores), *Cybercrime: Digital Cops in a Networked Environment*, New York University Press, 2007. La traducción es de Alberto Cerda Silva, profesor asistente de Derecho Informático de la Universidad de Chile. La presente traducción y publicación ha sido gentilmente autorizada por la autora del texto, Susan W. Brenner, y su editor, Jack M. Balkin.

PALABRAS CLAVE Delitos informáticos, privacidad, cibercrimen, Convención sobre Cibercrimen.

ABSTRACT The council of Europe Convention on Cybercrime (November 23rd 2001) recognizes and assumes the possibility of evading criminal conduct beyond the boarders of the country where the crime was committed. The Convention proposes a functionalist theory of penal law in order to base the imposition of the sentence guaranteeing fundamentals rights. The author highlights the inadequacy of traditional systems aim at persecuting informatics crime. He considers, however, that the Convention puts cyber crime and habitual delinquency on the same footing. It demands from Party States the adoption of a specific manner of investigation (electronic evidence, confiscation through informatics systems, traffic data collection, among others) Nevertheless, the Convention has been often criticized because it may jeopardize privacy.

KEYWORDS Informatic crime, privacy, cybercrime, Convention on Cybercrime.

El 23 de noviembre de 2001 la Convención sobre Cibercrimen fue abierta para su suscripción en Budapest.[2] La Convención fue elaborada pensando en la que es quizá la característica más distintiva del cibercrimen: su capacidad para trascender las fronteras nacionales y, de este modo, eludir la acción de la legislación local.

ANTECEDENTES

La Convención es la culminación de un esfuerzo que comenzó décadas atrás, cuando se hizo claro que la tecnología computacional podía ser empleada en la comisión de diversos tipos de actividades indeseables. Algunas de éstas tomaban la forma de delitos tradicionales; los computadores eran y son usados para cometer este tipo de ilícitos, tales como el robo, los fraudes, la extorsión y el acoso.[3] Los computadores también

2. Convención sobre Cibercrimen del Consejo de Europa (CETS nro. 185), Chart of Signatures and Ratifications. Disponible en español en <http://conventions.coe.int/treaty/en/Treaties/Html/185-SPA.htm>.

3. El texto original emplea la expresión *stalking*, que hemos traducido por acoso, que

pueden ser usados en actividades que son «nuevas» en varios sentidos, como el acceso indebido a los sistemas informáticos, el daño a la información contenida en ellos y el lanzamiento de ataques de denegación de servicios por tales sistemas. En los ochenta, los países habían comenzado a adoptar leyes que específicamente penalizaban tanto este «nuevo» tipo de actividades, como el uso de la tecnología computacional para la comisión de delitos convencionales. Esto fue particularmente cierto para Europa y Norteamérica; en los noventa, los países de ambas regiones adoptaron leyes que penalizaban un conjunto de actividades que incluían obtener acceso no autorizado a los sistemas informáticos, dañar la información contenida en tales sistemas y liberar *software* malicioso.

De este modo, implícitamente se asumió que esto era todo lo necesario para permitir a las naciones ocuparse del cibercrimen; después de todo, la respuesta histórica a la aparición de nuevas conductas indeseables ha sido su penalización. La adopción de leyes locales responden proscribiendo determinadas conductas; aquellos que incurren en tales comportamientos pueden ser aprehendidos, procesados, condenados y sancionados, lo cual impide que vuelvan a delinquir y desalienta a otros a seguir su desafortunado ejemplo. Por supuesto, no todos aquellos que delinquen serán aprehendidos y condenados; la incidencia de conductas proscritas en una sociedad puede ser mantenida dentro de márgenes razonables si el total de aprehensiones y condenas por delitos es suficiente para persuadir a la mayoría de los eventuales infractores de que es poco aconsejable involucrarse en tales actividades.

Este es el fundamento del sistema de justicia penal en todas las naciones modernas y, por consiguiente, ha sido la premisa de la legislación nacional sobre cibercrimen adoptada en los años ochenta y noventa. Estas leyes eran «legislación interna», esto es, leyes que asumían que las actividades prohibidas ocurrirían por completo dentro de las fronteras territoriales de la nación, que tanto el ofensor como la víctima, si no eran ciudadanos de la misma nación, estaban a lo menos situados al interior de ella cuando estos ilícitos acaecían. Esta suposición tiene sustento histórico para la actividad criminal, la que desde diversas perspectivas

---

en el *common law* corresponde al acto o caso en el cual una persona sigue a otra con sigilo, frecuentemente de modo subrepticio, ya sea simplemente para incomodarle o para hacerle víctima de otro hecho delictivo, tal como un robo o asalto (N. del T.).

tiene resabios más primitivos que la de su homóloga civil. El comercio a lo largo del tiempo comenzó a trascender las fronteras y legislaciones nacionales, en cambio la criminalidad mantuvo un carácter provincial en su mayor parte, incluso hasta recientemente, porque ésta supone una dinámica personal, un cara a cara entre la víctima y el ofensor. Así, por ejemplo, es imposible incurrir en el delito de violación si el violador y la víctima están a cinco millas de distancia; y, en un entorno no tecnológico, es igualmente imposible hurgar en los bolsillos de alguien o tomar su propiedad por la fuerza si el ladrón y la víctima están en diferentes países.

CIBERCRIMEN

Muchas cosas pueden llegar a ser posibles en un entorno tecnológico. Mientras es aún imposible cometer remotamente un delito como la violación, la informática ha facilitado la comisión de los delitos más tradicionales, los cuales pueden trascender fácilmente las fronteras nacionales. Esto es también cierto respecto de los «nuevos» delitos que han emergido en el ciberespacio; *hacking*, *software* malicioso, ataques de denegación de servicio y otras figuras relacionadas se esfuerzan por ignorar las fronteras territoriales y jurisdiccionales. Tal como este aspecto del cibercrimen se hizo evidente, lo fue igualmente el hecho de que la legislación nacional «interna», aquella que se había adoptado para ocuparse de él, resultaba insuficiente para hacerse cargo de la actividad delictiva con base externa.

El cibercrimen no es, por supuesto, el primer ejemplo de actividad criminal con base externa. Los países a lo largo del tiempo idearon mecanismos para ocuparse de aquellos casos en que los delincuentes o la actividad criminal trascendían las fronteras nacionales. Una idiosincrásica red de tratados de asistencia legal recíproca comprometían a varios países a prestarse apoyo para la investigación de actividades criminales del mundo real, como el tráfico de drogas; y si tales tratados no existían, las autoridades podían invocar los antiguos procedimientos de cartas rogatorias o exhortos para obtener evidencia desde el extranjero (Cassella, 2004: 99). Y los tratados de extradición podían ser usados para asegurar a una persona, a efectos de ser posteriormente llevada a juicio.

Mientras los mecanismos recién mencionados pueden ser apropiados para aproximarse a la investigación de un delito o aprehensión de un de-

lincuente del mundo real, ellos resultan demasiado inadecuados y fútiles respecto del cibercrimen y los delincuentes informáticos. Un problema es que, no obstante la legislación nacional adoptada en las décadas de los ochenta y noventa, muchos países aún carecen de leyes sobre cibercrimen. Si el país A solicita la asistencia del país B porque uno de sus ciudadanos ha sido víctima de un cibercrimen (de acuerdo a la legislación del país A) cometido por un ciudadano del país B (el cual carece de leyes sobre cibercrimen), la falta de incriminación de la actividad por el segundo se traducirá en que: i) ningún tratado de asistencia legal recíproca surtirá efecto para requerir apoyo en la investigación; ii) las cartas rogatorias o exhortos serán probablemente inválidos también; y iii) el delincuente, si es identificado, no podrá ser extraditado para ser procesado en el país A, donde su conducta es ilegal. El resultado es el mismo si el país B tiene adoptada alguna ley sobre cibercrimen, pero ella no penaliza exactamente la misma conducta en cuestión. En los hechos el resultado es que los ciberdelincuentes puede operar con impunidad desde el país B por tanto tiempo como ellos se limiten a ataques externos, esto es, por el tiempo en que ellos sólo ataquen ciudadanos de otros países, tal como el país B.

En este escenario, el país B es un «paraíso» para el cibercrimen, tal como algunas ciudades fueron el paraíso de los piratas de alta mar siglos atrás, cuando los mares estaban tan «incivilizados» como el ciberespacio lo está hoy en día. El estatus de paraíso del cibercrimen de un país puede ser voluntario o inadvertido, el resultado de un diseño o de la simple negligencia. El ímpetu de un país por evitar tal estatus es irrelevante; lo relevante es el efecto. Las leyes diseñadas para evitar que los ciudadanos de un país sean presa de otros ciudadanos del mismo país son irrelevantes cuando la delincuencia es una externalidad; no disponemos de leyes, ni de mecanismos, que sean diseñados para prevenir que los ciudadanos de un país sean víctimas de ciudadanos de otro país. Desde que asumimos la influencia de las fronteras físicas, hemos dividido la amenaza en interna («crimen») y externa («guerra») y hemos asignado responsabilidad para abordar cada una de tales amenazas a instituciones diferenciadas (el sistema legal y el militar). Esta aproximación trabaja satisfactoriamente para las actividades con base física, pero no en el caso del cibercrimen; lo que nosotros hemos definido como amenaza «interna» puede ahora provenir desde el exterior. Debemos, por consiguiente, idear una nueva forma de acercarnos al tema.

Esto nos lleva a la Convención sobre Cibercrimen, la cual pretende ser una nueva aproximación que resuelve los problemas esbozados precedentemente. Es la culminación de un esfuerzo que comenzó hace más de veinte años con un estudio de la Organización para la Cooperación y Desarrollo Económicos (OCDE) sobre la posibilidad de armonizar las legislaciones nacionales sobre cibercrimen; la premisa era que mejorando la consistencia de las leyes nacionales se mejoraría la capacidad para hacer cumplir la ley ante el cibercrimen. La OCDE emitió un reporte recomendando que los países penalizasen un conjunto de conductas como cibercrimen. Al mismo tiempo, el Consejo de Europa comenzó a estudiar el asunto, un esfuerzo que finalmente condujo a la Convención sobre Cibercrimen (cf. Consejo de Europa, 1997).

LA CONVENCIÓN

La Convención representa un acercamiento tradicional a la problemática del cibercrimen, planteado de conformidad con las agencias de cumplimiento y las sociedades a las cuales ellas protegen. Se equipara el cibercrimen con la delincuencia y enseguida trata a aquél como una amenaza interna, de la cual se ocupa con el sistema de justicia criminal de una nación cuyos ciudadanos han sufrido «daño» de una actividad particular. A diferencia del foco de atención sobre la cuestión según lo constatado precedentemente —el hecho de que el ciberespacio permite que los ciudadanos de una sociedad sean víctimas remotas de los ciudadanos de otras sociedades—, la Convención incorpora una aproximación tradicional al fenómeno delictivo y trata al cibercrimen como una afrenta a un específico Estado-nación. En consecuencia, se articulan estrategias que intentan mejorar la capacidad del Estado-nación para responder al cibercrimen.

Esta sección examina el tratamiento del tema adoptado por la Convención; las conclusiones, en cambio, consideran la aproximación que debía tomarse al respecto.

DELITOS

La Convención comienza requiriendo de los Estados partes la definición de ciertas actividades como cibercrimen. Este aspecto de la Convención

(artículos 2.º a 9.º) es diseñado para hacerse cargo del tema del «paraíso» discutido en la sección precedente, a efectos de asegurar una línea base de consistencia en relación a un conjunto de ofensas. La meta es inobjetable, pero la metodología es peculiar. Las partes de la Convención deben criminalizar: i) varias actividades que tienen en la mira los sistema informáticos y la data; ii) la falsificación informática; iii) los fraudes informáticos; iv) el uso de la tecnología computacional para crear, distribuir o procesar pornografía infantil; y v) el uso de la tecnología computacional para cometer infracciones a la propiedad intelectual (artículos 2.º a 10.º). Las actividades que tienen en la mira a los sistemas informáticos y la data i), en concreto, son: obtener acceso no autorizado a ellos, dañar los mismos y el denominado «abuso de dispositivos» (artículos 2.º a 6.º).[4]

No hay nada de especial en requerir de los países la criminalización de la mayor parte de tales actividades; la excepción es el delito de «abuso de dispositivos», el cual ha sido criticado porque suprime la libertad de expresión y, a su vez, penaliza actividades legítimas de los profesionales de la seguridad informática. Lo que sí es peculiar es que esta bastante limitada lista de actividades no parezca una efectiva manera de hacerse cargo de la cuestión del «paraíso»; como he explicado anteriormente, los delincuentes informáticos pueden explotar la ausencia de leyes sobre la materia en general o en un área específica para cometer delitos con relativa impunidad. Una de las metas de la Convención es la eliminación de esa oportunidad mediante la «armonización de las normas sustantivas de derecho interno… en el área del cibercrimen».[5] Pero la Convención sólo exige a las partes para que se criminalice un subgrupo de actividades ilegales que pueden ser facilitadas por la tecnología computacional; así, por ejemplo, no exige a los países penalizar el uso de los computadores para cometer defraudación, extorsión, acoso, terrorismo o para infringir lesión física a una persona o a su propiedad.

Uno puede argumentar que no era necesario incluir estos delitos tradicionales porque ellos ya se encuentran prohibidos por los códigos cri-

4. La versión original del texto emplea la expresión *misuse of devices*, mientras el texto oficial de la Convención en francés califica este ilícito como *abus de dispositifs* (N. del T.).

5. Reporte Explicativo. Convenio sobre Cibercrimen del Consejo de Europa (CETS nro. 185), ¶ 16, disponible en <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

minales de las naciones modernas, pero la misma Convención incluye a lo menos tres delitos tradicionales: falsificación, fraude y pornografía infantil. La razón para incluirlos fue presumiblemente que el uso de la tecnología computacional incrementa los casos en que puede eludirse la definición tradicional de tales delitos, pero ello es igualmente cierto respecto de otros delitos, tal como el hurto. Ni la Convención ni el Reporte Explicativo adjunto a la misma indican: i) ¿porqué sólo un subgrupo de delitos fueron incluidos en la Convención?, y ii) ¿porqué este particular conjunto de conductas fue elegida? A excepción del abuso de dispositivos, los delitos que tienen en la mira los sistemas informáticos y la data fueron obviamente seleccionados por la Convención; pero esto mismo no es cierto tratándose de otros delitos. Es efectivo que la tecnología computacional puede incrementar exponencialmente la capacidad de alguien para cometer fraude o para producir y diseminar pornografía infantil, pero esto es igualmente cierto respecto de otros delitos, tales como la extorsión.

Existen otras dos peculiaridades en el modo en que la Convención se acerca a la armonización de la legislación sustantiva sobre cibercrimen. Una de ellas es que no suministra una legislación modelo que las partes de la Convención deban implementar; tal como un documento que haga las veces de gran acuerdo para asegurar la consistencia en la implementación de las leyes adoptadas en varios países. Una legislación modelo podría también aliviar la carga que significará para algunos países desarrollar la legislación de implementación. Los Estados Unidos tuvieron mucha influencia en la elaboración de los borradores de la Convención, de este modo ella tiende a seguir la legislación estadounidense; en consecuencia, implementar la Convención debía ser un asunto sencillo para este país. Pero ello no será así tratándose de otros países.

La última peculiaridad en las disposiciones sustantivas de la Convención es que la mayoría de los artículos que contemplan los «delitos» permiten a las partes reservarse el derecho a no imponer responsabilidad en algunas de dichas conductas. Así, por ejemplo, el artículo 9 se refiere a la pornografía infantil y requiere, por defecto, la penalización del uso de tecnología computacional para producir, diseminar o poseer pornografía infantil, ya sea «real» o «virtual». Sin embargo, los países pueden elegir o no criminalizar: i) el uso de la tecnología computacional para obtener y/o poseer pornografía infantil, y ii) cualquier actividad que implique

pornografía infantil generada mediante computadoras o «virtual» (artículo 9º [4]). Al tiempo que la capacidad de limitar la responsabilidad impuesta por la Convención da a los países cierta flexibilidad, ella también socava la pretendida meta de alcanzar la armonización de las leyes nacionales sobre cibercrimen.

PROCEDIMIENTO

Las más extensas y controvertidas disposiciones de la Convención son aquellas que se ocupan de la investigación y el procedimiento relativo al cibercrimen. En esencia, la Convención requiere que los Estados partes adopten una legislación que sea diseñada para facilitar la investigación: i) permitiendo la preservación y producción de evidencia electrónica; ii) solicitando búsqueda e incautación legal de los sistemas informáticos; y iii) autorizando a la autoridad para recolectar datos de tráfico y de contenidos (artículos 16.º a 21.º). Las partes también deben colaborar mediante: i) la extradición de los delincuentes; ii) compartir información; y iii) preservar, acceder, interceptar y revelar datos de tráfico y contenido (artículos 23.º a 34.º). Y cada parte debe designar un punto de contacto 24/7, el que será responsable de asegurar «asistencia inmediata» en «investigaciones y procedimientos» relativos a cibercrimen (artículo 35.º).

El objetivo es hacer más expedito el procedimiento para acceder a la evidencia —y a los delincuentes mismos— entre los países. Como hemos observado, los investigadores tradicionalmente han confiado en un conjunto de tratados de asistencia recíproca o en las cartas rogatorias, las cuales permiten a los tribunales de un país requerir la colaboración de los tribunales de otro país para llevar a cabo cierta diligencia, tal como obtener una prueba. Ambos procedimientos son muy lentos, lo cual los hace inadecuados para la investigación de cibercrimen.

En su mayor parte, la investigación del cibercrimen se centra en evidencia digital, por ejemplo, en el contenido de los mensajes de correo electrónico, en las direcciones empleadas para enviar un *e-mail*, en los archivos *logs* de actividad computacional y en la data almacenada en los computadores personales o portátiles. Los países han desarrollado el procedimiento aplicable durante el último siglo y se han ocupado esencialmente de la evidencia tangible, tal como armas, drogas, documentos de papel, huellas dactilares o similares. La evidencia física puede desapa-

recer, pero no se puede destruir fácilmente; y usualmente es muy difícil, si no imposible, alterarla. En cambio, la prueba digital es frágil y su destrucción o alteración es muy sencilla. Un prestador de servicios de Internet, por ejemplo, puede programar rutinas para eliminar los archivos *logs* relativos a la actividad de los sistemas; y puede que tales archivos contengan evidencia necesaria para la investigación de un cibercrimen. Los investigadores, entonces, necesitan un modo de asegurarse que la evidencia será preservada y estará disponible para su uso. Ni los tratados de asistencia recíproca, ni las cartas rogatorias son apropiados para ello, pues ambos mecanismos resultan excesivamente lentos. La Convención está diseñada para mejorar el proceso usado para localizar, preservar y compartir evidencia digital a través de las fronteras nacionales; la Convención complementa las disposiciones de los tratados mencionados o las disposiciones legales aplicables, en su caso.

Como hemos apuntado con antelación, las normas sobre procedimiento de la Convención han suscitado controversia, una buena parte de la cual se ha centrado en tres cuestiones. Una de ellas deriva del artículo 14, el cual determina el ámbito de estas disposiciones. Este artículo requiere que las partes apliquen los procedimientos establecidos por la Convención no sólo para los delitos definidos de acuerdo a ella misma, sino que también i) para la investigación de cualquier delito «cometido mediante un sistema computacional», y ii) para la recolección de evidencia digital a ser usada en un procedimiento relativo a cualquier otro delito. Los artículos 20º. y 21.º permiten a los países limitar la interceptación de datos de contenido y la recolección en tiempo real de datos de tráfico a investigaciones relativas a «delitos graves» de acuerdo con su «legislación interna», pero, por otro lado, estas amplias facultades conferidas por la Convención aplican a la investigación de cualquier cibercrimen y a la investigación de cualquier delito que requieran evidencia digital.

La Convención no explica por qué sus disposiciones procesales tienen una aplicación ostensiblemente más amplia que sus disposiciones sustantivas, esto es, por qué aquéllas aplican tanto para delitos comprendidos en la Convención como para delitos que no califican como cibercrimen. Por lo demás, esto hace aparecer a las disposiciones sustantivas de la Convención como irrelevantes. Si los procedimientos requeridos pueden ser empleados para la investigación de cualquier delito cuya comi-

sión ha implicado el uso de tecnología computacional o la existencia de medios de prueba electrónicos, cabe preguntarse cuál es realmente la importancia de los delitos definidos en los artículos 2º. a 11.º de la misma Convención. El mismo resultado podría haberse obtenido si las disposiciones procesales simplemente aplicasen a cualquier cibercrimen y a cualquier delito que sin cibercrimen ha generado prueba electrónica. Adicionalmente, hay una situación de potencial abuso: una parte de la Convención podría verse obligada a brindar asistencia en la investigación de otra parte en la cual tal actividad no es un cibercrimen (u otro delito) bajo su legislación interna. Tradicionalmente, los tratados sobre extradición han requerido de la doble incriminación, lo cual supone que la conducta en cuestión sea delito tanto en el país requirente de la extradición, como en el requerido; y si bien ello no ha sido siempre cierto tratándose de tratados de asistencia recíproca, ello generalmente incluye disposiciones conforme a las cuales un país puede denegar la asistencia requerida si se trata de «delitos políticos».

Este tema de la doble incriminación también se suscita en otras disposiciones. Los artículos 23.º a 35.º establecen los estándares y requisitos para la cooperación internacional. El artículo 25.º requiere a las partes proveerse «la más amplia asistencia mutua posible para los objetivos de la investigación o procedimientos asociados a delitos relacionados con sistemas informáticos y data, o para la recolección de evidencia en formato electrónico de un delito». De acuerdo con el Reporte Explicativo, los borradores imponían «una obligación de cooperar para tan amplia clase de delitos porque existe la misma necesidad de perfilar mecanismos de cooperación internacional en ambas categorías de ilícitos».[6] Muchos, particularmente en Estados Unidos, critican la ausencia de requisitos asociados a la doble incriminación. Como ha sido apuntado por algunos:

> El tratado requeriría que las autoridades estadounidenses cooperasen con las fuerzas policiales extranjeras inclusive cuando una agencia esté investigando una actividad que, si bien constituye delito en su territorio, es perfectamente lícita en los Estados Unidos. Ningún gobierno

6. Reporte Explicativo. Convenio sobre Cibercrimen del Consejo de Europa (CETS nro. 185), 253.

> debería ser puesto en la situación de asumir una investigación respecto de uno de sus ciudadanos que ha actuado lícitamente.[7]

Aquellos que defienden la Convención recalcan que el artículo 25 condiciona la entrega de asistencia a la existencia de una genérica doble incriminación. Además, ellos recalcan que bajo el artículo 27 (4), un país puede rehusar un requerimiento cuando: i) el requerimiento está relacionado con un delito político, o ii) «sea probable que perjudique su soberanía, seguridad [...] u otros intereses esenciales». Esta disposición aparentemente permitiría a los Estados Unidos declinar la asistencia cuando las investigaciones entrañen asuntos relativos a libertad de expresión u otras garantías constitucionales.

El tercer asunto que ha suscitado una controversia sustantiva es la privacidad. El artículo 15.º es la única disposición de la Convención que se refiere a la privacidad y otros derechos. Este artículo exige a las partes asegurar que la «implementación y aplicación de las facultades y procedimientos» prescritos por la Convención «estén sujetos a condiciones y salvaguardias [...] las cuales provean una adecuada protección de los derechos humanos y libertades». Se refiere a las convenciones para la Protección de los Derechos Humanos y las Libertades Fundamentales del Consejo de Europa de 1950, al Pacto Internacional sobre Derechos Civiles y Políticos de las Naciones Unidades de 1966, y otros instrumentos internacionales sobre derechos humanos aplicables. Muchos consideran que el artículo 15.º es completamente inadecuado. Electronic Privacy Information Center, por ejemplo, reclama que el artículo 15.º es «bastante impreciso» y que, además:

> [La Concención fracasa en] el respeto fundamental a la doctrina de los derechos humanos a que adhieren las convenciones internacionales precedentes, tales como la Declaración Universal de Derechos Humanos de 1948 y la Convención para la Protección de los Derechos Humanos y las Libertades Fundamentales de 1950. La Convención sobre Cibercrimen también ignora una multitud de tratados relacionados con la privacidad y la protección de los datos personales, incluida la Con-

7. Electronic Privacy Information Center, Carta a Richard Lugar, Presidente del Comité del Senado sobre Relaciones Exteriores (17 de junio de 2004). Disponible en <http://www.epic.org/privacy/intl/senateletter-061704.pdf>.

> vención para la Protección de las Personas en relación con el Tratamiento Automatizado de Datos Personales del Consejo de Europa de 1981 y la Directiva de la Unión Europea sobre Protección de Datos de 1995.

Irónicamente, quizás, algunos atribuyen la negligencia de la Convención en relación con garantías a la privacidad a la influencia de los Estados Unidos:

> Una Convención desarrollada por el Consejo de Europa debió dar alta prioridad a la cuestión de la protección de datos [...] Tan importantes salvaguardas fueron marginales para acomodarse a los intereses del gobierno de los Estados Unidos, el cual no favorece las leyes sobre protección de datos personales como una política. A diferencia de la Unión Europea [...] no hay una legislación general sobre protección de datos en los Estados Unidos. Los Estados miembros de la Unión Europea debieron ser condescendientes con lo que constituye un común denominador más bajo en el campo de la protección de datos.

Los defensores de la privacidad critican la Convención no sólo por su fracaso en incluir garantías generales respecto de la privacidad, sino también por algunas de las facultades que ella confiere para obtener el cumplimiento de la ley. Así, por ejemplo, el artículo 18.º (1) (a) requiere a las partes tomar las «medidas legislativas u otras» que sean necesarias para autorizar a sus «autoridades competentes» disponer que alguien en su territorio «someta un computador determinado que está en posesión o control de tal persona». Y el artículo 19 (4) requiere a las partes tomar similares medidas para «facultar» a sus «autoridades competentes para ordenar a cualquier persona que ha conocido acerca del funcionamiento de un sistema computacional o medidas aplicadas para proteger el sistema a proveer» la información necesaria para explorar el sistema computacional o un «medio de almacenamiento de la información». Los críticos de la Convención alegan que, cuando se leen en conjunto dichas disposiciones autorizan a las autoridades a forzar a los individuos a divulgar sus llaves de encriptación, lo cual podría violar «derechos tales como la privacidad de las comunicaciones» y el derecho a la no autoincriminación.

Los críticos de la Convención también mencionan otros problemas específicos en relación con las disposiciones procesales, tales como la ausencia de garantías para el error judicial en las búsquedas computa-

cionales, de órdenes judiciales de interceptación de datos y de órdenes de cumplimiento. Sus críticos también sostienen un reparo general, que no apunta a las disposiciones de la Convención, sino al proceso a través del cual ella fue elaborada. Muchos son quienes reclaman que la Convención fue redactada

> de un modo muy secreto y antidemocrático. El Comité de Expertos sobre Crimen en el Ciberespacio del Consejo de Europa [...] completó diecinueve borradores de la Convención antes de que el documento fuese comunicado al público. Entre los años 1997 y 2000 ninguno de los borradores fue liberado ni se solicitó aportes al público. La Convención fue redactada por personas y agrupaciones principalmente asociadas a autoridades de cumplimiento de la ley y refleja exclusivamente sus preocupaciones, con el consiguiente menoscabo a la privacidad y las libertades civiles.[8]

Quienes formulan estas reclamaciones objetan haber dispuesto de sólo un tiempo limitado para revisar y comentar la Convención y que sus sugerencias no fueron incluidas en el texto final. Los representantes del Departamento de Justicia de los Estados Unidos, en cualquier caso, rechazan la idea de que la Convención sea el producto de negociaciones secretas.

CONCLUSIONES

La Convención sobre Cibercrimen es un documento complejo que ha suscitado reacciones también complejas desde varios puntos de vista. Es difícil, en este punto de la historia, evaluar cuál será el efecto que tendrá en la lucha contra el cibercrimen, si alguno llega a haber. Hay razones para creer que tal impacto podría ser mínimo.

Uno es empírico: el sorprendentemente lento ritmo de ratificación. La Convención fue abierta a su suscripción y ratificación el 23 de noviembre de 2001. Tres años después, ha sido firmada por treinta y ocho países, pero sólo ha sido ratificada por ocho: Albania, Croacia, Estonia, Hungría, Lituania, Rumania, Eslovenia y la antigua República Yugoes-

8. Electronic Privacy Information Center, en nota anterior.

lava de Macedonia.[9] Ninguno de los principales países europeos la ha ratificado, ni los Estados Unidos, ni Canadá o Japón.[10] En noviembre de 2003, el Presidente Bush llamó al Senado a aprobar la ratificación y el Comité del Senado sostuvo audiencias sobre la Convención en junio del 2004, pero nada ha sucedido desde entonces. En septiembre del 2004, el Consejo de Europa sostuvo una conferencia cuyo objetivo fue alentar a más países a firmar y ratificar la Convención. Al ser consultado uno de los conferencistas sobre el lento ritmo de ratificación, éste lo atribuyó a la complejidad de las cuestiones planteadas en ella.

Los primeros en adoptar la Convención han ignorado lo dicho por tres años; la ratificación e implementación no son obviamente un tema de alta prioridad en tales países. Su inacción es extraña y un tanto inquietante. Esto puede ser, tal como sugirió el conferencista antes mencionado, que la Convención sea víctima de sus propias ambiciones: que la naturaleza y extensión de los esfuerzos requeridos para implementarla se hayan descuidado por los países que la han ratificado. Es difícil, sin embargo, entender por qué ello podría ser cierto tratándose de los principales países de Europa y de los Estados Unidos, considerando su participación en la redacción de la Convención, lo cual hace presuponer que han incorporado los principios y prácticas que ellos consideran aceptables y alcanzables. De hecho, el Departamento de Justicia ha hecho ver que si los Estados Unidos ratifica la Convención, no necesitarán adoptar legislación de implementación, ya que la normativa actual es adecuada.

Para que la Convención logre su objetivo —la armonización de la normativa nacional sustantiva y procesal sobre cibercrimen— debe ser ratificada e implementada por todos los países en el mundo. De otro modo, lo conseguido será el escenario del «paraíso». La ausencia de premura con que los Estados Unidos y los principales países de Europa se han acercado al tema nos sugiere que es improbable el logro de su

9. A diciembre del 2010, treinta países han adherido/ratificado a la Convención, ellos son: Albania, Alemania, Armenia, Azerbaijan, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estados Unidos, Estonia, Finlandia, Francia, Holanda, Hungría, Islandia, Italia, Latvia, Lituania, Moldavia, Montenegro, Noruega, Portugal, Rumania, Servia, Ucrania y la antigua República Yugoeslava de Macedonia (N. del T.).

10. La Convención fue ratificada por los Estados Unidos el 29 de septiembre del 2006; Canadá y Japón, pese a haberla firmado, aún no la han ratificado (N. del T.).

objetivo. Si la ratificación continúa con su actual paso cansino tomará muchos años para el resto del mundo, se trata aproximadamente de 180 países (eso, por su puesto, si todos ellos están dispuestos a hacerlo). Entretanto, la Convención puede ser una herramienta útil para facilitar la cooperación entre aquellos países que la han implementado; esto nos dejaría, después de todo, una idea de cómo trabajarán en la práctica sus disposiciones y si ellas sobrevivirán a los cambios que de seguro traerán para ciertos países. Puede que la Convención finalmente sirva sólo como un primer paso en un proceso que tomará varios años en lograr su objetivo.

Y lo dicho nos lleva a otro asunto: la aproximación que la Convención hace respecto del cibercrimen. Como hemos apuntando antes, ella trata el cibercrimen como un delito convencional, esto es, como un problema interno que debe ser resuelto unilateralmente por el Estado-nación ofendido. Es verdad que el cibercrimen constituye una forma de delincuencia, pero puede ser caracterizado con precisión como algo más que eso; tiene las características básicas propias de la delincuencia tradicional (un actor, una víctima y la comisión de un daño socialmente intolerable), pero no tiene base territorial. A diferencia de los delitos tradicionales, el cibercrimen puede trascender fácilmente las fronteras nacionales. En cambio, la respuesta de la Convención para tal circunstancia es tradicional: tal como los tratados de asistencia legal recíproca, ella solicita a los países brindarse asistencia unos a otros a través de investigaciones y procedimientos en los respectivos países. Esto implica continuar con el sistema de cumplimiento local y descentralizado de que hemos dispuesto por siglos.

Quizá nosotros necesitamos un nuevo sistema para el cibercrimen. Quizá no podemos adoptar el sistema existente para ocuparnos efectivamente del cibercrimen. Quizá otra manera de resolver el vacío de la progresiva implementación de la Convención atestigua acerca de la inutilidad de tratar de adoptar el sistema tradicional de cumplimiento de base nacional para una delincuencia sin base territorial. Entonces, deberíamos considerar una alternativa.

Lógicamente, existen tres modos de estructurar una respuesta apropiada para el cibercrimen. Una de ellas es la adoptada por el Consejo de Europa, en la cual la responsabilidad frente al cibercrimen es analizada en detalle entre los Estados-nación, cada uno de ellos define e investiga el

cibercrimen, procesa y sanciona a los delincuentes informáticos. Como hemos visto, el problema con esta aproximación es que ella tiene una base territorial, mientras el cibercrimen no.

Otra solución en centralizar el cumplimiento de la ley en una agencia individual responsable de controlar el Cibercrimen en todo el mundo. Éste es el modo más extremo. Esta opción generaría una agencia global que sería responsable de declarar fuera de la ley e investigar el cibercrimen, procesar a los delincuentes y sancionarlos. Conceptualmente esta aproximación estaría basada en la premisa de que el ciberespacio ha llegado a ser otra jurisdicción, otra área para la actividad humana y, como tal, requiere de su propia institucionalidad. Implementar esta fórmula requeriría aceptar algo que parece inevitable y que es desconocido en el derecho.

Los países no están dispuestos a entregar la responsabilidad por el cibercrimen en un futuro cercano, lo cual nos lleva al tercer modo de responder ante él, que es una solución intermedia entre las primeras dos. En ésta, el procesamiento y la sanción de los delincuentes permanece en manos de cada Estado-nación, pero los procesos de investigación criminal y aprehensión de los delincuentes serían delegados a una agencia central, una suerte de Súper-Interpol. A diferencia de Interpol, esta agencia no coordinaría simplemente las investigaciones entre las autoridades locales de varios países, en vez de ello sería responsable de la conducción de las investigaciones y del envío de la evidencia y ofensores a los Estados-nación ofendidos. En este escenario, los Estados-nación presumiblemente asumirían la responsabilidad por definir qué es y qué no es un cibercrimen, para ello puede ser aconsejable establecer algún sistema para asegurarse de que sus leyes sean sustancialmente similares. Aparte de constituir la base para la investigación criminal y aprehensión de los delincuentes, este modelo podría tener la virtud adicional de mejorar la respuesta general al cibercrimen. Una agencia global centralizada podría observar las tendencias del cibercrimen, identificándolas mucho antes de convertirse en asunto para los investigadores dispersos en todo el mundo, cada uno trabajando en los confines de su propia estructura institucional.

Obviamente, los últimos dos modos de aproximarse al cibercrimen son especulativos. La reacción visceral que genera el crimen (y el cibercrimen) garantiza que nuestras aproximaciones continúen siendo parro-

quianas en el futuro previsible. Estamos suficientemente impregnados de la realidad territorial para encontrar difícil entregar el control sobre un asunto que ofende nuestro sentido de la moralidad a una entidad «foránea»; como los Padres de la Patria, creemos que los delitos y las penas son asuntos locales.[11] El desafío que tenemos enfrente es reconciliar nuestras creencias con la realidad que está emergiendo en el ciberespacio.

REFERENCIAS

Cassella, Stefan D. (2004). «Bula Cash Smuggling and the Globalization of Crime: Overcoming Constitutional Challenges to Forfeiture under 31 U.S.C. §5332». *Berkeley Journal of International Law*, 22.

Consejo de Europa, «583 Reunión de Delegados Ministeriales», 4 de febrero de 1997, apéndice 13, disponible en <http://www.cm.coe.int/dec/1997/583/583.a13.html>.

SOBRE LA AUTORA

Susan W. Brenner es NCR Distinguished Professor of Law and Technology en la University of Dayton School of Law, Estados Unidos. Su correo electrónico es <susan@cyb3rcrim3.com>.

Este artículo fue recibido el 1 de diciembre de 2010 y aprobado el 20 de diciembre de 2010.

11. *Founding Fathers* o Padres de la Patria es la expresión empleada en Estados Unidos para referirse a quienes firmaron la Declaración de Independencia o la Constitución, o de algún modo manera participaron apoyando la guerra por la Independencia (N. del T.).